

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ
ТЕХНІЧНИЙ УНІВЕРСИТЕТ



Збірник
праць молодих науковців
ЦНТУ

Випуск 16
Частина 2



МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

**Збірник
праць молодих науковців
ЦНТУ**

Випуск 16
Частина 2

Кропивницький – 2026

Збірник праць молодих науковців ЦНТУ. – Вип. 16, ч.2 – Кропивницький: ЦНТУ, 2026 – 324 с.

Збірник праць молодих науковців складається зі змісту, статей та тез здобувачів вищої освіти по матеріалам дипломних робіт.

Організаційний комітет:

Голова – А. Кириченко, д-р техн. наук, професор

Редакційна колегія:

В Крöpfивний	канд. техн. наук, професор (головний редактор)
А. Тихий	канд. техн. наук, доцент (заступник головного редактора)
Л. Резнік	відповідальний секретар
Р. Жовновач	д-р. екон. наук, професор
В. Мажара	канд. техн. наук, доцент
С. Магопець	канд. техн. наук, доцент
О. Медведєва	канд. біол. наук, доцент
М. Мостіпан	канд. біол. наук, універс-професор
І. Миценко	д-р. екон. наук, професор
О. Магопець	канд. екон. наук, доцент
В. Настоящий	канд. техн. наук, універс-професор
В. Орлик	д-р. іст. наук., професор
О. Дідик	канд. техн. наук, доцент
А. Гречка	канд. техн. наук, доцент
В. Сибірцев	д-р. екон. наук, професор
П. Плєшков	канд. техн. наук, універс-професор
О. Васильковський	канд. техн. наук, професор
В. Зайченко	д-р. екон. наук, доцент
О. Смірнов	д-р. техн. наук, професор

Автори опублікованих матеріалів несуть відповідальність за підбір і точність наведених фактів, цитат, економіко-статистичних даних, власних імен та інших відомостей, а також за те, що матеріали не містять дані, які не підлягають відкритій публікації. Друкується в оригіналі згідно поданих робіт.

© Центральноукраїнський національний технічний університет

УДК 004

П.Лобода, магістр гр. КН-24М,

Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ІЄРАРХІЧНОГО ЗБЕРІГАННЯ ДАНИХ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ TIERED STORAGE

У статті розроблено програмне забезпечення, яке призначено для системи ієрархічного зберігання даних з використанням технології Tiered Storage. Метою розробки є дослідження та принципи побудови системи ієрархічного зберігання даних з використанням технології Tiered Storage. Об'єктом дослідження є процес ієрархічного зберігання даних з використанням технології Tiered Storage. Предметом дослідження є методи ієрархічного зберігання даних з використанням технології Tiered Storage. Методи дослідження базуються на методах великих даних, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи ієрархічного зберігання даних з використанням технології Tiered Storage. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

ієрархічне зберігання даних, Tiered Storage

Постановка проблеми. Програмне забезпечення, також відоме як багаторівневе сховище, було розроблено для розподілених серверних середовищ, щоб автоматизувати процес ідентифікації холодних наборів даних та автоматичної міграції їх з основного диска на менш дорогі оптичні та стрічкові пристрої зберігання даних. Повертаючись до ери мейнфреймів, HSM також мав автоматично обробляти запити на відкриття файлів щоразу, коли користувач натискав на файл-заглушку.

На жаль, ці ранні продукти HSM мали низку недоліків. Ці недоліки були настільки серйозними, що HSM стало «поганим словом» серед ІТ-фахівців. Багато з цих ІТ-фахівців вважали, що єдиний життєздатний спосіб управління сховищем – це просто продовжувати додавати більше потужностей до основного рівня.

Оскільки ландшафт центрів обробки даних змінився, організації отримали широкий спектр варіантів зберігання даних, флеш-пам'ять замінила високопродуктивні фізичні дискові накопичувачі як сховища першого рівня. Високопродуктивні та звичайні фізичні жорсткі диски тепер функціонують як вторинні та третинні рівні зберігання. Доступні хмарні сховища файлів та об'єктів для обробки великих обсягів довгострокових вимог до зберігання. Всі ці опції необхідні для боротьби з неструктурованим напливом даних (а також розростанням даних та високими витратами на зберігання даних), з якими стикається більшість організацій. Однак основна проблема залишається: як автоматично виявляти «теплі» та «холодні» набори даних, а потім безперервно переносити їх на найефективніший рівень зберігання, одночасно керуючи всім життєвим циклом файлу.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи ієрархічного зберігання даних з використанням технології Tiered Storage.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи ієрархічного зберігання даних з використанням технології Tiered Storage.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем ієрархічного зберігання даних з використанням технології Tiered Storage.

– Дослідження системи ієрархічного зберігання даних з використанням технології Tiered Storage.

– Програмна реалізація системи ієрархічного зберігання даних з використанням технології Tiered Storage.

Об'єктом дослідження є процес ієрархічного зберігання даних з використанням технології Tiered Storage.

Предметом дослідження є методи ієрархічного зберігання даних з використанням технології Tiered Storage.

Методи дослідження базуються на методах великих даних, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Існують проблеми, пов'язані з обробкою, переміщенням, зберіганням або обробкою великих обсягів чого завгодно, і в абсолютно не пов'язаних між собою сферах ці проблеми можуть виглядати дуже схожими. Розглянемо поштову службу: для доставки листів і посилок туди, куди їм місце, потрібна складна мережа літаків, кораблів, напівпричепів, машин, транспортних засобів доставки та людей. І на кожному етапі існують величезні ризики, пов'язані з ефективністю, вартістю, затримками та помилками.

Наприклад, уявіть собі використання напівпричепа для доставки пошти від дверей до дверей і скільки місця буде витрачено у вантажівці. Або уявіть собі парк невеликих електричних поштових транспортних засобів, які перевозять пошту з Аляски до Флориди, замість використання літака.

Це спрощені приклади, але вони допомагають пояснити, чому існує ієрархічне управління сховищами (HSM). Організації з великими обсягами даних постійно стикаються з проблемами ефективності, і багато зусиль витрачається на планування того, як зберігати, переміщувати та обробляти всю цю інформацію. Ієрархічне управління сховищами (HSM) – це історичний метод, який гарантує, що організації по суті не використовуватимуть напівпричепа як засоби доставки своїх цифрових даних.

У даному розділі ми розглянемо HSM, проблеми, які він прагне вирішити, та деякі сучасні альтернативи йому.

Що таке ієрархічне управління сховищами?

Ієрархічне управління сховищем, або HSM, – це процес управління цифровими даними, метою якого є максимально економічне використання носіїв інформації, мінімізуючи при цьому неефективність використання даних.

Два ключові факти лежать в основі HSM: по-перше, різні методи зберігання цифрових носіїв мають різні характеристики. По-друге, не всі дані обробляються однаково. Щодо першого пункту, найбільш очевидною відмінністю між різними цифровими носіями інформації є вартість. Найшвидші, найдоступніші та найуніверсальніші носії інформації, як правило, є найдорожчими. А що стосується другого пункту, деякі дані використовуються щодня, тоді як деякі дані використовуються набагато рідше.

Прибуток багатьох компаній залежить від швидкого доступу до найважливіших даних. Але було б надзвичайно неефективно платити стільки ж за зберігання та доступ до даних, які вони використовують лише частку часу, з тим самим рівнем швидкості та доступності.

Різні організації впроваджують HSM по-різному – єдиного зводу правил для використання HSM не існує. Але щоразу, коли організація розділяє своє сховище даних щонайменше на два рівні, HSM – це процес встановлення правил щодо того, що де зберігається та як це переміщується.

Переваги ієрархічного управління сховищами

Організації можуть побачити низку переваг від впровадження ієрархічного управління сховищами. Економія коштів є найбільш очевидною перевагою HSM: переміщуючи менш термінові дані на дешевші носії, компанії можуть пожертвувати доступністю заради вартості. Продуктивність також загалом покращується завдяки

принципам HSM. Коли програми, яким потрібен доступ до даних, не витрачають час на перегляд старих, застарілих або нерелевантних даних, вони можуть забезпечити кращі результати швидше.

І хоча HSM може здатися складним, чіткі правила визначення місця розташування різних категорій даних та їх автоматичне застосування призводять до спрощеного управління даними. HSM також оптимізує використання сховища, оскільки автоматично переносить дані на відповідний рівень сховища на основі правил, встановлених ІТ-фахівцями.

Як працює ієрархічне управління сховищами?

HSM може складатися з багатьох шарів носія інформації, але його суть полягає в тому, що на одному кінці знаходиться високопродуктивний рівень, а на іншому – повільніший і дешевший рівень. Високопродуктивний рівень традиційно складався з пам'яті класу сховища, твердотільних накопичувачів (SSD) корпоративного класу та високопродуктивних жорстких дисків. На нижчому рівні знаходяться такі пристрої, як оптичні диски та навіть стрічкові накопичувачі.

Фактичне впровадження політик HSM є досить складним, але HSM по суті працює, визначаючи частоту доступу до файлу, і з плином часу система автоматично переміщує рідко використовувані файли до повільнішого та дешевшого сховища. ІТ-команди пишуть правила для параметрів, які визначають, коли дані переміщуються, які дані виключені з цих правил та інші уточнення. Але HSM, як правило, є автоматизованим процесом, який оптимізує доступ до даних та витрати на їх зберігання.

Які рівні HSM?

Ключ до розуміння HSM та використання носіїв інформації, таких як стрічкові накопичувачі, полягає в тому, що колись різниця між вартістю, продуктивністю та швидкістю була надзвичайною. Хоча ці розриви зменшилися і постійно зменшуються, був час, коли різниця у вартості між оптичними дисками та твердотільними накопичувачами була достатньо суттєвою, щоб виправдати складні методи сортування даних, щоб ви ніколи не витрачали гроші даремно.

Рівень HSM з найменшим обсягом та найвищою продуктивністю зазвичай називається Рівнем 0. Це критично важливі дані, які не можуть дозволити собі затримок або перебоїв у роботі. Рівень 1 часто називають «гарячими даними», даними, які постійно використовуються для щоденних бізнес-операцій, а терміновість яких може бути збалансована витратами на зберігання. Рівень 2 – це «теплі дані», де вартісним міркуванням надається значний пріоритет, і куди поміщаються дані, до яких не часто звертаються. Нарешті, Рівень 3 зазвичай стосується «холодних даних», або даних, до яких рідко звертаються або оновлюють дані, якщо взагалі звертаються.

Альтернативи рівням HSM, що базуються на повністю флеш-пам'яті

В ідеальному світі компанія могла б мати швидке, високодоступне сховище на всіх рівнях, з тонкими розмежуваннями між ними. Протягом десятиліть мрією було повністю флеш-сховище даних на рівні підприємства. Але донедавна це було просто неможливо. Однак за останні кілька десятиліть вартість повністю флеш-сховища на рівні підприємства не просто можлива, це робиться регулярно.

Pure Storage є помітним лідером у сфері повністю флеш-сховищ для підприємств і ще у 2012 році розробила рішення для флеш-сховищ, які могли задовольнити потреби корпоративної мережі рівня Tier 0. Коли FlashArray//C™ був випущений, Pure Storage міг гарантувати стабільну затримку в одну мілісекунду для критично важливих бізнес-навантажень і даних корпоративних мереж, з доступністю 99,9999% та оновленнями без переривання роботи.

Це саме по собі було новаторським, а потім FlashArray//X™ та FlashArray//XL™ дозволили запускати на флеш-пам'яті все: від величезних баз даних до хмарних програм. Навіть з цими досягненнями все ще вважалося, що рівні 2 та 3 ніколи не потраплять до флеш-пам'яті через вартість.

Але у 2023 році Pure Storage випустила FlashArray//E™ та FlashBlade//E™, які кидають виклик низькоякісним обертовим дискам та стрічкам. Розроблений для довготривалого зберігання, FlashArray//E забезпечує ємність зберігання необроблених, уніфікованих файлових та блочних даних від 1 ПБ до 4 ПБ. FlashBlade//E може заощадити компаніям купу грошей під час зберігання неструктурованих та об'єктних робочих навантажень.

Pure Storage показує приклад повністю флеш-альтернатив рівням HSM для організацій будь-якого розміру. Хоча ми не скасовуємо HSM як такий, ми радикально змінюємо межі, що розділяють рівні HSM.

Ієрархічне управління сховищами виникло як необхідна відповідь на величезну різницю у вартості, що існувала між найшвидшими, найдорожчими та найповільнішими, але найдоступнішими формами зберігання даних. Технологічні обмеження призвели до появи цілої сфери кар'єри, присвяченої автоматичній категоризації, переміщенню та оптимізації рішень для зберігання даних.

HSM все ще є важливим процесом економії коштів, але повністю флеш-рішення корпоративного масштабу, такі як ті, що пропонуються Pure Storage, швидко позбавляються чітких розмежувань між ними, водночас забезпечуючи величезні обсяги швидких даних за значно меншу ціну, ніж раніше.

Організація ієрархічних даних є унікальною проблемою в галузі управління базами даних СУБД. Ієрархічні структури поширені в багатьох галузях, від організації в діаграмах до систем зберігання даних та категорій продуктів.

Для ефективного зберігання та запитування ієрархічних даних у реляційних базах даних RDBMS необхідний ретельний розгляд схеми бази даних та обраної моделі зберігання.

У цій статті ми розглянемо доступні варіанти зберігання ієрархічних даних у реляційній базі даних, досліджуючи їхні переваги, недоліки та варіанти використання. Основні варіанти:

1. Модель списку суміжності.
2. Перерахування шляхів.
3. Модель вкладеного набору.
4. Модель матеріалізованого шляху.

Перш ніж заглибитися, давайте розберемося з цими концепціями:

Що таке реляційна база даних?

Реляційна база даних – це тип бази даних, яка впорядковує дані в рядки та стовпці, що разом утворюють таблицю, де точки даних пов'язані одна з одною (РСБД).

SQL-запити агрегують дані, допомагаючи фірмам аналізувати ефективність бізнесу, оптимізувати процеси та генерувати аналітичні висновки. Вони впорядковують дані, пов'язуючи таблиці за допомогою первинних та зовнішніх ключів, виявляючи взаємозв'язки.

Зберігання ієрархічних даних у базі даних

Керування ієрархічними даними в реляційних базах даних є складним завданням через невідповідність між ієрархічними структурами та табличною природою реляційних баз даних. Стратегії пояснюються нижче:

1. Модель списку суміжності

Модель списку суміжності – це простий та інтуїтивно зрозумілий спосіб представлення ієрархічних даних у реляційних базах даних. У цій моделі кожен запис містить посилання на батьківський запис, утворюючи деревоподібну структуру. Наприклад, таблиця співробітників може містити поле, що посилається на ідентифікатор менеджера для кожного співробітника.

Переваги:

- Легко зрозуміти та застосувати на практиці.
- Гнучкість є відображенням асиметричних ієрархій.

Недоліки:

- Можуть виникати неефективні запити та перетин ієрархій, особливо для глибоко вкладених структур.
- Часто потрібні рекурсивні запити, які можуть бути складними та ресурсомісткими.

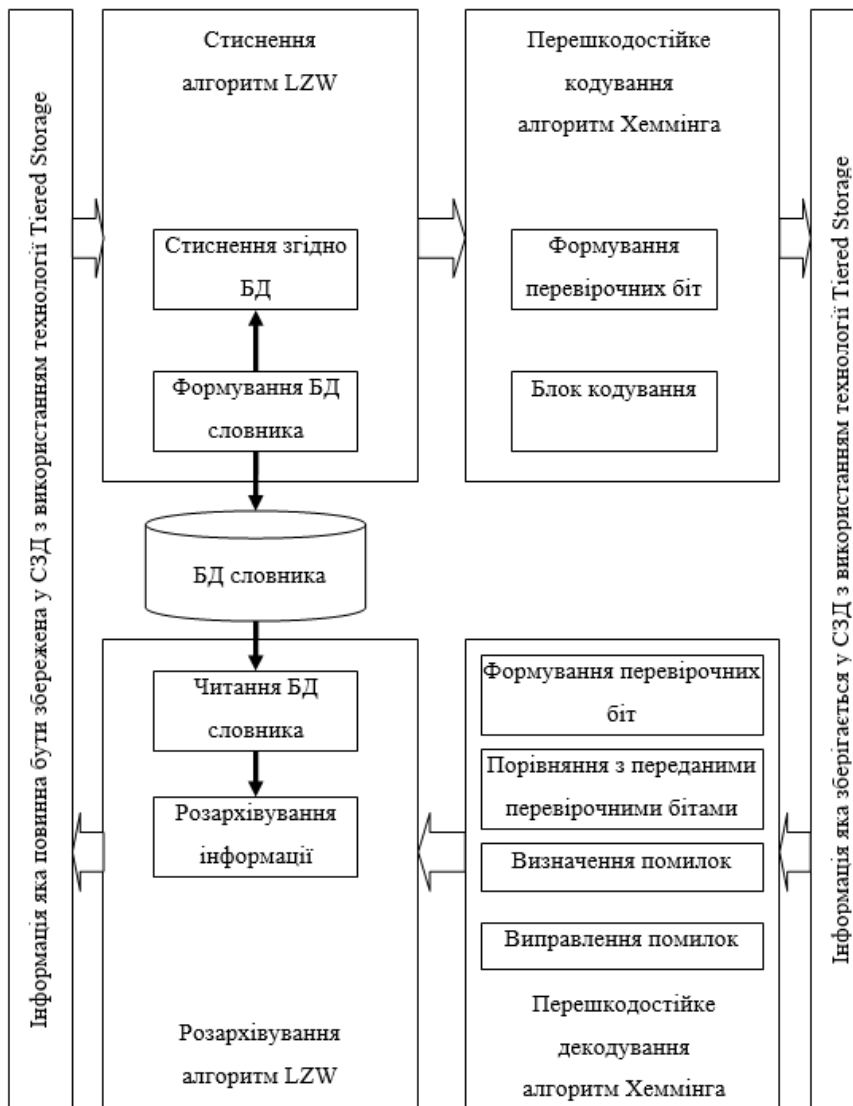


Рисунок 1 – Структурна схема системи

2. Перерахування шляхів

У реляційній базі даних перерахування шляхів – це метод зберігання ієрархічних даних, в якому записується повний шлях кожного вузла від кореневого вузла. За допомогою заданого шляху цей метод спрощує отримання батьківських або дочірніх вузлів, але це може призвести до уповільнення запитів, особливо для великих наборів даних.

Перерахування шляхів спрощує отримання ієрархічних даних, але може збільшити тривалість пошуку, особливо для структур з кількома рівнями вкладеності. Крім того, може знадобитися оновити кілька рядків для оновлення ієрархії, що може вплинути на продуктивність. Через це важливо ретельно зважити всі компроміси під час вибору формату зберігання реляційної бази даних для ієрархічних даних.

Переваги:

- Простий у впровадженні.
- Просте отримання батьківських або дочірніх вузлів за певним шляхом.

Недоліки:

- Отримання та перетин ієрархій може бути повільним та ресурсомістким, особливо для великих наборів даних.

– Обмежена підтримка таких операцій, як запити до піддерев або переупорядкування вузлів.

3. Модель вкладених множин

У моделі вкладених множин два числа – ліве значення та праве значення – представляють кожен вузол у дереві для зберігання ієрархічних даних у реляційній базі даних. Спосіб розподілу цих значень дозволяє ефективно запитувати ієрархічну структуру, отримувати піддерева та виконувати такі операції, як підрахунок нащадків.

Переваги:

- Ефективний для пошуку піддерев та операцій, таких як підрахунок нащадків.
- Добре підходить для ієрархій з частими операціями читання.

Недоліки:

- Складно обслуговувати, особливо під час вставки або видалення вузлів.
- Запити, що включають оновлення ієрархії, можуть бути складними та обчислювально дорогими.

Модель матеріалізованого шляху

Подібно до перерахування шляхів, матеріалізована модель шляху зберігає повний шлях кожного вузла, а також додаткові оптимізації, такі як зберігання глибини кожного вузла.

Переваги:

- Спрощує запити та перехід через ієрархії.
- Ефективно підтримує такі операції, як пошук піддерев та запити на основі шляхів.

Недоліки:

- Може знадобитися додаткове місце для зберігання.
- Оновлення ієрархії можуть бути складними, особливо коли вузли переміщуються або реорганізуються.

На завершення, вибір відповідної моделі зберігання ієрархічних даних у реляційній базі даних залежить від різних факторів, включаючи розмір і складність ієрархії, частоту оновлень і типи запитів, які будуть виконуватися. Хоча кожна модель зберігання має свої переваги та недоліки, розуміння нюансів кожного підходу є вирішальним для розробки ефективних і масштабованих схем баз даних, які ефективно керують ієрархічними даними.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів ієрархічного зберігання даних з використанням технології Tiered Storage. Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем ієрархічного зберігання даних з використанням технології Tiered Storage.

– Досліджена система ієрархічного зберігання даних з використанням технології Tiered Storage.

– На основі отриманих результатів досліджень створена програмна реалізація системи ієрархічного зберігання даних з використанням технології Tiered Storage.

Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання ієрархічного зберігання даних з використанням технології Tiered Storage. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Смірнов, О.А., Константинова, Л.В., Коноплицька-Слободенюк, О.К., Козірова, Н.В., Якименко, Н.М., Доренський, О.П., Буравченко, К.О. «Дослідження інструментів штучного інтелекту для роботи з базами даних та аналізу даних». Кібербезпека: освіта, наука, техніка. 2025. №3(27), С. 429–448.)

2. Smirnov O., Fedorov E., Neskorodieva A., Neskorodieva T. «Intellectual Classification method of Gymnastic Elements Based on Combinations of Descriptive and Generative Approache». CEUR Workshop Proceedings Volume 3664, 2024, Pages 11-23.
3. Вінтенко, Б., Миронець, І., Смірнов, О., Коваленко, А., Коноплицька-Слободенюк, О., Смірнова, Т., Константинова, Л. «Дослідження застосування систем підтримки оперативного персоналу об'єкту критичної інфраструктури при керуванні енергоблоком АЕС з реактором типу ВВЕР-1000». Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2024. № 2(26), С. 6-26.
4. Вінтенко, Б., Миронець, І., Смірнов, О., Кравчук, О., Козірова, Н., Савеленко, Г., Коваленко, А. «Дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». Кібербезпека: освіта, наука, техніка. 2024. №3(23), С. 111-131.
5. Kuznetsov O., Ilchenko O., Kryvinska N., Buravchenko K., Smirnov O., Savchenko Iu. «An Empirical Assessment of Leading Blockchain Financial Services». 2023 IEEE 1st Ukrainian Distributed Ledger Technology Forum (UADLTF), Kyiv, Ukraine, 2023, pp. 1-6,
6. Kuznetsov, O., Kryvinska, N., Ilchenko, O., Smirnova, T., Ulianovska, Y. «Comparative Analysis of Cryptocurrency Trading Platforms Using the Analytic Hierarchy Process». CEUR Workshop Proceedings, 2023, 3628, pp. 106-115.
7. Malyukov V., Bebesheko B., Lakhno V., Smirnov O., Malyukova I., Mohylnyi H. «Managing the Purchase-Sale Process of Digital Currencies Under Fuzzy Conditions». Lecture Notes in Networks and Systems, 2023, 729 LNNS, pp. 104–112.
8. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». Advanced Information Systems, 2023, 7(2), pp. 49-56.
9. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchey, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». CEUR Workshop Proceedings, Volume 3530, 2023, pp. 256-265.
10. Smirnov, O., Odarchenko, R., Smirnova, T., Bondar, S., Volosheniuk, D. «Optimal Structure Construction of Private 5G Network for the Needs of Enterprises». Lecture Notes on Data Engineering and Communications Technologies, 2023, 178, pp. 208–223.
11. Вінтенко Б.Ю., Смірнов О.А., Коваленко А.С., Смірнов С.А., Буравченко К.О. «Дослідження вимог міжнародних стандартів IEC60880 та IEC62138 з розробки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». Системи управління, навігації та зв'язку, 2023, вип. 3(73), С. 155-166.
12. Вінтенко, Б., Миронець, І., Смірнов, О., Кравчук, О., Козірова, Н., Савеленко, Г., Коваленко, А. «Дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». Кібербезпека: освіта, наука, техніка. 2024. №3(23), С. 111-131.
13. Вінтенко Б.Ю., Смірнов О.А., Коваленко О.В., Смірнов С.А., Коваленко А.С. «Дослідження нормативних документів та галузевих стандартів розробки програмного забезпечення комп'ютерних систем управління АЕС, важливих для безпеки». Системи управління, навігації та зв'язку, 2023, вип. 2(72), С. 170-178.
14. Аль-Мудхафар Акіл Абдулхуссейн М., Смірнова Т.В., Буравченко К.О., Смірнов О.А. «Метод оцінки та підвищення користувальницького досвіду абонентів в програмно-конфігурованих мережах на основі використання машинного навчання». Сучасні інформаційні системи, 2023, том 7, № 2, С. 49-56.
15. Вінтенко Б.Ю., Смірнов О.А., Коваленко О.В., Смірнов С.А. «Дослідження нормативної документації та стандартів розробки програмного забезпечення комп'ютерних систем управління АЕС, важливих для безпеки». VI міжнародна науково-практична конференція «Інформаційна безпека та комп'ютерні технології», м. Кропивницький. 20-21 квітня 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 35-36.
16. Smirnov, O., Karapetyan, A., Fedorov, E., «Creating Neural Network and Single Solution Human-Based Metaheuristic Methods of Solving the Traveling Salesman Problem». CEUR Workshop Proceedings, Volume 3312, 2022, pp. 47-58.
17. Smirnov O., Kuznetsov A., Kryvinska N., Kiian A., Kuznetsova K. «Full Non-Binary Constant-Weight Codes». SN Computer Science, Vol 2, 337, 2021. <https://doi.org/10.1007/s42979-021-00739-w>.
18. Smirnov O., Kovalenko O., Kovalenko A., Kavun S. «Quantitative Risk Assessment Method Development in the Context of the SDLC-model». 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), 2021, pp. 203-208, doi: 10.1109/PICST54195.2021.9772143
19. Smirnova T., Gnatyuk S., Berdibayev R., Avkurova Zh., Iavich M. «Cloud-Based Cyber Incidents Response System and Software Tools». Communications in Computer and Information Science, 2021, vol 1486. Springer, Cham. pp 169-184.
20. Smirnov, O., Kuznetsov, A., Potii, O., Poluyanenko, N., Stelnyk, I., Mialkovsky, D. «Combining and filtering functions in the framework of nonlinear-feedback shift register». International Journal of Computing; 2020, Volume 19, Issue 2 – Research Institute for Intelligent Computer Systems – 2020. – P. 247-256.
21. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
22. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on

- Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177.
23. Smirnov, O., Shekhanin, K., Kuznetsov, A., Krasnobayev, V. «Detecting Hidden Information in FAT». International Journal of Computer Network and Information Security (IJCNIS). Vol. 12, No. 3, 2020. PP.33-43.
 24. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645.
 25. Smirnov O. Kuznetsov A., Zaichenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019; Odessa; Ukraine; 9-13 September 2019. P.22-28.
 26. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.
 27. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019 . P.517-522.
 28. Smirnov, O., Krasnobayev, V., Yanko, A., Kuznetsova, T. «Methods of nulling numbers in the system of residual classes». CEUR Workshop Proceedings, Vol 2588, P. 90-106, 2019.
 29. Kuznetsova, T., «Code-Based Schemes for Post-Quantum Digital Signatures», 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2019; Metz; France; 18-21 September 2019. P. 707-712.
 30. Smirnov, O., Kuznetsov, A., Stefanovych, O., Gorbenko, Y., Krasnobayev, V., Kuznetsova K. «Information Hiding Using 3D-Printing Technology», 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2019; Metz; France; 18-21 September 2019. P.701-706.
 31. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Averchev, A., Pastukhov, M., Kuznetsova, K., «Formation of Pseudorandom Sequences with Special Correlation Properties», 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT -2019/ Lviv, Ukraine, 2-6 July, 2019, P. 395-399.
 32. Смірнов, О.А., Усік П.С., Полігенько О.О., Одарченко Р.С., Терещенко Л.Ю. «Інформаційна технологія та програмне забезпечення для підвищення ефективності планування підсистеми базових станцій стільникового зв'язку». Проблеми телекомунікацій. № 1(26). С. 83-96. 2020.

УДК 004

В.Маламуж, магістр гр. КН-24М,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ УПРАВЛІННЯ У РОЗПОДІЛЕНИХ CLOUD-CИСТЕМАХ GENI

У статті розроблено програмне забезпечення, яке призначено для системи управління у розподілених Cloud-системах GENI. Метою розробки є дослідження та принципи побудови системи управління у розподілених Cloud-системах GENI. Об'єктом дослідження є процес управління у розподілених Cloud-системах GENI. Предметом дослідження є методи управління у розподілених Cloud-системах GENI. Методи дослідження базуються на методах хмарних обчислень, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи управління у розподілених Cloud-системах GENI. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

методи управління, розподілені Cloud-системи, GENI

Постановка проблеми. GENI використовується для досліджень у сфері майбутніх інтернет-архітектур, програмно-визначених мереж, нових протокольних наборів, які можуть базуватися на IP, а можуть і не базуватися, бездротових мереж 4G та хмарних обчислень. GENI добре підходить для експериментів, які потребують:

- Масштабна експериментальна інфраструктура. GENI надає вам доступ до сотень широко розподілених ресурсів, включаючи обчислювальні ресурси, такі як віртуальні машини та «голі машини», а також мережеві ресурси, такі як з'єднання, програмовані комутатори та бездротові базові станції 4G.

- Не-IP-з'єднання між ресурсами. GENI дозволяє налаштовувати з'єднання 2-го рівня між комп'ютерними ресурсами та запускати власні протоколи 3-го рівня та вище.

- Глибокі можливості програмування. За допомогою GENI ви можете програмувати не лише кінцеві хости вашої експериментальної мережі, але й комутатори в ядрі вашої мережі. Це дозволяє експериментувати з новими протоколами мережевого рівня або з новими алгоритмами IP-маршрутизації.

- Інструменти та засоби вимірювання. Системи приладів та вимірювань GENI дозволяють вам інструментально аналізувати ваші експерименти, візуалізувати вимірювання та архівувати їх.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи управління у розподілених cloud-системах GENI.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи управління у розподілених Cloud-системах GENI.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем управління у розподілених Cloud-системах GENI.
 - Дослідження системи управління у розподілених Cloud-системах GENI.
 - Програмна реалізація системи управління у розподілених Cloud-системах GENI.
- Об'єктом дослідження є процес управління у розподілених Cloud-системах GENI.
Предметом дослідження є методи управління у розподілених Cloud-системах GENI.

Методи дослідження базуються на методах хмарних обчислень, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Проблеми управління розподіленими системами

Керування розподіленими системами створює кілька проблем через їхню притаманну складність та розподілену природу. Керування розподіленими системами створює кілька проблем через їхню притаманну складність та розподілену природу.

— Складність:

○ Впровадження розподілених систем вимагає великої кількості самодостатніх компонентів, які є взаємопов'язаними та мають власну конфігурацію, залежності та протоколи зв'язку.

○ В цифрову епоху, коли правильне виконання цих частин та ефективне управління ними може бути болісним завданням.

— Консистенція:

○ З іншого боку, найскладнішим питанням є досягнення узгодженості даних між розподіленими вузлами, особливо для обробки одночасних оновлень та збоїв.

○ Це вимагає вдосконалених методів координації та синхронізації.

— Безпека:

○ Гарантія того, що розподілені системи не будуть зламані, а неавторизовані особи не отримають до них доступу за допомогою надійних інструментів безпеки, є важливим заходом і потребує шифрування, автентифікації та контролю доступу для всіх зацікавлених сторін.

Централізоване проти децентралізованого управління

1. Централізоване управління

У централізованому управлінні всі повноваження щодо контролю та прийняття рішень зосереджені в межах однієї сутності або центрального органу. Ця сутність зазвичай має повноваження приймати рішення, розподіляти ресурси та забезпечувати дотримання політик у всій системі.

— Повноваження щодо прийняття рішень належать центральному органу влади або керівному органу.

— Політики, правила та процедури встановлюються та застосовуються централізовано.

— Розподіл ресурсів, координація та контроль здійснюються з однієї точки.

— Комунікація та потік інформації зазвичай спрямовуються через центральний орган влади.

2. Децентралізоване управління

У децентралізованому управлінні повноваження щодо прийняття рішень, контроль та координація розподілені між кількома об'єктами або вузлами в системі. Кожен об'єкт або вузол працює автономно та має право самостійно приймати рішення в межах своєї сфери відповідальності.

— Повноваження щодо прийняття рішень розподілені між кількома сутностями або вузлами.

— Сутності або вузли мають автономію приймати рішення та діяти самостійно.

— Координація та комунікація відбуваються безпосередньо між сутностями або вузлами без централізованого контролю.

Моніторинг розподілених систем

Спостереження за розподіленими системами є ключовою функцією; воно має забезпечувати відстеження відхилень, оптимізацію роботи та усунення помилок. Ключові показники для моніторингу включають:

— **Пропускна здатність:** Вимірює час відгуку окремо як показник загальних можливостей системи упаковувати та поміщати транзакції в чергу за раз.

– **Затримка:** З іншого боку, вона позначає період часу, необхідний для виконання запиту, що може бути ознакою того, наскільки швидко працює система.

– **Використання ресурсів:** Відстежує використання процесора, а також пам'яті, сховища та пропускної здатності мережі. Таким чином, немає можливості затримки, а ресурси розподіляються ефективно.

– **Коефіцієнти помилок:** Він також досліджує, як часто виникають помилки та збої, пропонуючи вам уявлення про регулярність та надійність систем.

Реєстрація та трасування в розподілених системах

Ведення журналу та трасування є важливими компонентами моніторингу та налагодження розподілених систем, допомагаючи розробникам та адміністраторам розуміти поведінку системи, діагностувати проблеми та оптимізувати продуктивність.

1. Вхід у розподілених системах

Ведення журналу включає запис подій, повідомлень та інформації про системні операції, помилки та дії на постійне сховище (наприклад, файли, бази даних або системи керування журналами). Ведення журналу забезпечує історичний запис поведінки системи, допомагаючи розробникам та адміністраторам відстежувати потік виконання, виявляти помилки або аномалії та усувати неполадки.

– Повідомлення журналу зазвичай містять позначки часу, рівні серйозності (наприклад, INFO, DEBUG, WARN, ERROR), контекстну інформацію (наприклад, назву компонента, ідентифікатор запиту) та описові деталі (наприклад, трасування стека помилок, параметри запиту).

– Розробники використовують ведення журналу для моніторингу стану програм, відстеження потоку програм, налагодження проблем, аудиту дій користувачів та дотримання нормативних вимог.

2. Трасування в розподілених системах

Трасування включає фіксацію та кореляцію розподілених транзакцій або запитів, коли вони поширюються через різні компоненти чи служби в розподіленій системі. Трасування допомагає розробникам та адміністраторам зрозуміти наскрізний потік запитів між розподіленими компонентами, виявити вузькі місця в продуктивності та проаналізувати затримку та залежності.

– Трасування складаються з серії корельованих інтервалів, кожен з яких представляє певну операцію або дію в межах компонента чи сервісу. Інтервали містять метадані, такі як назви операцій, позначки часу початку та завершення, а також контекстну інформацію (наприклад, назву сервісу, ідентифікатор запиту).

– Розробники використовують трасування для візуалізації потоків запитів, вимірювання показників продуктивності на рівні сервісів (наприклад, часу відгуку, пропускної здатності), аналізу залежностей між сервісами та оптимізації продуктивності розподіленої системи.

Управління конфігурацією в розподілених системах

Управління конфігурацією охоплює процеси, інструменти та методи для визначення, розгортання, оновлення та моніторингу параметрів конфігурації та ресурсів розподілених систем. Деякі з цілей управління конфігурацією включають:

– **Забезпечення узгодженості:** управління конфігурацією гарантує, що всі вузли або компоненти в розподіленій системі мають узгоджені налаштування конфігурації, запобігаючи дрейфу конфігурації та невідповідностям.

– **Покращення масштабованості:** автоматизуючи завдання управління конфігурацією, розподілені системи можуть масштабуватися ефективніше, що дозволяє швидко розгортати та надавати нові вузли або ресурси.

– **Підвищення надійності:** Підтримуючи стандартизовану конфігурацію та впроваджуючи найкращі практики, управління конфігурацією допомагає підвищити надійність і стабільність розподілених систем.

– Спрощення управління змінами: управління конфігурацією дозволяє систематично відстежувати, версіювати та аудит змін конфігурації, що спрощує керування та відкат змін за потреби.

Розподіл ресурсів у розподілених системах

Розподіл ресурсів передбачає визначення того, як розподілити доступні ресурси між конкуруючими завданнями або роботами в розподіленій системі для оптимізації продуктивності, використання та справедливості.

– Оптимізація продуктивності: розподіл ресурсів таким чином, щоб максимізувати пропускну здатність системи, мінімізувати час відгуку та відповідати вимогам якості обслуговування (QoS).

– Забезпечення справедливості: розподіл ресурсів справедливо між конкуруючими завданнями або користувачами, щоб запобігти їх дефіциту та сприяти рівному доступу до ресурсів.

Деякі з підходів до розподілу ресурсів у розподілених системах включають:

– Статичне розподілення:

○ Попередньо розподіляйте ресурси між завданнями або роботами на основі попередньо визначених політик, пріоритетів або квот.

○ Цей підхід підходить для передбачуваних робочих навантажень з фіксованими вимогами до ресурсів.

– Динамічне розподілення:

○ Динамічно налаштовуйте розподіл ресурсів на основі характеристик робочого навантаження, системних умов та показників продуктивності.

○ Такі методи, як балансування навантаження, автоматичне масштабування та адаптивне виділення ресурсів, використовуються для коригування розподілу ресурсів у режимі реального часу.

– Розподіл кількох ресурсів:

○ Розподіляючи ресурси між завданнями або роботами, враховуйте одночасно кілька ресурсів (наприклад, процесор, пам'ять і диск), враховуючи взаємозалежність та обмеження ресурсів.

Планування в розподілених системах

Планування включає визначення часу і місця виконання завдань на розподілених вузлах для досягнення цільових показників продуктивності, обмежень ресурсів та системних вимог.

– Мінімізація затримки: Плануйте завдання або роботи, щоб мінімізувати час очікування, час відгуку та затримки обробки, покращуючи швидкість реагування системи та взаємодію з користувачем.

– Максимізація пропускну здатності: Планування завдань або проектів для максимізації пропускну здатності системи та обчислювальної потужності, забезпечення ефективного використання доступних ресурсів.

Деякі з підходів до розподілу ресурсів у розподілених системах включають:

– Планування на рівні завдань:

○ Плануйте окремі завдання або роботи на основі пріоритету, термінів, залежностей та потреб у ресурсах.

○ Такі методи, як планування на основі пріоритетів, планування за термінами та планування з урахуванням залежностей, використовуються для оптимізації виконання завдань.

– Пакетне планування:

○ Плануйте групи пов'язаних завдань або проектів (наприклад, завдання пакетної обробки, завдання MapReduce), щоб оптимізувати використання ресурсів та мінімізувати час виконання завдань.

- Глобальне планування:
 - Координуйте рішення щодо планування між кількома вузлами або кластерами для оптимізації продуктивності всієї системи та розподілу ресурсів.
 - Такі методи, як глобальне балансування навантаження, розподілені алгоритми планування та централізовані планувальники, використовуються для координації рішень щодо планування в розподілених середовищах.

Виявлення та відновлення несправностей у розподілених системах

Інструмент виявлення дефектів – це механізм виявлення несправностей, який допомагає визначити стан розподілених компонентів і, таким чином, швидко виявляти збої та реагувати на них. Вбудовані механізми відновлення, які можуть обробляти реплікацію, резервування та відновлення після відмови в системі, забезпечують безперервність та стійкість обслуговування з метою мінімізації простоїв або перебоїв у роботі.

1. Підходи до виявлення несправностей

– Моніторинг на основі серцебиття: Вузли періодично надсилають повідомлення про серцебиття, щоб вказати свою доступність та стан. Вузли моніторингу виявляють несправності, аналізуючи повідомлення про серцебиття та виявляючи відхилення від очікуваних шаблонів.

– Детектори відмов: Розподілені алгоритми та протоколи використовують детектори відмов для виявлення відмов вузлів або збоїв на основі спостережуваної поведінки, таймаутів повідомлень або збоїв зв'язку.

– Виявлення аномалій: Машинне навчання та статистичні методи використовуються для виявлення аномалій або незвичайних закономірностей у системних метриках, даних про продуктивність або поведінці зв'язку, що вказує на потенційні несправності або збої.

2. Підходи до відновлення після несправностей

– Резервування та реплікація: Використовуйте методи резервування та реплікації для реплікації критично важливих даних або послуг на кількох вузлах або в центрах обробки даних. У разі збою резервні копії можуть бути активовані для підтримки доступності послуг.

– Відкат та контрольні точки: Механізми відкату та методи контрольних точок дозволяють системі повернутися до попереднього відомого справного стану до виникнення помилки. Транзакції або процеси можна відкатити до узгодженого стану, а контрольні точки можна використовувати для відновлення обробки з відомої точки.

– Реконфігурація та самовідновлення: механізми самовідновлення автоматично переконфігурують систему, перерозподіляють робоче навантаження або замінюють компоненти, що вийшли з ладу, для відновлення функціональності системи. Для автоматизації процесів відновлення використовуються такі методи, як автоматичне масштабування, динамічна реконфігурація та автоматичне перемикання на резервний ПК.

Безпека та контроль доступу в розподілених системах

Заходи безпеки, включаючи використання шифрування, автентифікації та авторизації, значною мірою допомагають гарантувати безпеку розподіленої системи від кібератак та несанкціонованого доступу. Заходи контролю доступу – це засоби забезпечення дотримання політики щодо заборони доступу до деяких конфіденційних ресурсів і даних. Це гарантує конфіденційність даних та дотримання чинних правил.

Масштабування та балансування навантаження в розподілених системах

Масштабування означає або динамічний приплив, або зменшення ресурсів, що збігається зі збільшенням або зменшенням використання цих ресурсів.

– Балансування навантаження служить для рівномірного розподілу вхідних запитів до кожного вузла розподіленої системи, що сприяє ефективному використанню ресурсів та зменшує перевантаження, тим самим забезпечуючи масштабованість, високу доступність та продуктивність у розподілених системах.

– Такі методи, як горизонтальне та вертикальне масштабування, а також автоматичне масштабування, є одними зі способів, за допомогою яких розподілені системи

масштабуються. Ці методи використовуються для розподілу робочого навантаження на основі доступності ресурсів та моделей попиту.

Ключові характеристики розподілених систем

1. Масштабованість: Розподілені системи можуть масштабуватися горизонтально (додаючи більше машин), а не вертикально (збільшуючи потужність однієї машини), що робить їх ідеальними для застосувань, які потребують швидкого зростання.

2. Паралелізм: Багато розподілених систем обробляють тисячі або навіть мільйони запитів одночасно. Це призводить до потреби в ефективних протоколах зв'язку та обробці спільних ресурсів.

3. Відмовостійкість: оскільки розподілені системи працюють на кількох машинах, вони розроблені таким чином, щоб переносити збої окремих вузлів, не впливаючи на доступність усієї системи.

4. Гетерогенність: Розподілені системи можуть складатися з різних типів машин, операційних систем або мереж, що означає, що вони повинні безперешкодно обробляти цю різноманітність.

5. Прозорість: Розподілені системи намагаються приховати складність кількох машин від кінцевого користувача, забезпечуючи єдиний інтерфейс, ніби система працює на одному комп'ютері.

Типи розподілених систем

1. Клієнт-серверні системи

У цій моделі сервер надає послуги, а клієнти споживають ці послуги, надсилаючи запити до сервера. Прикладами є веб-сервери та сервери баз даних. Приклад: Браузер (клієнт) надсилає HTTP-запит на веб-сервер, а сервер відповідає запитуваними даними (веб-сторінкою, відповіддю API тощо).

2. Однорангові системи

На відміну від клієнт-серверних систем, однорангові системи не мають централізованого сервера. Натомість кожен вузол (або одноранговий вузол) може виступати як клієнтом, так і сервером. Приклад: Системи обміну файлами, такі як BitTorrent, де кожен вузол завантажує та вивантажує файли з інших вузлів.

3. Кластерні обчислення

Кластер складається з групи комп'ютерів (часто званих вузлами), які працюють разом як єдина система для виконання великомасштабних обчислень. Вузли в кластері зазвичай розташовані в одному фізичному місці та з'єднані через високошвидкісну локальну мережу. Приклад: кластери Надоор, що використовуються для обробки великих даних.

4. Грід-обчислення

Грід-обчислення схожі на кластерні обчислення, але в більшому масштабі. Вузли в грід-обчисленнях часто географічно розподілені по різних місцях і з'єднані через Інтернет. Приклад: SETI@home, проект з мережових обчислень, який здійснює пошук позаземного розуму шляхом аналізу радіосигналів з космосу.

5. Хмарні обчислення

У хмарних обчисленнях ресурси (обчислювальні, сховища, мережеві) надаються як послуга через Інтернет. Хмарні системи – це розподілені системи, що забезпечують гнучкість, масштабованість та моделі ціноутворення «оплата за використання». Приклад: Amazon Web Services (AWS), Microsoft Azure та Google Cloud.

Ключові проблеми розподілених систем

1. Затримка

Коли вузли в розподіленій системі розташовані в різних географічних місцях, мережеві затримки (латентність) стають серйозною проблемою. Латентність впливає на швидкість зв'язку між вузлами, що може вплинути на продуктивність.

2. Послідовність

Узгодженість означає, що всі вузли мають однаковий вигляд даних у будь-який момент часу. У розподілених системах підтримка узгодженості може бути складною, особливо коли вузли реплікуються в різних регіонах.

— Теорема CAP: Теорема CAP стверджує, що розподілена система не може одночасно забезпечити всі три наступні гарантії:

— Узгодженість: кожне зчитування отримує останню записану інформацію або помилку.

— Доступність: На кожен запит надходить відповідь без гарантії, що вона містить найновіший запис.

— Допуск розділу: Система продовжує працювати, незважаючи на випадкову втрату повідомлень або збій частини системи.

— Розподіленим системам часто доводиться йти на компроміси між цими властивостями.

3. Відмовостійкість

Вузли в розподіленій системі можуть вийти з ладу з різних причин (збій обладнання, проблеми з мережею тощо). Система повинна мати можливість виявляти такі збої та відновлюватися після них без втрати даних або послуг.

4. Безпека

Розподілені системи стикаються з проблемами безпеки, оскільки дані передаються через мережі, які можуть бути вразливими до таких атак, як перехоплення даних, атаки типу «людина посередині» або несанкціонований доступ.

5. Координація та синхронізація

У розподілених системах координація між вузлами є критично важливою. Вузлам часто потрібно узгоджувати стан системи, обробляти одночасні операції та синхронізувати спільні ресурси.

Проектування розподіленої системи

Під час проектування розподіленої системи слід дотримуватися певних принципів та найкращих практик:

1. Реплікація: Для покращення відмовостійкості та доступності дані та послуги слід реплікувати на кількох вузлах.

2. Балансування навантаження: балансувальник навантаження повинен розподіляти вхідні запити між кількома вузлами, щоб запобігти перевантаженню будь-якого вузла.

3. Шардінг: У великих системах дані можна розділити на менші частини (шарди), які розподіляються по різних вузлах. Це покращує продуктивність, дозволяючи паралельну обробку.

4. Кешування: Дані, до яких часто звертаються, слід кешувати, щоб зменшити затримку та покращити продуктивність системи.

5. Моніторинг та спостережуваність: Впровадження надійних інструментів моніторингу забезпечує справність системи та допомагає виявляти збої на ранній стадії.

Розподілені системи є основою сучасних застосунків, що дозволяє їм масштабуватися, обробляти збої та задовольняти потреби мільйонів користувачів. Вони стали важливими для підприємств, яким потрібна висока доступність, відмовостійкість та масштабованість. Однак проектування та управління розподіленими системами пов'язане з власним набором проблем, таких як затримка, узгодженість та відмовостійкість.

Як інженери-програмісти, розуміння принципів та проблем розподілених систем може значно покращити вашу здатність проектувати надійні, масштабовані та ефективні системи. Незалежно від того, чи створюєте ви мікросервіси, хмарні платформи чи великомасштабні конвеєри обробки даних, розподілені системи відіграватимуть вирішальну роль у вашій архітектурі.

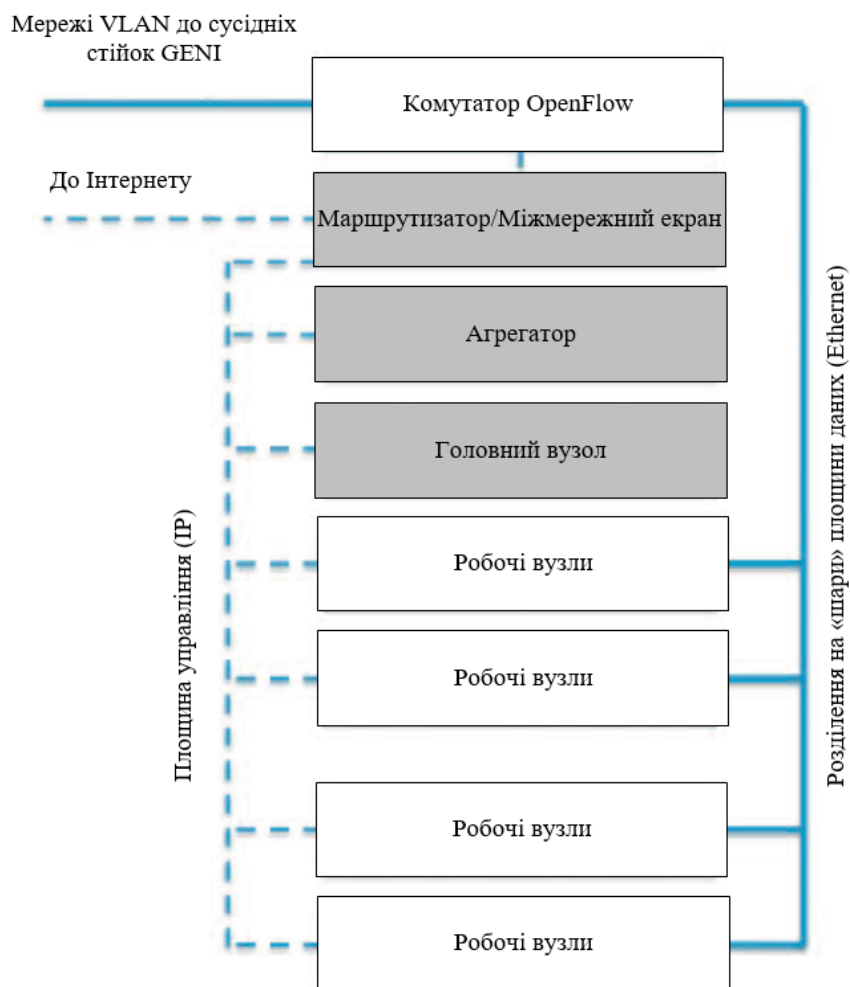


Рисунок 1 – Структурна схема системи

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів управління у розподілених Cloud-системах GENI. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем управління у розподілених Cloud-системах GENI.
- Досліджена система управління у розподілених Cloud-системах GENI.
- На основі отриманих результатів досліджень створена програмна реалізація системи управління у розподілених Cloud-системах GENI.

Розроблені алгоритми дозволяють успішно вирішувати завдання управління у розподілених Cloud-системах GENI. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». Advanced Information Systems, 2023, 7(2), pp. 49-56.
2. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchov, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». CEUR Workshop Proceedings, Volume 3530, 2023, pp. 256-265.
3. Smirnov, O., Odarchenko, R., Smirnova, T., Bondar, S., Volosheniuk, D. «Optimal Structure Construction of Private 5G Network for the Needs of Enterprises». Lecture Notes on Data Engineering and Communications Technologies, 2023, 178, pp. 208–223.

4. Аль-Мудхафар Акіл Абдулхуссейн М., Смірнова Т.В., Буравченко К.О., Смірнов О.А. «Метод оцінки та підвищення користувальницького досвіду абонентів в програмно-конфігурованих мережах на основі використання машинного навчання». Сучасні інформаційні системи, 2023, том 7, № 2, С. 49-56.
5. Smirnova, T., Gnatyuk, S., Yudin, O., Sydorenko, V., Polozhentsev, A., «The Model for Calculating the Quantitative Criteria for Assessing the Security Level of Information and Telecommunication Systems». CEUR Workshop Proceedings Volume 3156, 2022, Pages 390-399.
6. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». Проблеми інформатизації та управління, № 2(70). 2022. С. 28-37.
7. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції ґешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 3(69). С. 93-98.
8. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції ґешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Вісник Хмельницького національного університету. Серія: «Технічні науки», № 2 (307). С. 46-52. 2022.
9. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції ґешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 1(67). С. 84-89.
10. Smirnova T., Gnatyuk S., Berdibayev R., Avkurova Zh., Iavich M. «Cloud-Based Cyber Incidents Response System and Software Tools». Communications in Computer and Information Science, 2021, vol 1486. Springer, Cham. pp 169-184.
11. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
12. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». Journal of theoretical and applied information technology Vol.98. No 21, 2020, P. 3334-3346.
13. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177.
14. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587.
15. Smirnov, O., Markovets, O. Vovk, N., Turchyn, Y., «Model of informational support for social network administrators' content creation». CEUR Workshop Proceedings Volume 2616, 2020, Pages 125-136.
16. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». CEUR Workshop Proceedings Volume 2616, 2020, Pages 366-379.
17. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645.
18. Smirnov O. Kuznetsov A., Zaichenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019; Odessa; Ukraine; 9-13 September 2019. P.22-28.
19. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.
20. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019 . P.517-522.
21. Smirnov, O., Odarchenko, R., Abakumova, A., Usik, P., Kundyzy, M., «QoE optimization technique for media delivery in 5G networks». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019. P.597-601.
22. Smirnov, O., Krasnobayev, V., Yanko, A., Kuznetsova, T. «Methods of nulling numbers in the system of residual classes». CEUR Workshop Proceedings, Vol 2588, P. 90-106, 2019.
23. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Averchev, A., Pastukhov, M., Kuznetsova, K., «Formation of Pseudorandom Sequences with Special Correlation Properties», 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT -2019/ Lviv, Ukraine, 2-6 July, 2019, P. 395-399.

24. Smirnov, O., Kuznetsov, A., Kiian, A., Zamula, A., Rudenko, S., Hryhorenko, V., «Variance Analysis of Networks Traffic for Intrusion Detection in Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 353-358.
25. Smirnov, O., Kuznetsov, A., Kavun, S., Babenko, B., Nakisko, O., Kuznetsova, K., «Malware Correlation Monitoring in Computer Networks of Promising Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 347-352.
26. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Pastukhov, M., Kuznetsova, K., Prokopovych-Tkachenko, D., «Discrete Signals with Special Correlation Properties», CEUR Workshop Proceedings Volume 2353, CEUR Workshop Proceedings 2019, Pages 618-629.
27. Smirnov A.A., Kuznetsov A.A., Danilenko D.A., Berezovsky A., «The statistical analysis of a network traffic for the intrusion detection and prevention systems», Telecommunications and Radio Engineering. – Volume 74, Issue 1. – Begel House Inc. – 2015. – P. 61-78.
28. Смірнов О.А., Смірнова Т.В., Буравченко К.О., Кравченко С.С., Горбов В.О., «Хмарна система підтримки прийняття рішень технологічного процесу відновлення поверхонь конструкцій і деталей машин». Сучасні інформаційні системи. 2021. Т. 5, № 4. С. 79-95
29. Смірнов О.А., Усік П.С., Миронець І.В., Буравченко К.О., Якименко Н.М. «Метод підвищення ефективності розподіленої обробки даних у комп'ютерних системах операторів стільникового зв'язку» Вісник Черкаського державного технологічного університету. Технічні науки. №4. С. 103-110. 2020.
30. О.А.Смірнов, Т.В.Смірнова, Л.І. Поліщук, К.О. Буравченко, А.О.Макевнін, «Дослідження хмарних технологій як сервісів», Кібербезпека: освіта, наука, техніка. № 3(7). С. 43-62. 2020.
31. Смірнов О.А., Коноплицька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Поліщук Л.І. Інформаційна безпека в комп'ютерних мережах. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2020. – 294 с.
32. О.А. Смірнов, П.С. Усік, «дослідження перспектив використання технологічних рішень в мережах 5g» у Кібербезпека та інформаційні технології: монографія. – Х. : ТОВ «ДІСА ПЛЮС», 2020.С. 122-135.
33. Смірнов О.А., Дреєва Г.М., Дреєв О.М., Смірнова Т.В. «Фрактальний аналіз генератора самоподібного трафіку на основі ланцюга Маркова». Центральнотрапійський науковий вісник. Технічні науки. № 2(33). с. 161-172, 2019.

УДК 004

Б.Марченко, магістр гр. КІ-24М,

Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПРИ ДОСТУПІ ДО WEB-СЕРВЕРУ ЗА РАХУНОК ОПОРТУНІСТИЧНОГО ШИФРУВАННЯ

У статті розроблено програмне забезпечення, яке призначено для системи забезпечення безпеки при доступі до WEB-серверу за рахунок опортуністичного шифрування. Метою розробки є дослідження та принципи побудови системи забезпечення безпеки при доступі до WEB-серверу за рахунок опортуністичного шифрування. Об'єктом дослідження є процес забезпечення безпеки при доступі до WEB-серверу за рахунок опортуністичного шифрування. Предметом дослідження є методи забезпечення безпеки при доступі до WEB-серверу за рахунок опортуністичного шифрування. Методи дослідження базуються на методах теорії захисту інформації та теорії побудови комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи забезпечення безпеки при доступі до WEB-серверу за рахунок опортуністичного шифрування. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

забезпечення безпеки, доступ, WEB-сервер, опортуністичне шифрування

Постановка проблеми. Опортуністичний TLS схожий на згоду зустрітися з кимось для приватної розмови в людному громадському місці. Якщо є вільний куточок для приватної розмови, ви можете безпечно провести делікатну розмову; однак, якщо тихе місце вільне, ви будете вести розмову відкрито та ризикуватимете, що вас можуть підслухати. Спілкування відбувається, але його конфіденційність не гарантується. У світі електронної пошти, коли один поштовий сервер (наприклад, сервер вашої компанії) надсилає повідомлення на інший сервер (наприклад, сервер Gmail одержувача), він намагається встановити з'єднання, зашифроване за допомогою TLS. Зазвичай це робиться за допомогою команди STARTTLS у протоколі SMTP. Якщо сервер-отримувач підтримує STARTTLS і узгодження пройшло успішно, вміст електронного листа шифрується під час передачі. Однак, якщо сервер-отримувач не підтримує TLS або якщо проблема перешкоджає підтвердженню шифрування, електронний лист буде просто надіслано у вигляді звичайного тексту, тобто він не зашифрований і потенційно може бути прочитаний будь-ким, хто його перехопить.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи забезпечення безпеки при доступі до WEB-серверу за рахунок опортуністичного шифрування.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи забезпечення безпеки при доступі до WEB-серверу за рахунок опортуністичного шифрування.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем забезпечення безпеки при доступі до WEB-серверу за рахунок опортуністичного шифрування.
- Дослідження системи забезпечення безпеки при доступі до WEB-серверу за рахунок опортуністичного шифрування.

– Програмна реалізація системи забезпечення безпеки при доступі до WEB-серверу за рахунок опортуністичного шифрування.

Об'єктом дослідження є процес забезпечення безпеки при доступі до WEB-серверу за рахунок опортуністичного шифрування.

Предметом дослідження є методи забезпечення безпеки при доступі до WEB-серверу за рахунок опортуністичного шифрування.

Методи дослідження базуються на методах теорії захисту інформації та теорії побудови комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Примусовий TLS – це набагато суворіший підхід до шифрування. Примусовий TLS наполягає на тому, щоб ваша розмова проходила в приватному місці; якщо немає вільного місця, розмова просто не відбудеться.

Примусовий TLS (також відомий як «Суворий TLS» або «Обов'язковий TLS») вимагає від сервера електронної пошти зашифрованого з'єднання із сервером-отримувачем. Якщо рукописання TLS не вдається або якщо сервер-отримувач взагалі не підтримує TLS, електронний лист не буде доставлено. З'єднання просто розривається, і відправник зазвичай отримує повідомлення про повернення, що вказує на помилку доставки. Це гарантує, що електронний лист ніколи не буде передано у вигляді звичайного тексту.

Примусовий TLS часто передбачає попередньо налаштовані політики, які іноді називають «політиками TLS» або «конекторами» в системах електронної пошти, де ви явно вказуєте, що зв'язок із певними доменами має використовувати TLS. Це поширена функція в таких службах, як Opportunistic TLS у конфігураціях Office 365, під час налаштування суворих правил потоку пошти.

Переваги та ризики примусового TLS

Переваги:

- Максимальна безпека: Гарантує, що конфіденційна інформація завжди шифрується під час передачі, усуваючи ризик її незашифрованої передачі.
- Запобігає атакам зниження версії: Зловмисник не може змусити з'єднання стати розшифрованим.
- Необхідно для дотримання вимог: Вирішально важливо для виконання суворих нормативних вимог у різних галузях, таких як HIPAA та GDPR.

Ризики:

- Можливі збої доставки: якщо сервер одержувача не підтримує потрібну версію TLS або має проблеми з конфігурацією, електронний лист не буде доставлено.
- Накладні витрати на конфігурацію: Вимагає ретельного налаштування та постійного управління, щоб забезпечити підтримку та налаштування примусового TLS усіма цільовими доменами.

Випадки використання примусового TLS:

- Охорона здоров'я (комунікації, що відповідають HIPAA): Абсолютно необхідна для передачі захищеної медичної інформації (PHI) відповідно до таких правил, як HIPAA, які вимагають безпеки даних пацієнтів.
- Фінансові установи: використовуються для безпечного зв'язку, що включає конфіденційні фінансові дані, реквізити рахунків та транзакції, щоб відповідати стандартам відповідності, таким як PCI DSS.
- Урядові установи: Для обміну секретною або конфіденційною урядовою інформацією, що вимагає суворої конфіденційності.
- Внутрішня корпоративна електронна пошта: Багато організацій застосовують примусове використання TLS між власними внутрішніми поштовими серверами або з довіреними партнерами, щоб забезпечити безпеку всіх внутрішніх комунікацій.
- Висококонфіденційна комунікація B2B: обмін конфіденційною діловою інформацією між двома компаніями, які мають взаємну угоду про забезпечення максимальної безпеки.

Приклади примусового TLS:

– Лікарня надсилає записи пацієнтів до страхової компанії, де обидві сторони домовилися використовувати примусове TLS для всіх комунікацій між своїми доменами. Якщо TLS-з'єднання не вдається встановити, запис не надсилається.

– Система електронної пошти банку часто використовує примусовий TLS під час надсилання виписок з рахунку або конфіденційних сповіщень, гарантуючи шифрування цих листів під час передачі до вашого постачальника послуг електронної пошти (за умови, що ваш постачальник також підтримує необхідний TLS).

– Компанії, що використовують Microsoft 365, можуть налаштувати примусові правила TLS (часто їх називають «конекторами»), щоб електронні листи, надіслані до певних доменів партнерів або з них, повинні використовувати TLS, інакше вони відхиляються. Це допомагає забезпечити відповідність вимогам та надійний захист електронної пошти.

За замовчуванням Microsoft 365 (M365) не використовує примусовий TLS. Натомість він використовує опортуністичний TLS, який намагається зашифрувати електронну пошту під час передачі, якщо сервер-отримувач підтримує його. Якщо TLS недоступний, повідомлення надсилаються незашифрованими.

Однак, M365 можна налаштувати на використання примусового TLS через конектори або правила потоку пошти. За належного налаштування примусовий TLS у M365 гарантує, що електронна пошта надсилатиметься лише за умови встановлення безпечного з'єднання TLS, інакше доставка не вдається. Коротше кажучи, примусовий TLS – це налаштовуваний параметр, а не поведінка за замовчуванням.

Gmail не використовує примусовий TLS за замовчуванням. Gmail покладається на опортуністичний TLS, тобто намагатиметься зашифрувати електронну пошту під час передачі, якщо сервер-отримувач підтримує TLS; якщо TLS недоступний, повідомлення доставляється незашифрованим.

Хоча Google підтримує примусове використання TLS для певних доменів за допомогою розширених налаштувань Gmail (переважно в Google Workspace), примусове використання TLS не є поведінкою за замовчуванням і має бути налаштоване явно. Крім того, коли TLS не підтримується, а примусове використання TLS налаштоване, альтернативою є те, що повідомлення не надсилатимуться, і цю проблему може вирішити безпечне рішення для електронної пошти Zivver.

Як опортуністичний TLS, так і примусовий TLS відіграють певну роль у безпеці електронної пошти. Однак для організацій, які мають справу з конфіденційними даними та дотримуються вимог до дотримання вимог, примусовий TLS є явним переможцем, оскільки він гарантує шифрування під час передачі. Хоча опортуністичний TLS пропонує підхід «найкращих зусиль», він не усуває ризик незашифрованої передачі, якщо умови не виконуються; у традиційних рішеннях електронної пошти, якщо сервер одержувача не підтримує TLS, ваше повідомлення не може бути надіслано.

Для справді надійної безпеки електронної пошти, яка виходить за рамки базових можливостей TLS, спеціалізоване рішення для шифрування електронної пошти, розширює поштові клієнти, такі як Microsoft 365 та Gmail, за допомогою розширених протоколів шифрування, гарантуючи захист конфіденційних листів та їх можливість читання на безпечному веб-порталі, захищеному потужною двофакторною автентифікацією (2FA). Окрім розширеного шифрування, додатково захищає конфіденційні листи за допомогою зручних функцій запобігання втраті даних, допомагаючи запобігти людським помилкам – усі ці важливі елементи захисту вашої інформації.

Опортуністичний TLS – це стандартна конфігурація безпеки транспортування пошти на всіх агентах передачі повідомлень (MTA) та поштових серверах. Сервери відправника та одержувача пошти домовлятимуться один з одним про те, яке шифрування вони можуть використовувати. Буде використано найбезпечніше з'єднання, яке можуть підтримувати обидві сторони. Це означає, що пошту можна надсилати взагалі без шифрування. Але ви можете це змінити.

Дивно, що ми посилюємо безпеку наших операційних систем і хвилюємося про те, як захищений Microsoft Teams. Іноді ми також звинувачуємо у будь-якому витокі даних прислів'я-стажера (що, до речі, неправильно). Але коли справа доходить до пошти, організації досить погано налаштовують належну автентифікацію пошти. Це все про SPF, DKIM, DMARC, SRS та ARC, я продовжую працювати над своїми соціальними мережами. Особливо є простір для вдосконалення, коли домен організації використовується в сторонніх поштових продуктах.

Шифрування повідомлень

Звичайно, ви можете підписати або зашифрувати свою електронну пошту за допомогою S/MIME, PGP або Microsoft Purview Mail Encryption. Це означає, що окреме поштове повідомлення було зашифровано, незалежно від того, як воно передається. Але, на мою скромну думку, це не дуже зручно для користувача. Вам потрібно попереднє налаштування, таке як отримання сертифікатів та обмін ключами. Шифрування повідомлень забезпечує безпеку, але часто конфліктує з процесами відповідності (наприклад, збереження/архівування). Purview забезпечує захист лише на стороні відправника (для нових листів).

Так, існують шляхові рішення, але вони часто суттєво збільшують вартість (ліцензії на робоче місце, обслуговування тощо). Видима та прихована вартість електронної пошти зростатиме з кожним додаванням. Кілька причин, чому пошта є привабливим рішенням, – це високий рівень впровадження та сумісності. Вона також відносно проста у використанні та має відносно низьку вартість з майже миттєвою доставкою. (Справедливості заради, економічність пошти – це обґрунтоване припущення. Вона достатньо хороша та була першою, ймовірно, також є вагомими причинами).

Шифрування транспорту

Не зрозумійте мене неправильно. Шифрування повідомлень, безумовно, має свої варіанти використання. Мені здається, що воно іноді заважає думати про інші рішення чи практики. Наприклад, чи варто мені взагалі надсилати цю цінну інформацію, якщо вона потребуватиме шифрування повідомлень? Чи справді пошта є найкращим способом безпечного спілкування?

Хоча я починав із шифрування повідомлень, транспортне шифрування насправді є основною та неявною формою шифрування. Це означає, що наразі майже завжди використовується транспортне шифрування завдяки опортуністичному TLS. У більшості перевірених мною орендарів діапазон «Без TLS» знаходиться в межах 1%. І цей 1% «імовірність» може бути причиною для організації використовувати шифрування повідомлень, зменшуючи потенційні прогалини за допомогою транспортного шифрування та запобігаючи перехопленню повідомлень.

Як варіант, організації-партнери використовують обов'язкові TLS -з'єднання. Вони налаштовуються для забезпечення наявності шифрування транспорту перед надсиленням будь-якої пошти. Часто вони також мають форму автентифікації за IP-адресою або сертифікатом. Проблема, яку я бачу, полягає в тому, що вони вимагають спеціальної конфігурації та налаштування для кожного поштового домену, що збільшує витрати, а іноді вимагає контакту з вузлом для повідомлення правильної кінцевої точки SMTP. MTA-STS є покращенням, оскільки він певною мірою запобігає атакам Advisory-in-the-Middle, оскільки публікує кінцеву точку MX у файлі конфігурації на захищеному веб-сайті з тим самим доменом організації. Найкращим рішенням для безпеки транспорту на сьогодні є DANE. Він забезпечує навіть більший рівень безпеки, ніж обов'язковий TLS, оскільки значною мірою залежить від DNSSEC. На жаль, не всі організації можуть використовувати DNSSEC. (Azure DNS мав його в попередньому перегляді, але цього ярлика більше немає?). Особливо, коли Exchange Online підтримуватиме обов'язковий DANE пізніше у 2025 році. Це примусово використовуватиме DANE на основі клієнта або домену та не дозволить переходу на MTA-STS або опортуністичний TLS. Немає потреби в обов'язковому TLS або навіть маршрутизації через захищені приватні мережі.

Але і MTA-STLS, і DANE страждають від тих самих проблем, що й інші акроніми, а саме від їхнього впровадження. Іноді це пов'язано з технічними причинами, але частіше з усвідомленням або розумінням їхніх переваг порівняно з тим, що використовується за замовчуванням, тобто опортуністичним TLS.

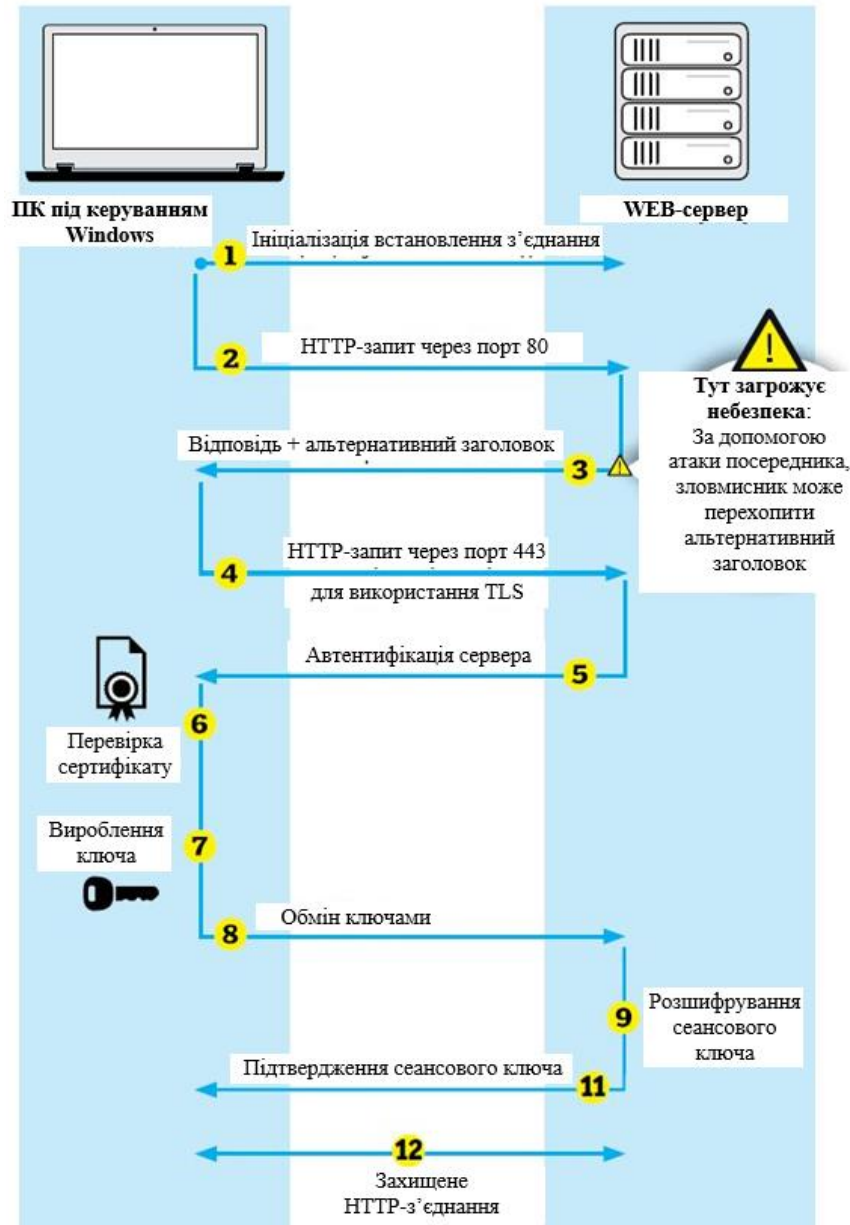


Рисунок 1 – Структурна схема системи

Примусове використання TLS в Exchange Online

Щоб примусово використовувати TLS для підключення SMTP за замовчуванням, потрібно налаштувати як вхідний, так і вихідний конектор. Базові однорядкові інструкції Exchange Online PowerShell у найпростішій формі (без виконання перевірки):

```
New-OutboundConnector -ConnectorType Partner -RecipientDomains * -TlsSettings EncryptionOnly -UseMXRecord $True -Name "Outbound Forced TLS"
```

```
New-InboundConnector -ConnectorType Partner -SenderDomains * -TlsSettings EncryptionOnly
```

Є три основні висновки: тип конектора – Партнер. Ви налаштовуєте домени одержувача та відправника за допомогою символу підстановки *. І останній етап – лише шифрування, а не перевірка сертифіката. Більш специфічні конектори (наприклад, ті, що мають IP-адреси та/або повні доменні імена) замінюють ці конектори. Ви можете мати певні

конектори, які не потребують TLS, якщо вам це потрібно для прямого надсилання або ретрансляції SMTP.

Якщо ваша організація надає пріоритет отриманню пошти перед шифруванням транспортування, ви можете розглянути можливість початку роботи з вихідного конектора. У поєднанні з оповіщенням про чергу пошти або використанням вбудованих звітів про повідомлення ви можете відстежувати ситуацію та діяти відповідно.

Більш цілісний підхід до безпеки (пошти)

Організації повинні регулярно перевіряти весь свій підхід до обміну інформацією з іншими сторонами. Пошта – це просто, і майже завжди вона вже доступна. Але за останні кілька років з'явилися інші продукти або їх удосконалили до такого стану, що це може бути найкращим рішенням для цієї роботи. Вона також може бути дешевшою, простішою в управлінні та навіть безпечнішою.

Я б зосередився на транспортному шифруванні, такому як примусове використання TLS та впровадження як MTA-STS, так і DANE. Особливо (обов'язкове) DANE є значним покращенням і може бути причиною для переоцінки використання шифрування повідомлень у певних сценаріях.

Опportunістичне шифрування

Опportunістичне шифрування починається з незашифрованого запиту. Шифрування встановлюється тільки тоді, коли сервер відправляє альтернативний заголовок із пропозицією зашифрувати канал.

Робота системи проілюстрована структурною схемою, відображеної на рисунку 1.

Тут загрожує небезпека: за допомогою атаки посередника зломисник може перехопити альтернативний заголовок.

Порт 80 – WWW-сервер. Показує присутність http-сервера в системі. За допомогою WWW-сервісу можна довідатися назву й версію програмного забезпечення встановленого на WEB-сервері.

Порт 443 – Протокол HTTPS (SSL). Варіант безпечного протоколу HTTP.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів забезпечення безпеки при доступі до WEB-серверу за рахунок опportunістичного шифрування.

Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем забезпечення безпеки при доступі до WEB-серверу за рахунок опportunістичного шифрування.
- Досліджена система забезпечення безпеки при доступі до WEB-серверу за рахунок опportunістичного шифрування.
- На основі отриманих результатів досліджень створена програмна реалізація системи забезпечення безпеки при доступі до WEB-серверу за рахунок опportunістичного шифрування. Розроблені алгоритми дозволяють успішно вирішувати завдання забезпечення безпеки при доступі до WEB-серверу за рахунок опportunістичного шифрування. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Усік, П.С., Смірнова, Т.В., Буравченко, К.О., Смірнов, О.А., Улічев, О.С., Смірнов, С.А. «Дослідження технологій забезпечення кібербезпеки банківських систем з використанням штучного інтелекту». Кібербезпека: освіта, наука, техніка. 2025. Том 1 № 29. С.704–716, 2025.
2. Kuznetsov, O., Frontoni, E., Kuznetsova, K., Arnesano, M., Smirnov, O. «A secure biometric authentication architecture for blockchain-driven cyber-physical systems». Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications, 2025, pp. 193–224.
3. Kuznetsov, O., Atzeni, G., Arnesano, M., Randieri, C., Smirnov, O. «Secure IoT-based smart wheelchair system: From implementation to security enhancement strategy». Security and Privacy of Cyber Physical Systems

- Emerging Trends Technologies and Applications, 2025, pp. 225–257.
4. Kuznetsov, O., Smirnov, O., Kuznetsova, T., Shaikhanova, A., Svatowsky, I. «Privacy-utility trade-offs in IoT networks: A comparative analysis of differential privacy mechanisms for sensor data aggregation». Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications, 2025, pp. 589–622.
 5. Kuznetsov, O., Poluyanenko, N., Smirnov, O., Kozhakhmetova, D. «Optimized Simulated Annealing for Efficient Generation of Highly Nonlinear S-Boxes». Advancements in Cybersecurity Next Generation Systems and Applications, 2025. 146-174
 6. Kuznetsov, O., Poluyanenko, N., Smirnov, O., Bekeshova, G. «Enhanced Cryptographic Security through Advanced S-Box Optimization: A Hybrid Heuristic Approach». Advancements in Cybersecurity Next Generation Systems and Applications, 2025. pp. 56-78.
 7. Kuznetsov, O., Poluyanenko, N., Smirnov, O., Abduraimova, B «Enhancing Cryptographic Strength: A Novel Approach to S-Box Generation Using Modified Simulated Annealing». Advancements in Cybersecurity Next Generation Systems and Applications, 2025. pp. 79-116.
 8. Kuznetsov, O., Derevianko, Y., Frontoni, E., Arnesano, M., Smirnov, O. «Factorial Representation of S-Boxes: A Novel Approach to Cryptographic Analysis and Optimization». Advancements in Cybersecurity Next Generation Systems and Applications, 2025. pp. 117-145.
 9. Kuznetsov, O., Poluyanenko, N., Smirnov, O., Shaikhanova, A., Khruskov, B. «Innovative Cost Functions for Optimizing Cryptographic S-Box Generation». Advancements in Cybersecurity Next Generation Systems and Applications, 2025. pp. 29-55.
 10. Kuznetsov, O., Smirnov, O., Akhmetov, B., Alimseitova, Z., Imoize, A.L. «Deep Learning Frontiers in Copy-Move Forgery Detection: Advances, Challenges, and Future Directions». Advancements in Cybersecurity Next Generation Systems and Applications, 2025. 202-229.
 11. Lakhno, V., Malyukov, V., Smirnov, O., Bebesko, B., Chubaievskiy, V., Zhumadilova, M., Malyukova, I., Smirnov, S. «Multifactorial Model for Targeted Attacks Counteracting Within the Framework of a Multi-Step Quality Game with Fuzzy Information». 8th International Symposium on Intelligent Informatics, ISI 2023, 2025. vol 389. pp 377-389. Springer, Singapore.
 12. Kuznetsov, O., Smirnov, O., Mormul, M., Kotukh, Y., Zvieriev, V. «Comparative Research on Cryptocurrency Efficiency: An Objective Analysis of Key Metrics». International Journal of Computing 23(4), 2024. pp. 563-573.
 13. Kuznetsov O., Frontoni E., Kuznetsova K., Smirnov O., Kostenko V. «Blockchain applications in metaverse environments: new horizons». Advanced Metaverse Wireless Communication Systems. pp. 255-293. 2024.
 14. Kuznetsov, O., Frontoni, E., Chevardin, V., Smirnov, O., Imoize, A.L. «Advancing metaverse security with cryptographic innovations». Advanced Metaverse Wireless Communication Systems. pp 351-386. 2024.
 15. Kuznetsov O., Frontoni E., Kuznetsova Y., Smirnov O., Moskovchenko I. «Trust-Based Security Architecture for Edge Computing: A Simulation Study of Dynamic Trust Evolution and Attack Detection». CEUR Workshop Proceedings, 2024, 3909, pp. 227–241.
 16. Kuznetsov, O., Frontoni, E., Kryvinska, N., Chevardin, V., Smirnov, O. «Wireless Network Encryption Stream Ciphers, Computational Modeling, and Security Analysis». Computational Modeling and Simulation of Advanced Wireless Communication Systems, 2024, pp. 379–402.
 17. Kuznetsov, O., Frontoni, E., Kryvinska, N., Smirnov, O., Imoize, G.L. «Computational Modeling of Enhanced Spread Spectrum Codes for Asynchronous Wireless Communication». Computational Modeling and Simulation of Advanced Wireless Communication Systems, 2024, pp. 403–447.
 18. Ткаченко, О., Ільєнко, А., Улічев, О., Мелешко, Є., Смірнов, О. «Правові засади поширення інформаційних впливів в соціальних мережах». Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2024. № 2(26), С. 170–188.
 19. Смірнова Т.В., Коноплицька-Слободенюк О.К., Буравченко К.О., Смірнов С.А., Кравчук О.В., Козірова Н.Л., Смірнов О.А. «Дослідження технологій забезпечення кібербезпеки хмарних сервісів IaaS, PaaS та SaaS». Кібербезпека: освіта, наука, техніка. 2024. №4(24), С. 6-27.
 20. Вінтенко, Б., Миронець, І., Смірнов, О., Кравчук, О., Козірова, Н., Савеленко, Г., Коваленко, А. «Дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». Кібербезпека: освіта, наука, техніка. 2024. №3(23), С. 111-131.
 21. Kuznetsov, O., Frontoni, E., Kandiy, S., Smirnova, T., Prokopov, S., Bilanovych, A. «New Cost Function for S-boxes Generation by Simulated Annealing Algorithm». Lecture Notes on Data Engineering and Communications Technologies, 2023. vol 180. pp. 310-320. Springer, Cham.
 22. Kuznetsov, O., Frontoni, E., Kandiy, S., Smirnov, O., Ulianovska, Y., Kobylanska, O. «Heuristic Search for Nonlinear Substitutions for Cryptographic Applications». Lecture Notes on Data Engineering and Communications Technologies, 2023. vol 180. Springer, Cham. pp. 288-298.
 23. Kuznetsov, O., Kuznetsova, Y., Smirnov, O., Kostenko, O., Zvieriev, V. «Evaluating Hashing Algorithms in the Age of ASIC Resistance». CEUR Workshop Proceedings, 2023, 3628, pp. 93-105.
 24. Kuznetsov O., Frontoni E., Kuznetsova Ye., Smirnov O., Chevardin V. «Achieving Enhanced Security in Biometric Authentication: A Rigorous Analysis of Code-Based Fuzzy Extractor». CEUR Workshop Proceedings, Volume 3624, 2023, pp. 330-339.
 25. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchев, S. «Simulation of the cloud IoT-based

- monitoring system for critical infrastructures». CEUR Workshop Proceedings, Volume 3530, 2023, pp. 256-265.
26. Kuznetsov, O., Kandiy, S., Frontoni, E., Smirnov, O. «Trade-offs in Post-Quantum Cryptography: A Comparative Assessment of BIKE, HQC, and Classic McEliece». CEUR Workshop Proceedings, Volume 3504, 2023, pp. 1-11.
27. Смірнов О.А., Козлов Я.О., Смірнова Т.В. «Дослідження застосування SIEM-систем для забезпечення кібербезпеки та захисту інформації». II Міжнародна науково-практична Інтернет-конференція «Інновації та перспективні шляхи розвитку інформаційних технологій (ІПШРІТ-2023)» м.Черкаси 6 грудня 2023 року – Черкаси: ЧДТУ. – 2023. – С.251-252.
28. Козлов Я.О., Смірнова Т.В., Смірнов О.А. «Дослідження SIEM-систем для забезпечення кібербезпеки». VII міжнародна науково-практична конференція “Інформаційна безпека та комп’ютерні технології” до 30-ти річчя кафедри кібербезпеки та програмного забезпечення, м. Кропивницький. 1 листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 26.
29. Козлов Я.О., Козірова Н.Л., Смірнов О.А. «Дослідження структури та принципу роботи SIEM-системи». VII міжнародна науково-практична конференція “Інформаційна безпека та комп’ютерні технології” до 30-ти річчя кафедри кібербезпеки та програмного забезпечення, м. Кропивницький. 1 листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 59.
30. Вінтенко Б.Ю., Смірнов О.А., Коваленко О.В., Смірнов С.А., Коваленко А.С. «Дослідження нормативних документів та галузевих стандартів розробки програмного забезпечення комп’ютерних систем управління АЕС, важливих для безпеки». Системи управління, навігації та зв’язку, 2023, вип. 2(72), С. 170-178.
31. Смірнова Т.В., Гнатюк С.О., Бердибасв Р.Ш., Сидоренко В.М., Жигаревич О.К., «Система корелювання подій та управління інцидентами кібербезпеки на об’єктах критичної інфраструктури». Кібербезпека: освіта, наука, техніка, №3(19), 2023, С. 176-196.
32. Smirnov, O., Neskorodieva, T., Fedorov, E., Rudakov, K., Neskorodieva, A. «Method Detection Audit Data Anomalies on Basis Restricted Cauchy Machine» CEUR Workshop Proceedings, Volume 3187, 2022,

УДК 004

Ю.Молчанов, магістр гр. КІ-24Мз,

Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ SOFTWARE DEFINED STORAGE

У статті розроблено програмне забезпечення, яке призначено для системи Software Defined Storage. Метою розробки є дослідження та принципи побудови системи Software Defined Storage. Об'єктом дослідження є процес Software Defined Storage. Предметом дослідження є методи Software Defined Storage. Методи дослідження базуються на методах теорії побудови комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи Software Defined Storage. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

Software Defined Storage

Постановка проблеми. Дані не чекають на бюджетні цикли. Вони зростають саме тоді, коли ваша система зберігання вирішує нагадати вам, хто насправді володіє вашим часом безвідмовної роботи. NAS та SAN все ще мають своє застосування, але їх масштабування схоже на плату за захист постачальникам обладнання – дороге, негнучке та розраховане на вчорашні робочі навантаження.

У 2025 році, коли конвеєри штучного інтелекту, аналітичні завдання та дані користувачів множаться швидше, ніж ваші сповіщення моніторингу, вам потрібне сховище, яке гнучко адаптується до потреб користувачів. Саме тут на допомогу приходять програмно-визначені сховища (Software Defined Storage, SDS): жодних оновлень навантажувачів, жодної прив'язки до постачальника, лише програмний рівень, який дозволяє масштабуватися в горизонтальному напрямку.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи Software Defined Storage.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи Software Defined Storage.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем Software Defined Storage.
- Дослідження системи Software Defined Storage.
- Програмна реалізація системи Software Defined Storage.

Об'єктом дослідження є процес Software Defined Storage.

Предметом дослідження є методи Software Defined Storage.

Методи дослідження базуються на методах теорії побудови комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. По суті, SDS – це програмний рівень, який відокремлює фізичні ресурси зберігання від базових пристроїв зберігання даних. Замість того, щоб прив'язувати дані безпосередньо до власного обладнання, SDS використовує віртуалізацію сховища для створення гнучкої та економічно ефективної інфраструктури зберігання даних.

На відміну від традиційних систем зберігання даних, таких як NAS та SAN, де зміни ємності або продуктивності часто вимагають заміни всіх фізичних ресурсів зберігання, система SDS робить масштабування майже безперешкодним. Ви можете додавати більше

дисків, вузлів або навіть хмарну ємність без переписування програм або зміни робочих процесів. Однак віртуалізація має недоліки, тому деякі організації неохоче впроваджують технологію SDS.

Коротше кажучи, програмно-визначені рішення для зберігання даних дозволяють керувати складними операціями зберігання даних з єдиного інтерфейсу, підвищуючи гнучкість та знижуючи витрати. Хіба це не та перевага, яка робить SDS кращим підходом до зберігання даних у 2025 році?

Які переваги та недоліки сучасної системи SDS?

Впровадження програмно-визначених сховищ різко зросло з однієї причини: це вирішує проблеми, які не дають системним адміністраторам та DevOps спати вночі. Вигоди переважають головний біль, особливо якщо ви перестали платити данину завищеним постачальникам обладнання.

Ось що насправді дає вам SDS:

1. Гнучкість у виборі обладнання

За допомогою SDS ви можете запускати сховище даних на виділених серверах або пристроях, які легше оновити або замінити. Це зменшує залежність від масивів певних постачальників і робить фізичні ресурси сховища більш адаптивними.

2. Масштабованість у всіх напрямках

Завдяки віртуалізації сховища, SDS масштабується як вертикально (додаючи більше потужності до існуючих вузлів), так і горизонтально (додаючи більше вузлів або дисків), що робить керування ресурсами сховища приємним процесом.

3. Економічно ефективність

Оскільки SDS абстрагує програмний рівень від фізичних ресурсів зберігання, вам не потрібно інвестувати в дорогі традиційні рішення для зберігання даних. Натомість ви можете перепрофілювати стандартне обладнання та розширювати його лише за потреби.

4. Централізоване управління сховищами

Єдина панель інструментів на базі програмного забезпечення для керування та автоматизації дозволяє адміністраторам керувати реплікацією, резервним копіюванням та моніторингом.

5. Висока доступність та аварійне відновлення

SDS дозволяє реплікувати дані між кількома вузлами або навіть географічними регіонами. У разі збою обладнання або форс-мажору відновлення відбувається швидше та надійніше.

6. Підтримка багатотипного зберігання даних

Добре розроблене програмно-визначене рішення для зберігання даних може поєднувати блочне, файлове та об'єктне сховище в одній уніфікованій системі, оптимізуючи інфраструктуру зберігання даних у різних відділах.

7. Виділений сервер

Виділений хостинг для тих, кому потрібна більша потужність, контроль та справжня стабільність.

Але користувачі технології програмно-визначеного сховища вказують на деякі недоліки:

Оскільки SDS повністю залежить від програмного рівня, продуктивність та надійність залежать від правильного налаштування та моніторингу. Неправильна конфігурація або недостатній моніторинг призводять до погіршення продуктивності.

Розгортання та обслуговування системи SDS вимагає навчання з віртуалізації та автоматизації сховищ. Брак досвіду може уповільнити впровадження.

Абстрагуючи сховище від апаратного забезпечення, SDS вводить нові міркування безпеки. Неправильно налаштоване програмне забезпечення для керування та автоматизації або неконтрольовані пристрої зберігання даних можуть стати векторами атаки.

Як керувати та оптимізувати програмно-визначену систему зберігання даних?

Розгортання програмно-визначеного сховища даних – це не фінішна пряма, а саме початок справжньої роботи. Ставлення до нього як до рішення за принципом «налаштував і забув» – це найшвидший спосіб виявити, що ваш рівень сховища даних перетворився на найслабшу ланку вашої інфраструктури.

Перша проблема – це планування ємності сховища. Занадто висока оцінка – і ви витрачаєте бюджет на обладнання, яке простоює. Занадто низька оцінка – і ви будете боротися з вузькими місцями у найневідповідніший момент. Баланс досягається шляхом моніторингу реальних робочих навантажень, прогнозування зростання за допомогою чітких показників та масштабування навмисно, а не реактивно.

Програмне забезпечення для управління та автоматизації є основою SDS, але воно надійне настільки, наскільки надійне його налаштування. Панелі інструментів та сповіщення повинні зменшувати кількість людських помилок, а не замінювати оперативну обізнаність. Відстеження IOPS, затримки та пропускну здатності в режимі реального часу – це спосіб виявити проблеми, перш ніж вони переростуть у збої.

Стратегії резервного копіювання та відновлення також змінюються в рамках SDS. Знімки та реплікація між вузлами або регіонами значно спрощують відновлення після збоїв, але лише за умови дотримання та тестування політик. Занадто багато команд вважають, що реплікація відбувається тому, що вона була налаштована один раз; на практиці кластер без моніторингу може швидко вийти з синхронізації. Практики безпеки для захисту даних також повинні залишатися суворими.

Зрештою, **підтримка постачальників або спільноти** – це тиха, але критично важлива частина оптимізації SDS. Стеж, який сьогодні виглядає надійним, може стати крихким, якщо оновлення перестануть надходити або спільнота проекту втратить імпульс. Перевірка стану екосистеми так само важлива, як і перевірка стану власного кластера.

Програмно-визначене сховище зазвичай буває двох видів: конвергентна інфраструктура та гіперконвергентна інфраструктура.

Конвергентна інфраструктура (CI):

- Структура: Обчислення, мережа та сховище даних – це окремі апаратні блоки, об'єднані між собою спеціальною інтерфейсною структурою.
- Продуктивність: Висока пропускну здатність і передбачувана затримка – добре, якщо ваші робочі навантаження пов'язані з великим обсягом операцій вводу/виводу.
- Відповідність варіантам використання: застарілі програми, транзакційні бази даних або середовища, де спеціалізація обладнання все ще має значення.
- Компроміси: масштабування незграбне, залежність від постачальника залишається, а гнучкість обмежена.

Гіперконвергентна інфраструктура (HCI):

- Структура: Обчислення, мережа та сховище даних об'єднані в один рівень, керований програмним забезпеченням.
- Масштабованість: додавання вузлів, масштабування. Просто. Без модернізації навантажувача.
- Відповідність варіантам використання: хмарні стеки, оркестрація контейнерів, конвеєри з інтенсивним використанням DevOps та робочі навантаження штучного інтелекту/машинного навчання.
- Компроміси: значною мірою залежить від експертизи програмного забезпечення – неправильно налаштуйте його, і ви щойно підвищите свій кластер до аномалії класу Keter.

Що обрати у 2025 році?

- Оберіть неперервну інтеграцію (CI), якщо ви використовуєте застарілі системи або вам потрібні гарантії продуктивності без будь-яких пошкоджень.
- Оберіть HCI, якщо бажаєте використовувати його за замовчуванням для сучасних програмно-визначених середовищ зберігання даних. Якщо відповідність вимогам або

застарілі обмеження не змушують вас використовувати CI, HCI позбавить вас головного болю.

Коли варто використовувати програмно-визначену систему зберігання даних

Не кожній організації потрібне програмно-визначене сховище з першого дня. Перевірте ці випадки, щоб визначитися.

- SDS спрощує налаштування та керування віртуальними машинами, робочими столами та програмами в гібридних або багатохмарних системах.

- Якщо ви аналізуєте поведінку клієнтів, ринкові тенденції або бізнес-рушії, SDS забезпечує єдиний доступ до великих обсягів сховища даних. Його централізований програмний рівень робить аналітику швидшою та легшою для автоматизації.

- Реплікація на кількох пристроях зберігання даних та в різних регіонах забезпечує швидке відновлення під час збоїв, що робить SDS кращим вибором для організацій, де простої дорівнюють фінансовим втратам.

- Деякі підприємства використовують програмно-визначені рішення для зберігання даних на периферії для локальної обробки даних, зберігаючи при цьому синхронізацію з централізованим обладнанням для зберігання даних. Це забезпечує продуктивність та стійкість навіть у розподілених середовищах.

Як захистити програмно-визначену систему зберігання даних?

Безпека – це те, де SDS або витримує тиск, або стає дуже дорогим звітом про інциденти. Оскільки SDS переносить контроль на рівень програмного забезпечення, неправильна конфігурація не просто можлива – вона неминуча без дисципліни.

1. Обмежте права root/адміністратора до найменшої можливої групи. Кожна дія має бути зареєстрована та відстежена, а не закопана на сервері журналів, який ніхто не перевіряє до завершення збою.

2. Дані в стані спокою, під час передачі, між вузлами – шифруйте все. Будь-що менше – це відкрите запрошення до витоку даних. Базовий рівень: TLS для трафіку, AES для зберігання.

3. Автоматизуйте сканування на вразливості та не покладайтеся на електронні листи постачальників, щоб дізнатися про випадки зараження.

4. Перевіряйте кожен запит, ізолюйте робочі навантаження та сегментуйте ресурси сховища. Якщо один вузол скомпрометовано, радіус вибуху слід вимірювати в гігабайтах, а не петабайтах.

5. Відкритий код SDS забезпечує прозорість, але також робить вразливості публічними. Відстежуйте частоту виправлень спільноти.

Яка різниця між SDS, NAS та SAN для зберігання даних?

Коли люди оцінюють сховище даних, вони завжди використовують одні й ті ж три аббревіатури. Ось їх простий розбив:

Програмно-визначене сховище (SDS)

SDS абстрагує сховище на програмно-керований рівень на стандартному обладнанні. Підтримує блоки, файли та об'єкти в одній системі.

- Сильні сторони: Висока масштабованість, незалежність від апаратного забезпечення, автоматизація. Ідеально підходить для гібридної хмари, конвеєрів штучного інтелекту/машинного навчання або робочих процесів DevOps.

- Слабкі сторони: Складніший у розгортанні, вимагає фактичного досвіду та додає поверхню для атаки у разі неправильного налаштування.

- Перевірка реальності: якщо ви хочете гнучкості та втомилися від прив'язки до постачальника, то саме в цьому напрямку рухається галузь – це не «новітній розвиток», це стандартний процес.

Мережеве сховище даних (NAS)

Мережеве сховище даних (NAS) – це архітектура сховища даних на основі файлів, яка дозволяє користувачам отримувати доступ до даних через мережу, зазвичай за допомогою протоколів NFS або SMB.

- Сильні сторони: Просто, дешево, працює одразу після розпакування.
- Слабкі сторони: залежність від одного обладнання для зберігання даних, незграбне масштабування та обмежена продуктивність.
- Перевірка реальності: Чудово підходить для невеликої команди або лабораторного середовища. Завантажте його на виробниче навантаження, і ви зрозумієте, чому системні адміністратори ненавидять фразу «просто поставте його на NAS».

Мережа зберігання даних (SAN)

SAN, або мережа зберігання даних, – це блочна архітектура сховища, яка з'єднує сервери зі сховищем через виділену мережу за допомогою протоколів Fibre Channel або iSCSI.

- Сильні сторони: Низька затримка, висока пропускна здатність, надійна робота з критично важливими для продуктивності корпоративними робочими навантаженнями.
- Слабкі сторони: Власницька розробка, дорога, масштабування – це джерело доходу постачальника, а не ваш вибір.
- Перевірка реальності: SAN – це «безпечний варіант», який досі просувають фінансові та традиційні IT-фахівці. Він працює – доки вам не знадобиться масштабування або оплата рахунків.

Який вам слід обрати?

SDS: найкраще підходить для організацій, що переходять на гібридну хмару, робочі навантаження зі штучним інтелектом/машинним навчанням або автоматизовані середовища зберігання даних.

NAS: підходить для невеликих команд, яким потрібен простий обмін файлами з мінімальними накладними витратами.

SAN: все ще цінна для критично важливих для продуктивності робочих навантажень, але менш адаптивна, ніж сучасні програмно-визначені рішення для зберігання даних.

Програмно-визначене сховище даних (SDS) – це базовий варіант для тих, хто хоче масштабовану інфраструктуру без необхідності платити постачальникам обладнання за цю перевагу. Абстрагуючи програмний рівень від фізичних пристроїв, SDS надає вам гнучкість для зростання, відновлення та адаптації до ваших робочих навантажень.

Впровадження SDS означає планування потужності, моніторинг IOPS/затримки, забезпечення належних політик резервного копіювання та реплікації, виконання регулярних оновлень та перевірку справності стеку. Натомість ви отримуєте гнучкість обладнання, передбачувану масштабованість та зменшену залежність від пристроїв різних постачальників.

Коротко кажучи:

- Що робить SDS: він абстрагує сховище за допомогою програмного рівня, усуваючи залежність від конкретного обладнання та знижуючи сукупну вартість володіння (TCO) завдяки стандартним серверам та еластичному зростанню.
- Що змінюється на практиці: стало легше масштабувати горизонтально та вертикально, швидше відновлюватися після збоїв та стандартизувати управління в гібридних та багатохмарних середовищах.
- Хто отримує найбільшу вигоду: команди, чії робочі навантаження не зростають за календарним графіком – конвеєри штучного інтелекту/машинного навчання, аналітика, веб-проекти з високим трафіком та ландшафти DevOps.

NAS та SAN все ще мають свої ніші, але якщо ви створюєте системи, які повинні витримувати реальний трафік та реальні збої, SDS – це практичний вибір.

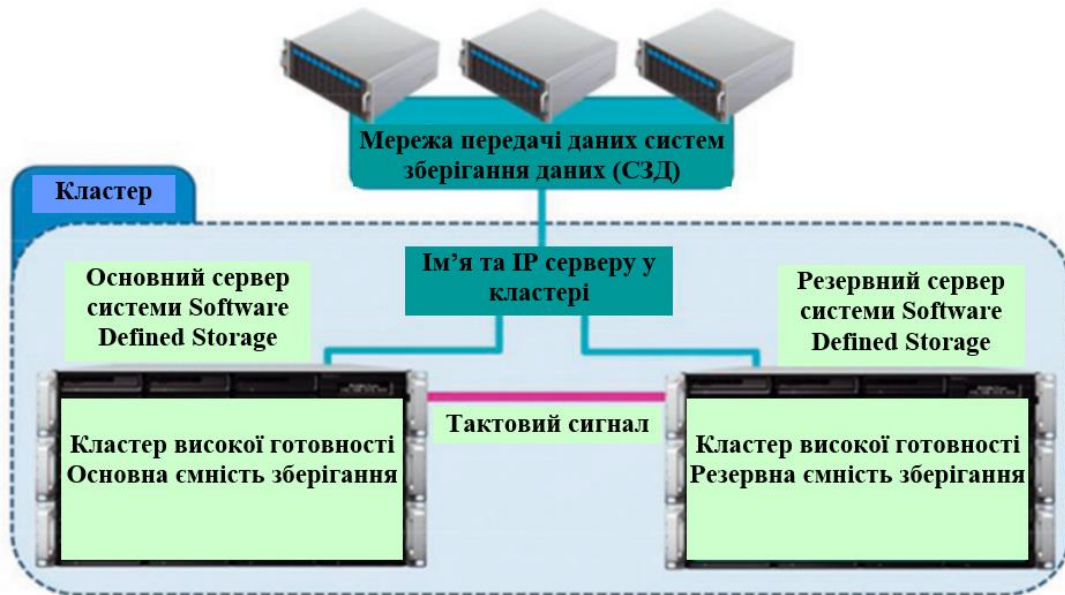


Рисунок 1 – Структурна схема системи

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів Software Defined Storage. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем Software Defined Storage.
- Досліджена система Software Defined Storage.
- На основі отриманих результатів досліджень створена програмна реалізація системи Software Defined Storage.

Розроблені алгоритми дозволяють успішно вирішувати завдання Software Defined Storage. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Smirnova, T., Gnatyuk, S., Yudin, O., Sydorenko, V., Polozhentsev, A., «The Model for Calculating the Quantitative Criteria for Assessing the Security Level of Information and Telecommunication Systems». CEUR Workshop Proceedings Volume 3156, 2022, Pages 390-399.
2. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». Проблеми інформатизації та управління, № 2(70). 2022. С. 28-37.
3. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції ґешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 3(69). С. 93-98.
4. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції ґешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Вісник Хмельницького національного університету. Серія: «Технічні науки», № 2 (307). С. 46-52. 2022.
5. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції ґешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 1(67). С. 84-89.
6. Smirnova T., Gnatyuk S., Berdibayev R., Avkurova Zh., Iavich M. «Cloud-Based Cyber Incidents Response System and Software Tools». Communications in Computer and Information Science, 2021, vol 1486. Springer, Cham. pp 169-184.
7. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.

8. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». *Journal of theoretical and applied information technology* Vol.98. No 21, 2020, P. 3334-3346.
9. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177.
10. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) *Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies*, vol 48. Springer, Cham. 2021. pp 557-587.
11. Smirnov, O., Markovets, O. Vovk, N., Turchyn, Y., «Model of informational support for social network administrators' content creation». *CEUR Workshop Proceedings Volume 2616*, 2020, Pages 125-136.
12. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». *CEUR Workshop Proceedings Volume 2616*, 2020, Pages 366-379.
13. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», *CEUR Workshop Proceedings Volume 2608*, 2020, Pages 633-645.
14. Smirnov O. Kuznetsov A., Zaichenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». *International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019*; Odessa; Ukraine; 9-13 September 2019. P.22-28.
15. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». *International Journal of Computing*; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.
16. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019. P.517-522.
17. Smirnov, O., Odarchenko, R., Abakumova, A., Usik, P., Kundyz, M., «QoE optimization technique for media delivery in 5G networks». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019. P.597-601.
18. Smirnov, O., Krasnobayev, V., Yanko, A., Kuznetsova, T. «Methods of nulling numbers in the system of residual classes». *CEUR Workshop Proceedings*, Vol 2588, P. 90-106, 2019.
19. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Averchev, A., Pastukhov, M., Kuznetsova, K., «Formation of Pseudorandom Sequences with Special Correlation Properties», 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT -2019/ Lviv, Ukraine, 2-6 July, 2019, P. 395-399.
20. Smirnov, O., Kuznetsov, A., Kiian, A., Zamula, A., Rudenko, S., Hryhorenko, V., «Variance Analysis of Networks Traffic for Intrusion Detection in Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 353-358.
21. Smirnov, O., Kuznetsov, A., Kavun, S., Babenko, B., Nakisko, O., Kuznetsova, K., «Malware Correlation Monitoring in Computer Networks of Promising Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 347-352.
22. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Pastukhov, M., Kuznetsova, K., Prokopovych-Tkachenko, D., «Discrete Signals with Special Correlation Properties», *CEUR Workshop Proceedings Volume 2353*, CEUR Workshop Proceedings 2019, Pages 618-629.
23. Smirnov A.A., Kuznetsov A.A., Danilenko D.A., Berezovsky A., «The statistical analysis of a network traffic for the intrusion detection and prevention systems», *Telecommunications and Radio Engineering*. – Volume 74, Issue 1. – Begel House Inc. – 2015. – P. 61-78.
24. Смірнов О.А., Смірнова Т.В., Буравченко К.О., Кравченко С.С., Горбов В.О., «Хмарна система підтримки прийняття рішень технологічного процесу відновлення поверхонь конструкцій і деталей машин». *Сучасні інформаційні системи*. 2021. Т. 5, № 4. С. 79-95
25. Смірнов О.А., Усік П.С., Миронець І.В., Буравченко К.О., Якименко Н.М. «Метод підвищення ефективності розподіленої обробки даних у комп'ютерних системах операторів стільникового зв'язку» *Вісник Черкаського державного технологічного університету. Технічні науки*. №4. С. 103-110. 2020.
26. О.А.Смірнов, Т.В.Смірнова, Л.І. Поліщук, К.О. Буравченко, А.О.Макевнін, «Дослідження хмарних технологій як сервісів», *Кібербезпека: освіта, наука, техніка*. № 3(7). С. 43-62. 2020.
27. Смірнов О.А., Коноплицька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Поліщук Л.І. *Інформаційна безпека в комп'ютерних мережах. Навчальний посібник* – Кропивницький: вид. Лисенко В.Ф. 2020. – 294 с.
28. О.А. Смірнов, П.С. Усік, «дослідження перспектив використання технологічних рішень в мережах 5g» у *Кібербезпека та інформаційні технології: монографія*. – Х.: ТОВ «ДІСА ПЛЮС», 2020.С. 122-135.
29. Смірнов О.А., Дреєва Г.М., Дреєв О.М., Смірнова Т.В. «Фрактальний аналіз генератора самоподібного

- трафіку на основі ланцюга Маркова». Центральнотураїнський науковий вісник. Технічні науки. № 2(33). с. 161-172, 2019.
30. Смірнов О.А., Коноплицька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В. Поліщук Л.І. Проектування комп'ютерних систем та мереж. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2019. – 264 с.
31. Smirnov, O., Kuznetsov, A., Kuznetsova., K. Synthesis of Discrete Signals with Improved Correlation Properties. Монографія: In.: ISCI'2019: Information Security in Critical Infrastructures. Collective monograph. Edited by Ivan D. Gorbenko and Alexandr A. Kuznetsov, ASC Academic Publishing, USA, 2019, pp. 281-299. – ISBN: 978-0-9989826-8-7 (Hardback), ISBN: 978-0-9989826-9-4 (Ebook).
32. Смірнов О.А., Дреєва Г.М. Метод генерування фрактального трафіку за допомогою моделі генератора на графі. Монографія: Інформаційна безпека та інформаційні технології: монографія / за заг. ред. В. С. Пономаренка. – Х. : Вид. Рожко С.Г. 2019. С. 123-139
33. Дреєва Г.М., Смірнов О.А., Дреєв О.М. Метод генерування фрактальноподібної числової послідовності на основі скінченного автомату для моделювання трафіку у мережі. Центральнотураїнський науковий вісник. Технічні науки. № 1(32). с. 173-183, 2019.

УДК 004

В.Мороз, магістр гр. КН-24М,*Центральноукраїнський національний технічний університет*

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ІНТЕЛЕКТУАЛЬНОГО КЕРУВАННЯ КАБЕЛЬНОЮ ІНФРАСТРУКТУРОЮ АІМ

У статті розроблено програмне забезпечення, яке призначено для системи інтелектуального керування кабельною інфраструктурою АІМ. Метою розробки є дослідження та принципи побудови системи інтелектуального керування кабельною інфраструктурою АІМ. Об'єктом дослідження є процес інтелектуального керування кабельною інфраструктурою АІМ. Предметом дослідження є методи інтелектуального керування кабельною інфраструктурою АІМ. Методи дослідження базуються на методах великих даних, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи інтелектуального керування кабельною інфраструктурою АІМ. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

інтелектуальне керування, кабельна інфраструктура АІМ

Постановка проблеми. Сьогодні ІТ-індустрія визнає важливу роль, яку можуть забезпечити рішення автоматизованого управління інфраструктурою (АІМ) завдяки розробці власних стандартів, щоб допомогти мережевим менеджерам оптимізувати свої інфраструктури та досягти більшої ефективності використання доступних ресурсів.

Системи АІМ інтегровані апаратними та програмними системами, які виявляють кабельні з'єднання та документують інфраструктуру, включаючи підключене обладнання, що дозволяє керувати інфраструктурою та обмінюватися даними з іншими системами управління, підвищуючи операційну ефективність кожної системи.

Системи АІМ відстежують та реєструють зміни в підключенні пристроїв і подають сигнали тривоги, щоб попередити персонал про будь-які несанкціоновані або проблемні події.

Системи АІМ показують, що саме у вас є, як взаємодіють різні елементи вашої інфраструктури та де ви можете знайти нові можливості для оптимізації, і все це в режимі реального часу.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи інтелектуального керування кабельною інфраструктурою АІМ.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи інтелектуального керування кабельною інфраструктурою АІМ.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем інтелектуального керування кабельною інфраструктурою АІМ.
- Дослідження системи інтелектуального керування кабельною інфраструктурою АІМ.
- Програмна реалізація системи інтелектуального керування кабельною інфраструктурою АІМ.

Об'єктом дослідження є процес інтелектуального керування кабельною інфраструктурою АІМ.

Предметом дослідження є методи інтелектуального керування кабельною інфраструктурою АІМ.

Методи дослідження базуються на методах великих даних, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. У сучасному швидкоплинному цифровому світі підтримка ефективного, масштабованого та надійного центру обробки даних є критично важливою для успіху бізнесу. Одним з фундаментальних елементів, який часто ігнорується, є структурована кабельна система. Інвестування в модернізацію кабельної системи може значно покращити продуктивність вашого центру обробки даних, забезпечити майбутнє вашої інфраструктури та скоротити час простою. Давайте розглянемо найефективніші вдосконалення структурованої кабельної системи, які ви можете впроваджувати протягом року, щоб залишатися на крок попереду.

1. Використовуйте високошільне оптоволоконне кабелювання. Оптоволоконне кабелювання стало золотим стандартом для сучасних центрів обробки даних. Рішення з високошільним оптоволоконним кабелем забезпечують неперевершену швидкість і пропускну здатність, що робить їх ідеальними для задоволення сучасних потреб у даних. Модернізація вашої структурованої кабельної системи для включення високошільного оптоволоконного кабелю може оптимізувати компонування вашого центру обробки даних і мінімізувати захаращення, забезпечуючи при цьому блискавично швидке підключення.

Основні переваги:

- Підтримує вищі швидкості передачі даних.
- Зменшує потреби у фізичному просторі.
- Покращує масштабованість для майбутнього зростання.

Інтегруючи це рішення для структурованої кабельної системи, ви забезпечите готовність вашого центру обробки даних до швидкого розвитку технологій.

2. Інвестуйте в кабель Cat8 Ethernet. Кабелі Cat8 Ethernet є одними з найсучасніших мідних кабелів. Забезпечуючи швидкість до 40 Гбіт/с і підтримку вищих частот, Cat8 ідеально підходить для модернізації вашої структурованої кабельної системи з метою підготовки до потреб мереж наступного покоління.

Чому це того варте:

- Зменшує затримку.
- Забезпечує чудове екранування для мінімізації перешкод.
- Забезпечує майбутнє вашої мережі для обладнання 25G та 40G.

Для компаній, які бажають модернізувати свою структуровану кабельну інфраструктуру, Cat8 – це економічно ефективне, але потужне рішення.

3. Оптимізуйте управління кабелями за допомогою модульних патч-панелей. Неорганізоване прокладання кабелів є поширеною проблемою в старіючих центрах обробки даних, що призводить до неефективності та непотрібного часу простою. Перехід на модульні патч-панелі як частину вашої кабельної системи може спростити управління кабелями та покращити доступність.

Переваги:

- Легке виявлення та вирішення проблем з підключенням.
- Підвищена гнучкість додавання або видалення з'єднань.
- Чисті, професійно виглядаючі установки.

Правильне управління кабелями в рамках вашої структурованої кабельної системи значно підвищить експлуатаційну ефективність.

4. Перехід на роз'єми МРО/МТР. Багатоволоконні роз'єми з підключенням до оптоволоконних вставок (МРО) та багатоволоконні роз'єми з підключенням до оптоволоконних вставок (МТР) є критично важливими для підтримки високошвидкісних волоконно-оптичних мереж. Ці роз'єми дозволяють одночасне підключення кількох волокон, оптимізуючи налаштування структурованої кабельної системи та підвищуючи ефективність.

Переваги:

- Спрощує встановлення оптоволоконних ліній.
- Зменшує ризик помилок підключення.
- Підтримує високошвидкісні програми, такі як Ethernet 100G та 400G.

Включення роз'ємів MPO/MTT у ваш кабельний проект гарантує, що ваш центр обробки даних зможе впоратися з вимогами сучасних мереж.

5. Розгортання передових рішень для охолодження. Хоча охолодження не пов'язане безпосередньо зі структурованою кабельною системою, воно є важливим фактором для будь-якої модернізації кабельної системи. Надмірне тепло може погіршити стан кабелів та обладнання, що призводить до дорогого ремонту та простоїв. Поєднання модернізації структурованої кабельної системи з передовими стратегіями охолодження може допомогти підтримувати оптимальну продуктивність.

Запропоновані покращення:

- Використовуйте кабельні канали під підлогою для кращої циркуляції повітря.
- Інвестуйте в системи утримання гарячих/холодних проходів.
- Вибирайте термостійкі матеріали для кабелів.

Інтеграція питань охолодження у вашу структуровану кабельну систему мінімізує ризики та збільшує термін служби.

6. Перейдіть на автоматизовані системи управління інфраструктурою (AIM). Керування структурованою кабельною інфраструктурою центру обробки даних може бути складним завданням без належних інструментів. Системи автоматизованого управління інфраструктурою (AIM) забезпечують моніторинг і контроль над вашими кабелями та з'єднаннями в режимі реального часу.

Як допомагають системи AIM:

- Надайте точну документацію щодо всіх кабельних засобів.
- Забезпечити швидше усунення несправностей та технічне обслуговування.
- Покращуйте безпеку, контролюючи фізичні з'єднання.

Додавання систем AIM до модернізації структурованої кабельної мережі може значно зменшити людський фактор та час простою.

7. Плануйте міграцію на 400G Ethernet. Зі зростанням потреб у даних, 400G Ethernet стає новим стандартом для високопродуктивних мереж. Модернізація структурованої кабельної системи для підтримки цієї технології гарантує, що ваш центр обробки даних залишиться конкурентоспроможним у найближчі роки.

Кроки з підготовки:

- Для більшої пропускної здатності перейдіть на багатомодове оптоволокно OM5.
- Використовуйте попередньо підготовлені кабельні системи для швидшого розгортання.
- Впровадити трансивери, сумісні з технологією 400G.

Підготовка вашої структурованої кабельної системи до використання з Ethernet 400G з урахуванням майбутніх потреб позиціонуватиме ваш центр обробки даних як лідера галузі. Модернізація вашої структурованої кабельної системи – це не просто технічне рішення, це стратегічна інвестиція в майбутнє вашого центру обробки даних. Від високощільного оптоволоконного кабелю до передових рішень для охолодження, кожне оновлення відіграє життєво важливу роль у підвищенні продуктивності, масштабованості та надійності. Не чекайте, поки застаріла інфраструктура загальмує ваш бізнес – почніть планувати модернізацію структурованої кабельної системи вже сьогодні.

Розроблене програмне забезпечення – рішення AIM для організацій, які прагнуть спростити та оптимізувати свої мережеві операції. Забезпечуючи видимість, контроль та безпеку в режимі реального часу, наше рішення дозволяє компаніям оптимізувати управління інфраструктурою, скоротити час простою та максимізувати продуктивність.

Монітор

Детальні мережеві представлення. Ієрархічні представлення відображають усю вашу мережу, від представлення інфраструктури стійок і шаф до робочих зон і схем поверхів – все з повними схемами електричних ланцюгів, включаючи активне обладнання. Схеми електричних ланцюгів також відображаються локально на РК-панелях керування.

Точність бази даних. Вся мережева інформація зберігається в програмно-керованій базі даних, яка автоматично оновлюється в режимі реального часу в міру переміщень, додавань та змін, що гарантує постійний контроль стану мережі.

Зменшення часу простою. Функція трасування ланцюгів швидко визначає місце несправності в каналі. Інформація може відображатися на панелях для допомоги персоналу на місці, що значно скорочує час, необхідний для пошуку та усунення збою в мережі.

Керувати

Максимізація використання мережевих ресурсів. Детальні підрозділи про використання, що генеруються нашим програмним забезпеченням наступного покоління, дозволяють користувачам бачити доступні порти комутаторів або патч-панелей. Кінцеві пристрої можна відстежувати за місцем розташування, типом обладнання, виробником, послугою або іншими критеріями, забезпечуючи кращу видимість та використання цих критично важливих ресурсів.

Віддалене керування сайтом забезпечує перегляд мереж у віддалених офісах у режимі реального часу, допомагаючи забезпечити дотримання корпоративних ІТ-політик та запобігаючи несанкціонованим змінам у мережі.

Оптимізація процесів виконання робочих замовлень. має інтегрований модуль виконання робочих замовлень, що забезпечує їх правильне виконання. Крім того, наші інноваційні головні панелі керування (MCP) та інтелектуальні патч-панелі (SPP) допомагають технікам направляти етапи виконання робочого замовлення та вказують, чи дія виконана правильно.

Захист

Сповіщення в режимі реального часу. може надсилати сповіщення електронною поштою ІТ-фахівцям або співробітникам служби безпеки в режимі реального часу, коли в мережі відбуваються несанкціоновані події, такі як виявлення несанкціонованих пристроїв, які намагаються підключитися до вашої локальної мережі.

Дотримання нормативних вимог веде журнал аудиту всіх мережевих подій, що спрощує дотримання нормативних вимог, включаючи: Sarbanes-Oxley, ITIL, HIPAA, FDA 21 CFR Part II тощо.

Зменшений час відгуку. оснащений потужною пошуковою системою, яка дозволяє користувачам швидко знаходити будь-який елемент у вашій мережі, переглядати його атрибути та стан підключення, а потім за потреби надавати додаткову підтримку.

Структурна схема системи зображена на рисунку 1.

З рисунку видно, що моніторинг локальної мережі здійснюється по трьох напрямках:

- Моніторинг обладнання автоматизованого керування кабельною інфраструктурою AIM.
- Моніторинг ресурсів автоматизованого керування кабельною інфраструктурою AIM.
- Моніторинг трафіку автоматизованого керування кабельною інфраструктурою AIM.

Моніторинг обладнання включає в себе побудову списку наявного обладнання та здійснення його контролю. До мережного обладнання, що підлягає моніторингу, відносяться: персональні комп'ютери, ноутбуки, сервери, принтери, ір-телефони.

Моніторинг ресурсів дозволяє переглядати та завантажувати наявні в мережі ресурси, а також розміщувати чи приховувати для загального доступу свої ресурси. До ресурсів локальної мережі відносяться: файли, мультимедіа, бази даних, сервіси інформаційної безпеки, список користувачів.

Моніторинг трафіку використовується для контролю вхідного та вихідного трафіку. Він включає у себе контроль підключених інтерфейсів, статистику подій по основним мережним протоколам: TCP, UDP, IP та ICMP.

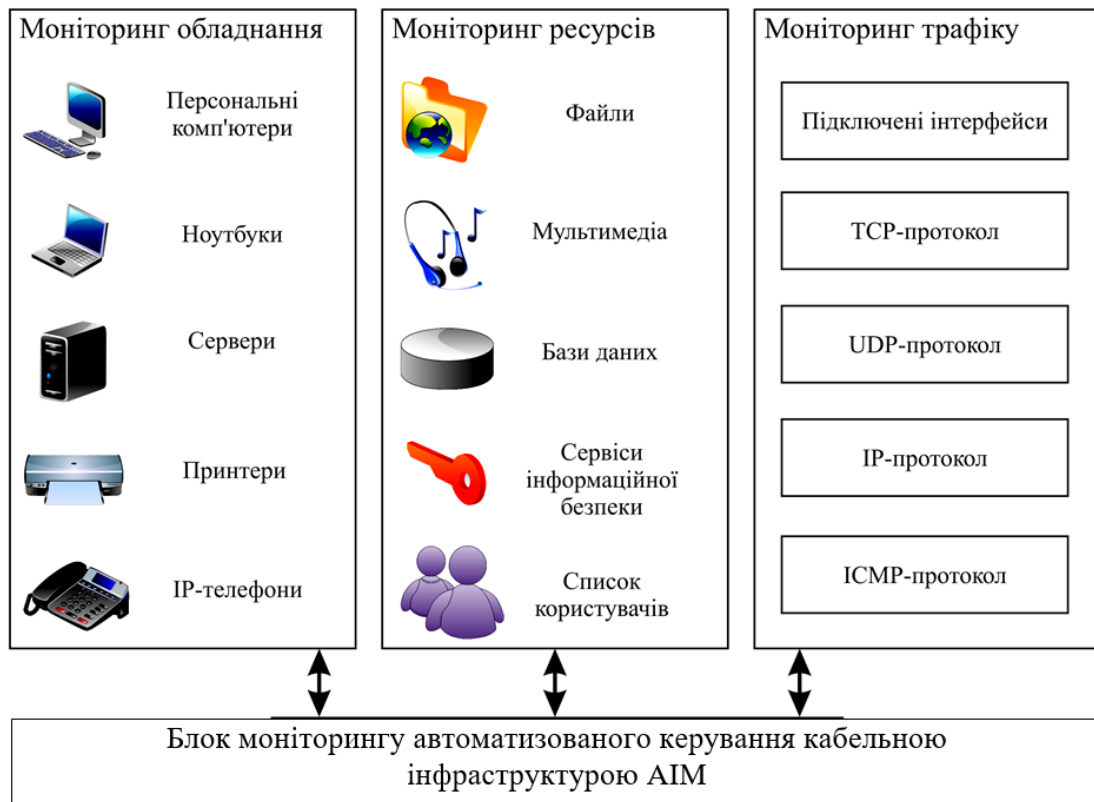


Рисунок 1 – Структурна схема системи

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів інтелектуального керування кабельною інфраструктурою AIM. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем інтелектуального керування кабельною інфраструктурою AIM.
- Досліджена система інтелектуального керування кабельною інфраструктурою AIM.
- На основі отриманих результатів досліджень створена програмна реалізація системи інтелектуального керування кабельною інфраструктурою AIM.

Розроблені алгоритми дозволяють успішно вирішувати завдання інтелектуального керування кабельною інфраструктурою AIM. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». Advanced Information Systems, 2023, 7(2), pp. 49-56.
2. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchев, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». CEUR Workshop Proceedings, Volume 3530, 2023, pp. 256-265.
3. Smirnov, O., Odarchenko, R., Smirnova, T., Bondar, S., Volosheniuk, D. «Optimal Structure Construction of Private 5G Network for the Needs of Enterprises». Lecture Notes on Data Engineering and Communications Technologies, 2023, 178, pp. 208–223.
4. Аль-Мудхафар Акіл Абдулхуссейн М., Смірнова Т.В., Буравченко К.О., Смірнов О.А. «Метод оцінки та підвищення користувацького досвіду абонентів в програмно-конфігурованих мережах на основі

- використання машинного навчання». Сучасні інформаційні системи, 2023, том 7, № 2, С. 49-56.
5. Smirnova, T., Gnatyuk, S., Yudin, O., Sydorenko, V., Polozhentsev, A., «The Model for Calculating the Quantitative Criteria for Assessing the Security Level of Information and Telecommunication Systems». CEUR Workshop Proceedings Volume 3156, 2022, Pages 390-399.
 6. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». Проблеми інформатизації та управління, № 2(70). 2022. С. 28-37.
 7. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції ґешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 3(69). С. 93-98.
 8. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції ґешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Вісник Хмельницького національного університету. Серія: «Технічні науки», № 2 (307). С. 46-52. 2022.
 9. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції ґешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 1(67). С. 84-89.
 10. Smirnova T., Gnatyuk S., Berdibayev R., Avkurova Zh., Iavich M. «Cloud-Based Cyber Incidents Response System and Software Tools». Communications in Computer and Information Science, 2021, vol 1486. Springer, Cham. pp 169-184.
 11. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
 12. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». Journal of theoretical and applied information technology Vol.98. No 21, 2020, P. 3334-3346.
 13. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177.
 14. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587.
 15. Smirnov, O., Markovets, O. Vovk, N., Turchyn, Y., «Model of informational support for social network administrators' content creation». CEUR Workshop Proceedings Volume 2616, 2020, Pages 125-136.
 16. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». CEUR Workshop Proceedings Volume 2616, 2020, Pages 366-379.
 17. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645.
 18. Smirnov O. Kuznetsov A., Zaichenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019; Odessa; Ukraine; 9-13 September 2019. P.22-28.
 19. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.
 20. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019 . P.517-522.
 21. Smirnov, O., Odarchenko, R., Abakumova, A., Usik, P., Kundyz, M., «QoE optimization technique for media delivery in 5G networks». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019. P.597-601.
 22. Smirnov, O., Krasnobayev, V., Yanko, A., Kuznetsova, T. «Methods of nulling numbers in the system of residual classes». CEUR Workshop Proceedings, Vol 2588, P. 90-106, 2019.
 23. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Averchev, A., Pastukhov, M., Kuznetsova, K., «Formation of Pseudorandom Sequences with Special Correlation Properties», 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT -2019/ Lviv, Ukraine, 2-6 July, 2019, P. 395-399.
 24. Smirnov, O., Kuznetsov, A., Kiian, A., Zamula, A., Rudenko, S., Hryhorenko, V., «Variance Analysis of Networks Traffic for Intrusion Detection in Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems

- (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 353-358.
25. Smirnov, O., Kuznetsov, A., Kavun, S., Babenko, B., Nakisko, O., Kuznetsova, K., «Malware Correlation Monitoring in Computer Networks of Promising Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 347-352.
26. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Pastukhov, M., Kuznetsova, K., Prokopovych-Tkachenko, D., «Discrete Signals with Special Correlation Properties», CEUR Workshop Proceedings Volume 2353, CEUR Workshop Proceedings 2019, Pages 618-629.
27. Smirnov A.A., Kuznetsov A.A., Danilenko D.A., Berezovsky A., «The statistical analysis of a network traffic for the intrusion detection and prevention systems», Telecommunications and Radio Engineering. – Volume 74, Issue 1. – Begel House Inc. – 2015. – P. 61-78.
28. Смірнов О.А., Смірнова Т.В., Буравченко К.О., Кравченко С.С., Горбов В.О., «Хмарна система підтримки прийняття рішень технологічного процесу відновлення поверхонь конструкцій і деталей машин». Сучасні інформаційні системи. 2021. Т. 5, № 4. С. 79-95
29. Смірнов О.А., Усік П.С., Миронець І.В., Буравченко К.О., Якименко Н.М. «Метод підвищення ефективності розподіленої обробки даних у комп'ютерних системах операторів стільникового зв'язку» Вісник Черкаського державного технологічного університету. Технічні науки. №4. С. 103-110. 2020.
30. О.А.Смірнов, Т.В.Смірнова, Л.І. Поліщук, К.О. Буравченко, А.О.Макевнін, «Дослідження хмарних технологій як сервісів», Кібербезпека: освіта, наука, техніка. № 3(7). С. 43-62. 2020.
31. Смірнов О.А., Коноплицька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Поліщук Л.І. Інформаційна безпека в комп'ютерних мережах. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2020. – 294 с.

УДК 004

А.Мукієнко, магістр гр. КН-24М,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ХМАРНОГО СЕРВІСУ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ РОЗУМНОГО БУДИНКУ

У статті розроблено програмне забезпечення, яке призначено для системи хмарного сервісу забезпечення безпеки розумного будинку. Метою розробки є дослідження та принципи побудови системи хмарного сервісу забезпечення безпеки розумного будинку. Об'єктом дослідження є процес хмарного сервісу забезпечення безпеки розумного будинку. Предметом дослідження є методи хмарного сервісу забезпечення безпеки розумного будинку. Методи дослідження базуються на методах хмарних технологій, методах інтернету речей, методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи хмарного сервісу забезпечення безпеки розумного будинку. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

хмарний сервіс, забезпечення безпеки, розумний будинок

Постановка проблеми. В останні роки хмарні системи домашньої безпеки революціонізували спосіб захисту наших домівок. Ці системи використовують можливості хмарних обчислень, щоб пропонувати розширені функції, віддалений доступ та безперешкодну інтеграцію з пристроями розумного дому.

Хмарні системи домашньої безпеки використовують підключені до Інтернету пристрої та хмарні обчислення для забезпечення моніторингу, оповіщення та керування в режимі реального часу. На відміну від традиційних систем безпеки, які часто потребують тривалої проводки та локального сховища, хмарні системи зберігають дані на безпечних зовнішніх серверах, що забезпечує легший доступ та керування.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи хмарного сервісу забезпечення безпеки розумного будинку.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи хмарного сервісу забезпечення безпеки розумного будинку.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем хмарного сервісу забезпечення безпеки розумного будинку.
- Дослідження системи хмарного сервісу забезпечення безпеки розумного будинку.
- Програмна реалізація системи хмарного сервісу забезпечення безпеки розумного будинку.

Об'єктом дослідження є процес хмарного сервісу забезпечення безпеки розумного будинку.

Предметом дослідження є методи хмарного сервісу забезпечення безпеки розумного будинку.

Методи дослідження базуються на методах хмарних технологій, методах інтернету речей, методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Очікується, що світовий ринок систем безпеки житлових приміщень до 2027 року перевищить 13 мільярдів доларів, зростаючи на 24,58%

щорічно. Оскільки загальна кількість систем «розумних будинків» досягла 258,54 мільйона, очевидно, що люди почали усвідомлювати важливість систем безпеки розумних будинків і більше не розглядають безпеку житлових приміщень як розкіш.

Як показують опитування, сучасні клієнти охоче інвестують у розумні системи безпеки, зокрема житлові, та платитимуть вищу орендну плату за розумні будинки.

У цьому розділі ми розповімо, як працює система безпеки розумного дому, перерахуємо її обов'язкові функції та розглянемо приклади популярних програм для домашньої безпеки. Ми почнемо з визначення розумної системи захисту для дому та перейдемо до її переваг.

Інтелектуальна система безпеки для житла – це мережа пристроїв, які працюють синхронно один з одним, забезпечуючи розширений захист та моніторинг будинку.

Основні компоненти такої мережі включають наступне:

1. Інструменти обмеження доступу

Інтелектуальні замки дозволяють домовласникам дистанційно замикати та відмикати свої двері за допомогою смартфона або голосових команд. Найбільш інноваційні замки оснащені сканерами відбитків пальців, які набагато безпечніші, ніж традиційні замки з кодом та паролем.

2. Детектори активності

Сучасні домогосподарства використовують датчики, що фіксують рух, розбиття скла, відкриття дверей та вікон, а також дим або шкідливі речовини та викиди. Ці датчики відстежують незвичайну активність та зміни в навколишньому середовищі та повідомляють про них мешканцям.

3. Спостереження

Відеоспостереження також є невід'ємною частиною потужної мережі безпеки житлового будинку. Внутрішні та/або зовнішні камери контролюють будівлю, записують відео та дозволяють користувачам переглядати відео в реальному часі зі своїх телефонів або комп'ютерів.

4. Звукові сирени

Ще однією традиційною частиною системи безпеки є звукова сигналізація. Сучасні засоби спостереження за будинком використовують звукові сирени або дзвінки для попередження мешканців та стримування зловмисників.

5. Голосові помічники

Деякі інтелектуальні платформи захисту дому інтегрують популярні голосові помічники, що дозволяє власникам керувати ними за допомогою голосових команд.

6. Служба моніторингу

Багато інтелектуальних систем захисту дому мають професійну службу моніторингу, здатну сповістити правоохоронні органи про випадок злому або іншої термінової ситуації.

7. Кнопки екстреного виклику

Це фізичні або віртуальні пристрої, які дозволяють мешканцям миттєво викликати екстрену допомогу у разі кризи чи загрози. Кнопки паніки призначені для швидкого реагування на потенційно небезпечні ситуації, такі як проникнення зі зломом, невідкладна медична допомога чи будь-які інші загрозливі обставини.

8. Панель керування/хаб

Панель керування об'єднує всі інші мережеві компоненти в один центральний вузол та керує ними. Вона діє як централізований вузол для ввімкнення та вимкнення системи, керування розумною домашньою технікою та отримання сповіщень.

Інтеграція цих пристроїв створює рішення, яке можна налаштувати відповідно до вподобань мешканця та забезпечити повний захист.

Безпека розумного дому: ключові принципи роботи

Як працює система безпеки розумного дому? Домашні мережі безпеки включають численні інтелектуальні пристрої, які підключаються до центральної панелі керування.

Остання підключається до Інтернету, що дозволяє власникам відстежувати її через додаток та керувати нею дистанційно за потреби.

Наприклад, якщо у вашій квартирі спрацював датчик, ваш телефон отримає сигнал. Додаток безпеки попросить вас вжити заходів або вимкнути сигналізацію.

Платформи розумного дому використовують інноваційні технології для виявлення та реагування на можливі загрози в режимі реального часу. Вони також можуть синхронно працювати з іншими розумними пристроями, забезпечуючи комплексне рішення для домашньої автоматизації та безпеки.

Переваги системи безпеки житлового будинку

Розумні системи безпеки житлових приміщень перевершують звичайні за кількома показниками. Мешканці можуть бути впевнені, що їхня власність у безпеці, коли її охороняє інтелектуальна мережа захисту. Користувачі також можуть перевіряти її будь-коли дистанційно.

Більш конкретно, переваги включають наступне:

Віддалене відстеження та управління

Сучасні мережі безпеки керуються за допомогою дистанційного керування. Мешканці також можуть спілкуватися з відвідувачами або давати вказівки домашньому персоналу в дистанційному режимі.

Миттєві сповіщення

Якщо щось відхиляється від норми, користувачі отримують миттєві сповіщення через мобільні додатки домашньої безпеки. Наприклад, домовласник отримуватиме своєчасні сповіщення про ввімкнений електроприлад, протікання крана або неочікуваного відвідувача.

Тільки дійсні виклики служби безпеки

Боротьба з хибними тривогами може бути складною. Якщо аварійній бригаді доручено забезпечити безпеку будинку, власникам можуть фактично стягнути чималу суму за хибний виклик охорони. Завдяки інтелектуальним системам розумного дому хибні тривоги більше не є проблемою.

Запобігання вторгненню

Сповіщення про те, що ввімкнено систему захисту розумного дому, слугує ідеальним захистом від грабіжників та зловмисників. Більшість злочинців, які сподіваються на швидкий та легкий доступ, легко зупиняться завдяки інтелектуальній системі захисту дому.

Важко відключити

Зловмисникам також досить важко вивести з ладу житлову мережу безпеки, просто відрізавши шнур. Такі платформи використовують бездротові технології та їх нелегко вивести з ладу.

Фінансово виправдано

Окрім захисту та безпеки вашої власності, хороша система цифрової безпеки може фактично забезпечити кращі страхові пакети для власників нерухомості, що робить її розумною інвестицією.

Комплексний захист, моніторинг у режимі реального часу, фінансові переваги та чудова зручність використання роблять програми та системи безпеки для розумного дому популярним вибором для сучасних технічно підкованих власників житлової нерухомості. У наступному розділі ми розглянемо приклади деяких популярних мобільних програм та систем домашньої безпеки.

Основні характеристики мобільного додатку для домашньої безпеки

Створення мобільного застосунку є невід'ємною частиною побудови системи безпеки для житлових приміщень. Набір функцій відрізнятиметься залежно від функціональності та компонентів рішення, проте деякі функції є абсолютно необхідними.

Також, якщо ви хочете, щоб ваш додаток працював з більшістю доступних розумних побутових пристроїв, подумайте про впровадження базового набору функцій.

8. Дистанційне керування

Ваш мобільний додаток для безпеки повинен дозволяти користувачам дистанційно отримувати доступ до своєї мережі безпеки та керувати нею. Це включає такі функції, як встановлення та зняття системи з охорони, керування інтелектуальними пристроями та налаштування параметрів з будь-якого місця, де є підключення до Інтернету.

9. Своєчасні сповіщення

Додаток має надсилати сповіщення в режимі реального часу на мобільні пристрої користувачів про різні події, такі як порушення безпеки, виявлення руху, відкриття дверей/вікон або спрацювання сигналізації. Користувачі повинні отримувати сповіщення своєчасно та мати можливість вжити негайних заходів за потреби.

10. Спостереження в реальному часі

Додаток для домашньої безпеки повинен забезпечувати пряму трансляцію відео з камер спостереження, розташованих зовні та всередині будівлі. Власники будинків повинні мати можливість переглядати зображення з камер у режимі реального часу, перемикатися між різними камерами та мати можливість двостороннього аудіозв'язку, якщо камери його підтримують.

11. Історія подій та відтворення відео

Додаток має зберігати журнали історії подій, включаючи позначки часу та деталі минулих подій безпеки. Крім того, він має надавати користувачам доступ до записаних відеоматеріалів з камер для відтворення, що дає їм змогу переглядати конкретні інциденти або події.

12. Геозонування

Геозонування – це корисна функція, яка дозволяє користувачам визначати віртуальні межі або зони. Додаток має підтримувати можливості геозонування, що дозволить користувачам отримувати автоматичні сповіщення або запускати певні дії на основі їхнього місцезнаходження, такі як вхід або вихід із зазначеної зони.

13. Персоналізація та налаштування

Найкращі системи безпеки для розумного дому повинні пропонувати варіанти налаштування відповідно до індивідуальних уподобань. Клієнти повинні мати можливість налаштовувати параметри, розклади та правила відповідно до своїх конкретних потреб. Це може включати налаштування різних режимів (наприклад, «вдома», «не вдома», «сон»), коригування параметрів сповіщень або створення правил автоматизації.

14. Керування користувачами та доступом

Мобільний додаток безпеки повинен дозволяти користувачам додавати та видаляти облікові записи користувачів, призначати різні рівні доступу та дозволів, а також налаштовувати тимчасовий або гостьовий доступ для таких осіб, як члени родини, друзі або постачальники послуг.

15. Інтеграція

Інтеграція з іншими інструментами та платформами покращує загальну функціональність та зручність системи захисту житлових приміщень. Додаток повинен підтримувати інтеграцію із сумісними пристроями, дозволяючи користувачам керувати кількома функціями розумного дому з одного інтерфейсу.

16. Відстеження стану та стану системи

Додаток має надавати інформацію про стан та справність пристроїв системи. Це включає відстеження рівнів заряду батареї, стану підключення та будь-яких потенційних проблем або несправностей. Користувачів слід попереджати про низький рівень заряду батареї або проблеми з підключенням, які можуть вплинути на ефективність платформи.

17. Ресурси підтримки та допомоги

Найкращі програми для систем безпеки розумного дому повинні містити ресурси підтримки та довідки, такі як поширені запитання, навчальні посібники, посібники з усунення несправностей або прямий контакт зі службою підтримки клієнтів. Це гарантує, що

користувачі зможуть легко знайти допомогу, якщо у них виникнуть будь-які проблеми або є запитання щодо програми чи їхньої системи безпеки.

Завдяки поєднанню цих основних функцій, програмне забезпечення для систем домашньої безпеки може забезпечити користувачам зручний та ефективний контроль над їхньою мережею інтелектуального захисту, забезпечуючи безперебійний та зручний користувацький досвід.

У найближчі роки технології розумного дому продовжуватимуть впливати на наше повсякденне життя. Інтелектуальні побутові пристрої, ймовірно, стануть ще більш взаємопов'язаними, що забезпечить безперебійну комунікацію між різними пристроями та платформами.

Асистенти та алгоритми на базі штучного інтелекту продовжуватимуть удосконалювати автоматизацію підключеного дому шляхом персоналізації, вивчення індивідуальних уподобань та адаптації до потреб мешканців.

Попит на автоматизацію розумного дому зростає, і для підприємців все ще існує багато невикористаних можливостей для впровадження нових та унікальних послуг з розробки розумного дому. Створюючи додаток для домашньої безпеки, компанії можуть представити свої інноваційні ідеї, задовольнити потреби конкретних клієнтів та виділитися серед конкурентів.

Ключові характеристики хмарної домашньої безпеки:

1. Віддалений доступ: домовласники можуть контролювати та керувати своїми системами безпеки з будь-якого місця за допомогою смартфонів, планшетів або комп'ютерів.
2. Масштабованість: ці системи можуть легко встановлювати додаткові пристрої та функції без значних змін у апаратному забезпеченні.
3. Інтеграція: Бездоганно інтегрується з іншими пристроями розумного дому, такими як освітлення, термостати та дверні замки.
4. Сповіщення в режимі реального часу: Забезпечує миттєві сповіщення про підозрілу активність, що дозволяє оперативно реагувати.
5. Економічно ефективний: часто доступніший за традиційні системи завдяки нижчим витратам на встановлення та обслуговування.

ВІoT

Система хмарного сервісу забезпечення безпеки розумного будинку реалізована з використанням функцій ВІoT.

З розвитком технологій концепція розумних будівель виходить на нові висоти завдяки інтеграції Інтернету речей у будівлях (ВІoT). Це наступне покоління автоматизації будівель використовує передові датчики, взаємопов'язані пристрої та складну аналітику даних для створення більш ефективних, адаптивних та зручних для користувача середовищ. У цій статті досліджується майбутнє ВІoT, його переваги, проблеми та трансформаційний вплив, який він має на те, як ми керуємо будівлями та взаємодіємо з ними.

Інтернет речей у будівництві (ВІoT) стосується інтеграції технології ІoT саме в контексті управління та автоматизації будівель. На відміну від традиційних систем автоматизації будівель, які працюють ізольовано, ВІoT створює цілісну, взаємопов'язану мережу пристроїв і датчиків, які взаємодіють у режимі реального часу. Така інтеграція дозволяє здійснювати комплексний моніторинг, керування та оптимізацію різних систем будівлі, включаючи опалення, вентиляцію та кондиціонування повітря, освітлення, безпеку тощо.

Роль передових датчиків та пристроїв Інтернету речей

Основою ВІoT є використання передових датчиків та пристроїв Інтернету речей. Ці датчики збирають величезні обсяги даних про різні аспекти продуктивності будівлі, такі як температура, вологість, заповнюваність та споживання енергії. Потім пристрої Інтернету речей передають ці дані до центральної системи, де їх можна проаналізувати та вжити заходів.

Наприклад, датчики присутності можуть виявляти присутність людей у кімнаті та відповідно регулювати освітлення й системи опалення, вентиляції та кондиціонування повітря для економії енергії. Датчики навколишнього середовища можуть контролювати якість повітря та запускати системи вентиляції для підтримки здорових умов у приміщенні. Завдяки постійному збору та аналізу даних, системи ВІоТ дозволяють будівлям працювати ефективніше та адаптуватися до потреб своїх мешканців у режимі реального часу.

Переваги ВІоТ:

1. Підвищена енергоефективність: системи ВІоТ оптимізують використання енергії, контролюючи та регулюючи системи освітлення, опалення та охолодження на основі заповненості приміщень та умов навколишнього середовища в режимі реального часу. Це призводить до значної економії енергії та зменшення викидів вуглецю.

2. Покращений комфорт та продуктивність мешканців: Створюючи адаптивне середовище, яке відповідає потребам та вподобанням мешканців, ВІоТ підвищує комфорт та продуктивність. Наприклад, системи освітлення можуть налаштовуватися відповідно до циклів природного освітлення, покращуючи самопочуття мешканців та зменшуючи втому.

3. Прогнозне обслуговування та скорочення часу простою: ВІоТ дозволяє проводити прогнозне обслуговування, постійно контролюючи стан систем будівлі та виявляючи потенційні проблеми до того, як вони призведуть до збоїв. Такий проактивний підхід мінімізує час простою та подовжує термін служби обладнання будівлі.

4. Комплексна аналітика даних: величезна кількість даних, зібраних системами ВІоТ, може бути проаналізована для отримання уявлення про продуктивність будівлі та виявлення можливостей для покращення. Розширена аналітика може виявляти закономірності та аномалії, допомагаючи керівникам об'єктів приймати обґрунтовані рішення та оптимізувати експлуатацію будівлі.

Незважаючи на численні переваги, впровадження ВІоТ не обходиться без труднощів. Однією з основних проблем є інтеграція різноманітних систем і пристроїв. Багато будівель мають застарілі системи, які можуть бути несумісними із сучасними технологіями Інтернету речей. Забезпечення безперебійної комунікації та сумісності між різними системами вимагає ретельного планування та інвестицій.

Безпека даних є ще однією критичною проблемою. Оскільки системи будівель стають більш взаємопов'язаними, вони також стають більш вразливими до кіберзагроз. Захист конфіденційних даних та забезпечення безпеки систем автоматизації будівель мають першочергове значення.

Крім того, початкові витрати на впровадження ВІоТ можуть бути високими. Хоча довгострокова економія та переваги часто виправдовують інвестиції, забезпечення необхідного фінансування та ресурсів може бути перешкодою для деяких організацій.

Майбутнє ВІоТ

Майбутнє ВІоТ виглядає багатообіцяючим, оскільки постійний розвиток технологій стимулює подальші інновації. Новітні технології, такі як 5G, периферійні обчислення та блокчейн, мають розширити можливості систем ВІоТ, забезпечуючи швидшу обробку даних, покращену безпеку та надійніше з'єднання.

Оскільки будівлі стають більш інтелектуальними та взаємопов'язаними, потенціал біотехнологій, що працюють в Інтернеті речей (ВІоТ), для трансформації забудованого середовища продовжуватиме зростати. Завдяки ВІоТ, керівники об'єктів можуть створювати розумніші, ефективніші та адаптивніші будівлі, які відповідають потребам мешканців та зацікавлених сторін, що постійно змінюються.

На завершення, інтеграція ВІоТ являє собою значний крок вперед в автоматизації будівель. Використовуючи можливості передових датчиків, пристроїв Інтернету речей та аналітики даних, ВІоТ створює цілісну та інтелектуальну систему управління будівлею, яка підвищує енергоефективність, комфорт мешканців та загальну продуктивність будівлі. Хоча проблеми залишаються, переваги ВІоТ роблять її переконливою та трансформаційною технологією для майбутнього розумних будівель.

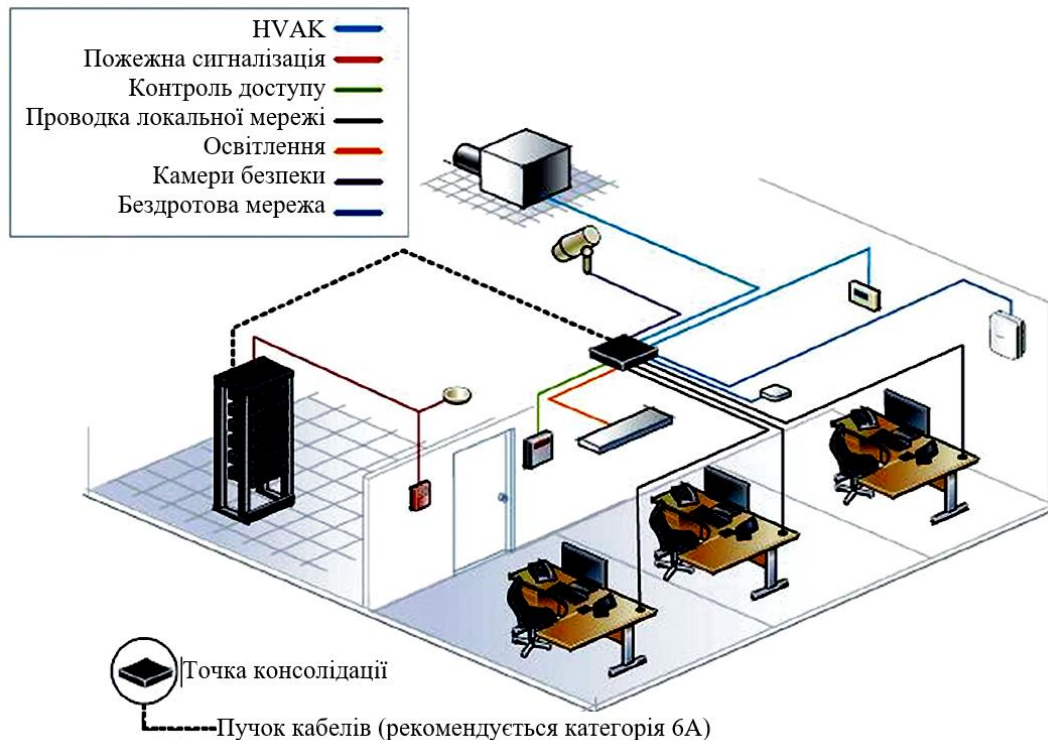


Рисунок 1 – Структурна схема системи

Висновки. У статті освіти наведені теоретичне узагальнення й рішення наукового завдання дослідження методів хмарного сервісу забезпечення безпеки розумного будинку. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем хмарного сервісу забезпечення безпеки розумного будинку.
- Досліджена система хмарного сервісу забезпечення безпеки розумного будинку.
- На основі отриманих результатів досліджень створена програмна реалізація системи хмарного сервісу забезпечення безпеки розумного будинку.

Розроблені алгоритми дозволяють успішно вирішувати завдання хмарного сервісу забезпечення безпеки розумного будинку. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Kuznetsov, O., Frontoni, E., Kuznetsova, K., Arnesano, M., Smirnov, O. «A secure biometric authentication architecture for blockchain-driven cyber-physical systems». Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications, 2025, pp. 193–224.
2. Kuznetsov, O., Atzeni, G., Arnesano, M., Randieri, C., Smirnov, O. «Secure IoT-based smart wheelchair system: From implementation to security enhancement strategy». Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications, 2025, pp. 225–257.
3. Kuznetsov, O., Smirnov, O., Kuznetsova, T., Shaikhanova, A., Svatowsky, I. «Privacy-utility trade-offs in IoT networks: A comparative analysis of differential privacy mechanisms for sensor data aggregation». Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications, 2025, pp. 589–622.
4. Вінтенко Б., Смірнов О., Миронець І., Смірнова Т., Смірнов С. «Імітаційна модель шляхів вхідних даних комп'ютерної інтелектуальної системи підтримки оператора енергоблоку АЕС». Комбінаторні конфігурації та їхні застосування: Матеріали XXVII Міжнародного науково-практичного семінару, присвяченого 125-річчю Національного університету «Запорізька політехніка» (Запоріжжя-Кропивницький-Київ, 4-6 червня 2025 р.). Запоріжжя: НУ «Запорізька політехніка», 2025. С.82-91.
5. Al-Azzeh, J., Ayyoub, B., Mesleh, A., Smirnova, T., Gnatyuk, S., Drieiev, O., Smirnov, O., Dorenskyi, O. «Cloud-Based Information System for Evaluating Caverns in the Process of Blasting Metal Surfaces of Details».

- International Review on Modelling and Simulations 18 (1), 2025. pp. 32-42.
6. Вінтенко Б.Ю., Смірнов О.А., Миронець І.В., Смірнова Т.В., Коваленко О.В., Мацуй А.М. «Модель шляхів отримання вхідних даних комп'ютерної інтелектуальної системи підтримки оперативного персоналу АЕС». Центральнотраїнський науковий вісник. Технічні науки. 2025. Вип. 11(42), ч. II. С.52-62.
 7. Вінтенко Б.Ю., Смірнов О.А., Миронець І.В., Смірнова Т.В. «Методи забезпечення відмовостійкості інтелектуальних систем підтримки оператора». VIII міжнародна науково-практична конференція «Інформаційна безпека та комп'ютерні технології», м. Кропивницький. 24-25 квітня 2025 р. – Кропивницький: ЦНТУ. – 2025. – С. 44-46.
 8. Вінтенко, Б., Миронець, І., Смірнов, О., Коваленко, А., Коноплицька-Слободенюк, О., Смірнова, Т., Константинова, Л. «Дослідження застосування систем підтримки оперативного персоналу об'єкту критичної інфраструктури при керуванні енергоблоком АЕС з реактором типу ВВЕР-1000». Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2024. № 2(26), С. 6-26.
 9. Смірнова Т.В., Коноплицька-Слободенюк О.К., Буравченко К.О., Смірнов С.А., Кравчук О.В., Козірова Н.Л., Смірнов О.А. «Дослідження технологій забезпечення кібербезпеки хмарних сервісів IaaS, PaaS та SaaS». Кібербезпека: освіта, наука, техніка. 2024. №4(24), С. 6-27.
 10. Вінтенко, Б., Миронець, І., Смірнов, О., Кравчук, О., Козірова, Н., Савеленко, Г., Коваленко, А. «Дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». Кібербезпека: освіта, наука, техніка. 2024. №3(23), С. 111-131.
 11. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». Advanced Information Systems, 2023, 7(2), pp. 49-56.
 12. Kuznetsov, O., Kuznetsova, Y., Smirnov, O., Kostenko, O., Zvieriev, V. «Evaluating Hashing Algorithms in the Age of ASIC Resistance». CEUR Workshop Proceedings, 2023, 3628, pp. 93-105.
 13. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchey, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». CEUR Workshop Proceedings, Volume 3530, 2023, pp. 256-265.
 14. Smirnov, O., Odarchenko, R., Smirnova, T., Bondar, S., Volosheniuk, D. «Optimal Structure Construction of Private 5G Network for the Needs of Enterprises». Lecture Notes on Data Engineering and Communications Technologies, 2023, 178, pp. 208–223.
 15. Вінтенко Б.Ю., Смірнов О.А., Коваленко А.С., Смірнов С.А., Буравченко К.О. «Дослідження вимог міжнародних стандартів IEC60880 та IEC62138 з розробки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». Системи управління, навігації та зв'язку, 2023, вип. 3(73), С. 155-166.
 16. Аль-Мудхафар Акіл Абдулхуссейн М., Смірнова Т.В., Буравченко К.О., Смірнов О.А. «Метод оцінки та підвищення користувальницького досвіду абонентів в програмно-конфігурованих мережах на основі використання машинного навчання». Сучасні інформаційні системи, 2023, том 7, № 2, С. 49-56.
 17. Smirnova, T., Gnatyuk, S., Yudin, O., Sydorenko, V., Polozhentsev, A., «The Model for Calculating the Quantitative Criteria for Assessing the Security Level of Information and Telecommunication Systems». CEUR Workshop Proceedings Volume 3156, 2022, Pages 390-399.
 18. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». Проблеми інформатизації та управління, № 2(70). 2022. С. 28-37.
 19. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 3(69). С. 93-98.
 20. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Вісник Хмельницького національного університету. Серія: «Технічні науки», № 2 (307). С. 46-52. 2022.
 21. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 1(67). С. 84-89.
 22. Smirnova T., Gnatyuk S., Berdibayev R., Avkurova Zh., Iavich M. «Cloud-Based Cyber Incidents Response System and Software Tools». Communications in Computer and Information Science, 2021, vol 1486. Springer, Cham. pp 169-184.
 23. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
 24. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». Journal of theoretical and applied information technology Vol.98. No 21, 2020, P. 3334-3346.
 25. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based

- pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177.
26. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587.
27. Smirnov, O., Markovets, O. Vovk, N., Turchyn, Y., «Model of informational support for social network administrators' content creation». CEUR Workshop Proceedings Volume 2616, 2020, Pages 125-136.
28. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». CEUR Workshop Proceedings Volume 2616, 2020, Pages 366-379.
29. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645.
30. Smirnov O. Kuznetsov A., Zaichenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019; Odessa; Ukraine; 9-13 September 2019. P.22-28.
31. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.
32. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019 . P.517-522.
33. Smirnov, O., Odarchenko, R., Abakumova, A., Usik, P., Kundyz, M., «QoE optimization technique for media delivery in 5G networks». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019. P.597-601.

УДК 004

Д.Нагірняк, магістр гр. КН-24М,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ІНТЕЛЕКТУАЛЬНОГО АРКАДНОГО МУЛЬТИМЕДІА ПРОЕКТУ НА ОСНОВІ ФРЕЙВОРКУ PHASER

У статті розроблено програмне забезпечення, яке призначено для системи інтелектуального аркадного мультимедіа проекту на основі фрейворку Phaser. Метою розробки є дослідження та принципи побудови системи інтелектуального аркадного мультимедіа проекту на основі фрейворку Phaser. Об'єктом дослідження є процес інтелектуального аркадного мультимедіа проекту на основі фрейворку Phaser. Предметом дослідження є методи інтелектуального аркадного мультимедіа проекту на основі фрейворку Phaser. Методи дослідження базуються на методах теорії обробки графічної інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи інтелектуального аркадного мультимедіа проекту на основі фрейворку Phaser. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

інтелектуальний аркадний мультимедіа проект, фрейворк Phaser

Постановка проблеми. Створення захопливих та неповторних ігрових вражень вимагає поєднання технічних навичок, креативності та глибокого розуміння психології гравця. Зі зростанням очікувань гравців та розвитком технологій розробники постійно розширюють межі можливостей, щоб запропонувати захопливий ігровий досвід. Цей динамічний ландшафт підкреслює зростання інновацій та розширення ігрової індустрії. В основі цієї трансформації лежать фреймворки та движки для розробки ігор, які надають необхідні інструменти та функції для втілення віртуальних світів у життя. Фреймворки для розробки ігор – це бібліотеки та платформи, що надають структурований набір ресурсів та інструментів для створення ігор на замовлення. Ці фреймворки спрощують процес розробки ігор, надаючи попередньо вбудовані функції, такі як фізичне моделювання, рендеринг графіки, управління звуком та керування вводом. Ці фреймворки дозволяють розробникам зосередитися на творчих аспектах гри для швидшої розробки та ефективнішого використання ресурсів.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи інтелектуального аркадного мультимедіа проекту на основі фрейворку PHASER.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи інтелектуального аркадного мультимедіа проекту на основі фрейворку Phaser.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем інтелектуального аркадного мультимедіа проекту на основі фрейворку Phaser.
- Дослідження системи інтелектуального аркадного мультимедіа проекту на основі фрейворку Phaser.
- Програмна реалізація системи інтелектуального аркадного мультимедіа проекту на основі фрейворку Phaser.

Об'єктом дослідження є процес інтелектуального аркадного мультимедіа проекту на основі фрейворку Phaser.

Предметом дослідження є методи інтелектуального аркадного мультимедіа проекту на основі фрейворку Phaser.

Методи дослідження базуються на методах теорії обробки графічної інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Аркадні ігри не зникли. Вони перетворилися на дизайнерську основу, яка продовжує формувати те, як будується цифрова взаємодія. Ранні машини змушували розробників зосереджуватися на швидкості, зрозумілості та реакції користувача. Обмежене обладнання та механіка оплати за гру призвели до ігор, які навчали гравців без інструкцій. Замість складних меню гравці навчалися на практиці.

Сьогоднішні студії часто застосовують принципи аркадних ігор, навіть не називаючи їх такими. Короткий ігровий цикл, зростання складності та зворотний зв'язок щодо винагороди досі є частиною найуспішніших продуктів. Дизайнери, які вивчають логіку аркадних ігор, розуміють, як утримувати увагу та залучати гравців. Погляд у минуле – це не ностальгія. Йдеться про використання перевірених методів, які працюють на сучасних платформах.

Незмінна привабливість фізичних ігрових просторів

Аркадні автомати досі привертають увагу, оскільки вони пропонують прямий та соціальний досвід. На відміну від домашніх консолей чи смартфонів, аркадні автомати вимагають від гравців діяти публічно. Таке середовище сприяє дружньому змагання та спільній грі. Діти, підлітки та дорослі часто збираються навколо автомата, щоб грати по черзі, порівнювати рахунки та реагувати разом. Навіть невеликі аркади в торгових центрах або розважальних центрах можуть генерувати довгі черги, коли автомати пропонують швидкий та корисний ігровий процес.

Фізичне керування також сприяє привабливості. Джойстик та набір кнопок із адаптивною реакцією дозволяють вводити дані, що відрізняються від сенсорного екрана. Мобільні аркадні ігри намагаються привнести подібну динаміку в смартфони, імітуючи темп і чіткість класичних ігор. Розробники часто створюють їх з простими правилами, короткими раундами та швидким зворотним зв'язком. Ці механіки відображають сильні сторони аркадних ігор і допомагають мобільним іграм досягати масштабного успіху. Незалежно від того, чи розміщені вони у фізичному кабінеті, чи завантажені з магазину додатків, ігри, що дотримуються цього формату, продовжують добре працювати.

Сучасна монетизація ретро-досвіду

Ностальгія повертає гравців, але ефективна монетизація забезпечує сталий розвиток продуктів. Багато студій зараз відтворюють або перевидають ігри в ретро-стилі, щоб залучити аудиторію, яка пам'ятає оригінали. Використовуючи сучасні движки, такі як Unity, розробники можуть створювати мобільні ігри, які виглядають класично, але працюють з високою стабільністю. Розробка мобільних ігор на Unity спрощує публікацію на кількох платформах, одночасно інтегруючи рекламні моделі, покупки в додатках та підписки.

Методи монетизації різняться, але одна поширена структура включає пропонування основного ігрового процесу безкоштовно з платними покращеннями візуальних елементів, бонусів або нового контенту. Графіка в ретро-стилі в поєднанні із сучасною монетизацією часто призводить до сильної залученості. Розробники, які розуміють, як збалансувати емоційну привабливість зі структурованою монетизацією, як правило, досягають кращих результатів на переповненому ринку.

Наприклад, деякі мобільні ігри, створені на Unity, використовують функції таблиці лідерів та щоденні винагороди для підвищення утримання користувачів. Інші відтворюють відомі механіки, такі як піксельні платформери або фіксовані шутери, пропонуючи їх у коротких сесіях, що відповідають сучасним звичкам користувачів. Однієї лише ностальгії не гарантує успіху. Дохід надходить від точного вибору дизайну в поєднанні з доступними бізнес-моделями.

Популярність аркадних відеоігор у 2025 році

Ігрова аудиторія у 2025 році все ще виявляє значний інтерес до аркадних відеоігор. Короткі сесії, високі бали та цикли повторів продовжують приваблювати гравців усіх вікових груп. Розробники, які розуміють структуру та простоту, часто швидше охоплюють ширшу аудиторію. Замість того, щоб прагнути складних наративів, ігри в стилі аркад надають гравцям пряму мету та негайний зворотний зв'язок.

Нові релізи в цьому жанрі з'являються як у вигляді інді-проектів, так і в каталогах великих видавців. Файтинги, шутери з кулями, ритмічні випробування та класичні перегони є одними з найпопулярніших ігор у магазинах та на онлайн-платформах. Багато творців зараз поєднують аркадну механіку з оновленою візуальною складовою або гібридними жанрами, пропонуючи ігри, які здаються одночасно знайомими та актуальними.

У світі жанрів відеоігор аркадні формати залишаються одними з найстабільніших. Гравці часто перемикаються між масштабними іграми з відкритим світом та короткими аркадними іграми залежно від вільного часу чи настрою. Ця гнучкість робить аркадні відеоігри актуальними, особливо коли вони представлені в сучасному стилі та мають орієнтовану на користувача взаємодію.

Визначення принципів дизайну аркадних ігор, які працюють

Потужний дизайн аркадних ігор зосереджений на швидкій взаємодії, видимих результатах та утриманні гравців. Розробники використовують короткі цикли, негайну реакцію та чіткість цілей, щоб зосередити увагу. На відміну від жанрів з насиченим сюжетом, аркадні ігри часто пропускають експозицію та одразу переходять до викликів та винагород. Елементи керування зазвичай мінімальні, тому немає потреби в інструкціях з експлуатації. Робоча структура дизайну в аркадних іграх часто добре застосовується до сучасних мобільних, консольних та браузерних ігор. При правильному застосуванні ці принципи створюють ігри, які легко освоїти та в які важко відірватися.

Швидкий зворотний зв'язок та щільні цикли

Розробники аркадних ігор працюють із короткими циклами, які спонукають гравців діяти швидко та бачити результати негайно. Цей цикл підвищує залученість, змушуючи кожну секунду відчувати себе корисною. Найкращі ігри в цій категорії усувають затримку між дією та відповіддю. Коли ви натискаєте кнопку, щось відбувається одразу. Цей зворотний зв'язок навчає механіці без письмових пояснень.

Сучасні розробники застосовують цю модель на мобільних, VR та ПК платформах. Ключ у циклі: діяти, спостерігати, що відбувається, покращувати, повторювати. Вузькі цикли також полегшують балансування. Дизайнери можуть точно налаштовувати швидкість, оцінювання та складність з меншим ризиком розриву довгих сюжетних ліній.

Ключові технології та платформи, що рухають сучасний дизайн аркадних ігор

Дизайн сучасних аркадних ігор залежить від поєднання передових двигунів, апаратного забезпечення та підключених сервісів. Розробники ігор використовують Unity, Unreal Engine та low-code інструменти для розробки як цифрових, так і кабінетних ігор. Мережеві функції, хмарне сховище та датчики розширюють можливості аркадної гри. На відміну від ранніх кабінетних ігор, обмежених апаратним забезпеченням, сучасні системи дозволяють грати в багатокористувацькому режимі, відстежувати рахунок у реальному часі та масштабовану доставку контенту. Вибір правильної платформи або налаштування обладнання залежить від цілей гри та фізичного середовища розгортання.

Рішення Unity, Unreal та Low-Code для шаф

Розробники ігор сьогодні часто обирають рушії, виходячи з необхідної гнучкості, вартості та простоти розгортання. Unity широко використовується для аркадних проектів завдяки своїй портативності та ефективній підтримці 2D та 3D. Багато комерційних ігрових рушіїв зараз запускають ігри, створені на Unity, на готових комп'ютерах на базі Windows. Unity також підтримує легку інтеграцію сенсорного екрана та надійний відгук вводу, що важливо для аркадної гри.

Двигун Unreal Engine частіше використовується у високоякісних ігрових враженнях. Хоча він вимагає більше системних ресурсів, Unreal підтримує розширені візуальні ефекти та складну логіку введення, що підходить для великоформатних аркадних дисплеїв або VR-кабін.

Лоукодові рішення тепер пропонують швидкі варіанти для простих аркадних ігор. Деякі команди використовують такі платформи, як Buildbox або GameMaker, для створення прототипів або швидкого запуску аркадних ігор.

1. Unity. Добре підходить для механіки в мобільному стилі, кросплатформної підтримки та швидкої ітерації.

2. Unreal Engine. Найкраще підходить для просунутої 3D-візуалізації, ігор з високим рівнем фізики та кінематографічних кабінетів.

3. Інструменти з низьким рівнем коду. Корисні для швидких циклів розробки, ігор, орієнтованих на навчання, або демонстрацій для підтвердження концепції.

Кожна платформа пропонує різні сильні сторони, залежно від цільового формату аркади.

Phaser Game Engine – це популярний фреймворк з відкритим кодом для створення 2D-ігор та інтерактивного досвіду. Побудований на технології HTML5, він надає потужний набір інструментів та функцій, що спрощують розробку ігор.

Що таке ігровий двигун Phaser?

Phaser – це швидкий та легкий фреймворк для розробки ігор, спеціально розроблений для створення 2D-ігор. Він підтримує рендеринг як WebGL, так і Canvas, що забезпечує сумісність з широким спектром пристроїв. Phaser має високі можливості налаштування та розширення. Це один з найкращих ігрових рушіїв для розробників усіх рівнів кваліфікації.

Кому варто використовувати ігровий движок Phaser?

Фазер ідеально підходить для:

- Розробники ігор: Phaser пропонує зручний API та розширену документацію.
- Незалежні розробники: безкоштовність, відкритий код та масштабованість Phaser приваблюють невеликі команди та незалежних творців.
- Професіонали: Студії можуть використовувати Phaser для швидкого прототипування та створення ігор на різних платформах.

Залежно від потреб та вимог, Phaser може бути підходящим фреймворком для багатьох команд розробників ігор.

Переваги ігрового двигуна Phaser

- Відкритий код та безкоштовний: Phaser знаходиться у вільному доступі, а активна спільнота робить внесок у його розробку та підтримку.
- Підтримка кросплатформності: ігри, створені за допомогою Phaser, можуть працювати у веббраузерах, настільних комп'ютерах та мобільних пристроях.
- Розширена документація: Вичерпні посібники, навчальні посібники та приклади роблять навчання та використання Phaser простим.
- Гнучкість рендерингу: Розробники можуть вибирати між WebGL та Canvas, оптимізуючи ігри для різних пристроїв та потреб у продуктивності.
- Багата екосистема плагінів: Різноманітні плагіни розширюють можливості Phaser, від фізичних двигунів до розширеної анімації.

Ігровий двигун Phaser та Incredibuild

Incredibuild покращує ігровий движок Phaser, пришвидшуючи процес збірки та розгортання. Розподіляючи обчислювальні завдання між кількома машинами, Incredibuild скорочує час збірки ресурсів та коду.

Однією з головних переваг фреймворку є його простота використання, і це, ймовірно, одна з причин, чому він набрав такої популярності за такий короткий проміжок часу (фреймворку трохи більше року).

Фактично, Phaser абстрагує всю складну математику, яка зазвичай потрібна для створення гри, надаючи вам більше, ніж просто ігрові компоненти. Це дозволяє вам пропустити частину, яку ви витрачаєте на роздуми про те, як можна реалізувати певну спеціальну функцію та який рівень обчислення вона вимагає.

Як працює Phaser.js?

Ігри Phaser розробляються з використанням об'єкта конфігурації гри, який визначає такі властивості, як розміри, тип рендерингу, налаштування фізики та сцени. Кожна сцена має три основні методи життєвого циклу.

- preload(): Завантажує такі ресурси, як зображення та звуки.
- create(): Ініціалізує об'єкти та логіку гри.
- update(): Виконується безперервно для обробки логіки гри та взаємодії з користувачем.

Порівняння з іншими ігровими двигунами

– Phaser проти Cocos2d-x: Cocos2d-x підтримує розробку як 2D, так і 3D ігор і є кросплатформним. Однак, зосередженість Phaser на HTML5 робить його дуже придатним для швидкої ітерації.

– Phaser проти Unity 2D: Unity пропонує потужні інструменти для розробки як 2D, так і 3D ігор, забезпечуючи розширену підтримку редакторів та платформ. Phaser, з іншого боку, легший та простий у вивченні, що робить його ідеальним для розробників, які зосереджені на веб-іграх.

– Phaser проти Three.js: Хоча Three.js використовується для створення анімованої 3D-графіки у веб-браузерах, Phaser зосереджений на розробці 2D-ігор, що робить його кращим для браузерних ігор з насиченим 2D-контентом.

Структурна схема розробленої системи зображена на рисунку 1. На ній показано структуру розробленої системи інтелектуального аркадного мультимедіа проекту на основі фрейворку Phaser. Вона включає в себе:

- Двигун Phaser.js.
- Блок функцій Phaser.js.
- Блок застосувань.
- Блок введення даних.

Блок функцій Phaser.js

Phaser пропонує широкий спектр функцій, які роблять розробку ігор дуже простою та плавною.

– Багаті фізичні системи: Phaser підтримує кілька фізичних движків, таких як Arcade Physics, Matter.js та ImpactJS, які надають розробникам інструменти для виявлення зіткнень, гравітації, прискорення тощо.

– Керування сценами та станами: Phaser пропонує керування сценами та станами, що спрощує створення меню, ігрових рівнів та переходів.

– Завантаження ресурсів: Phaser спрощує керування ресурсами завдяки вбудованим завантажувачам ресурсів для зображень, аудіо, відео, спрайтів, тайлмеп тощо.

– Анімація: Створення анімації в Phaser стає дуже простим завдяки вбудованій підтримці спрайтових аркушів та анімації на основі кадрів.

– Обробка вводу користувача: Phaser підтримує різноманітні методи введення, включаючи клавіатуру, мишу, сенсорне керування та навіть ігрові контролери.

– Керування аудіо: Phaser забезпечує вбудовану підтримку відтворення аудіо, включаючи звукові ефекти, музику та аудіопетлі.

– Керування камерою та вікном перегляду: Система камер Phaser дозволяє контролювати видиму область гри, забезпечуючи функції прокручування, масштабування та обертання.

– Тайлмапи: Завдяки підтримці рівнів на основі тайлмепів ви можете швидко створювати величезні ігрові світи та структуровані рівні.

– Вбудовані ігрові об'єкти: Phaser надає вбудовані об'єкти, такі як спрайти, текстові об'єкти, кнопки, графіка та фігури. Це зменшує необхідність створювати ігрові компоненти з нуля.

Блок застосувань

Блок застосувань включає в себе:

– Казуальні веб-ігри: Phaser ідеально підходить для створення браузерних ігор завдяки легкій конструкції та сумісності з браузерами.

– Освітні ігри: Цей фреймворк часто використовується для розробки освітніх ігор для дітей завдяки своїй простоті та інтерактивним можливостям.

– Розробка мобільних ігор: Завдяки функціям, адаптованим для мобільних пристроїв, легко розробляти кросплатформні мобільні ігри з підтримкою сенсорного керування та акселерометра.

– Прототипи та MVP: Розробники часто використовують Phaser для швидкого створення прототипів та мінімально життєздатних продуктів (MVP).

– Ігрові зустрічі: Завдяки швидкому циклу розробки, Phaser є популярним вибором для ігрових зустрічей та заходів зі швидкого прототипування.

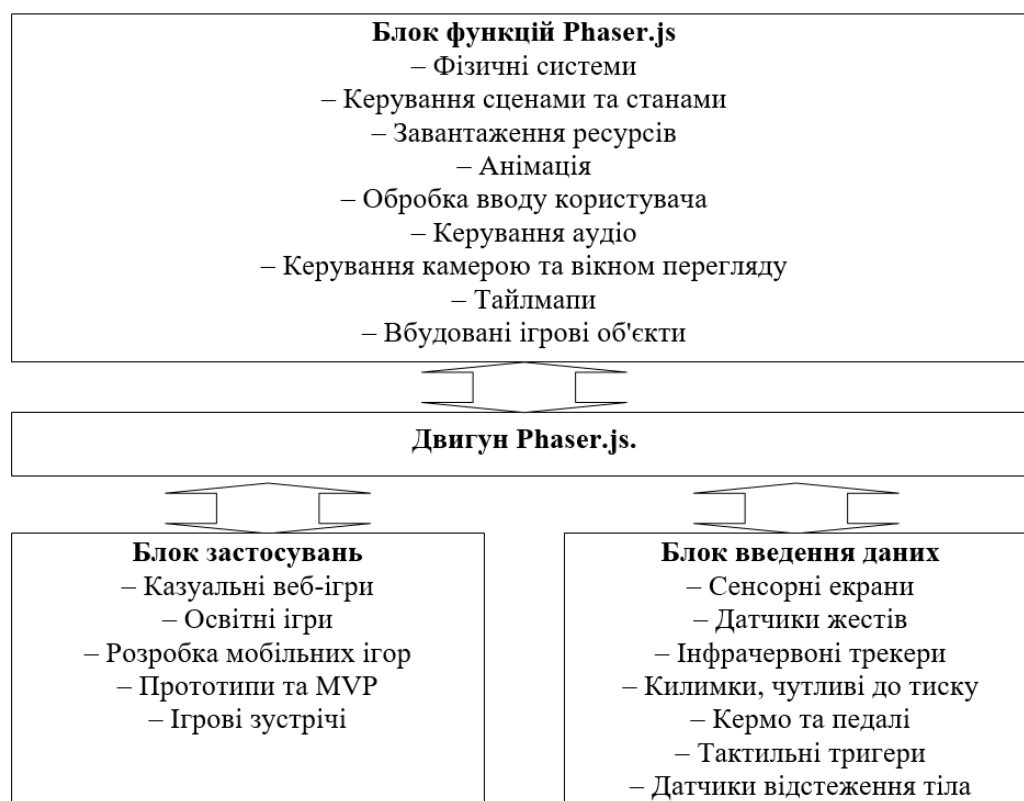


Рисунок 1 – Структурна схема системи

Блок введення даних

Сенсорні екрани, сенсори та альтернативні входи. Сучасні ігрові автомати використовують більше, ніж просто кнопки та джойстики. Розробники тепер створюють ігри, які використовують сенсорні екрани, датчики руху та натискні панелі для підтримки нових типів взаємодії. Цей зсув відкриває простір для дизайну ритм-ігор, ігор, орієнтованих на фітнес, або захопливих тренувань.

Сенсорні екрани поширені в іграх на основі квитків та мобільних портах, адаптованих для кабінетів. Їхня низька крива навчання робить їх ідеальними для коротких публічних ігор.

Датчики жестів, такі як Leap Motion або інфрачервоні трекери, додають цінності інтерактивним музейним експозиціям або фітнес-додаткам.

Альтернативні засоби введення виходять за рамки дотику:

1. Килимки, чутливі до тиску. Використовуються в танцювальних іграх або ігрових залах для фізичної реабілітації.

2. Кермо та педалі. Застосовується в гоночних іграх для додаткового реалізму.

3. Тактильні тригери. Забезпечують зворотний зв'язок у стрілялках або екшн-іграх.

4. Датчики відстеження тіла. Дозволяють грати всім тілом без носимих пристроїв.

Використання різноманітних вхідних даних дозволяє розробникам охоплювати нових гравців, адаптуватися до доступності та підтримувати ширший спектр фізичних просторів.

Тенденції розробки ігор на 2025 рік і далі

Якщо ви зайшли так далеко, вам може бути цікаво дізнатися про тенденції розробки ігор, які змінять та трансформуватимуть ігрову індустрію в найближчі роки.

Нижче ми перерахували тенденції, які допоможуть вам охопити більше людей і збільшити ваш дохід.

1. Захоплюючі ігри

Імерсивні ігри покращують розширену реальність (XR), поєднуючи віртуальну реальність, доповнену реальність та змішану реальність для забезпечення розширеного ігрового досвіду.

Завдяки захопливим іграм ми рухаємося до більш реалістичних ігор. Поєднуючи реалістичну графіку та високоякісний звуковий дизайн, розробники тепер готові втілити в життя ігрових персонажів та сюжети, дозволяючи гравцям глибше зануритися в гру.

З розвитком технологій та їхньою доступністю, захопливий ігровий досвід приваблюватиме ширшу аудиторію, стимулюючи подальші інновації в ігровій індустрії.

Кросплатформний геймплей: Ігровий ландшафт зазнає значних змін у 2025 році та надалі зі зростанням поширеності кросплатформної розробки ігор.

Зростаюча кількість розробників забезпечують безперебійну гру для гравців на різних платформах, таких як Xbox, PlayStation, ПК та мобільних пристроях. Цей зсув знаменує собою занепад ексклюзивних для платформ багатокористувацьких режимів, що дозволяє гравцям грати з родиною та друзями на різних пристроях.

Не тільки це, це також дозволяє іграм перемикатися між платформами, зберігаючи свій прогрес, зберігаючи свої серії незмінними, щоб їх не довелося починати спочатку.

2. Хмарні ігри

Зростання популярності хмарних ігор набирає обертів як серед гравців, так і серед розробників, завдяки віддаленим серверам. Хоча хмарні ігри існують вже деякий час, акцент змістився на те, щоб зробити їх більш доступними та захопливими за допомогою передових технологій.

Завдяки таким сервісам, як NVIDIA GeForce NOW та Xbox Cloud Gaming, гравці тепер мають можливість насолоджуватися іграми найвищого рівня практично на будь-якому пристрої. Ця інновація руйнує бар'єри та сприяє розвитку активних, пов'язаних ігрових спільнот.

3. Штучний інтелект та машинне навчання

Штучний інтелект (ШІ) та машинне навчання (МН) трансформують відеоігри, покращуючи занурення та взаємодію. Очікується, що в найближчі кілька років неіграбельні персонажі (NPC) вийдуть за рамки сценарної поведінки, адаптуючись до стратегій гравців та навчаючись на їхніх діях.

Ми також можемо передбачити процедурно згенерований контент, який розвиватиметься в режимі реального часу, дозволяючи ігровим середовищам та сюжетним лініям змінюватися залежно від вибору гравця.

Це створить персоналізовані наративи, поглиблюючи зв'язок гравців зі світом гри та його персонажами. Загалом, інтеграція штучного інтелекту та машинного навчання призведе до більш динамічного ігрового досвіду з високою реграбельністю, оскільки кожна сесія

пропонує унікальні завдання та історії, адаптовані до індивідуальних стилів гри. Майбутнє ігор виглядає інтерактивним та високо персоналізованим.

4. Реалістична графіка

Удосконалення ігрової графіки стрімко розвивається, і інтеграція технології трасування променів відіграє значну роль у цьому прогресі. У майбутньому ми можемо очікувати, що ігри демонструватимуть ще більш захоплюючі та реалістичні візуальні ефекти.

Технологія трасування променів імітує поведінку світла в реальному світі, створюючи неймовірно реалістичні відблиски, тіні та світлові ефекти. Це вдосконалення обіцяє перетворити ігровий досвід на кінематографічні пригоди.

Для тих, хто цінує ігри з сюжетом та приголомшливою візуальною складовою, потенційний вплив трасування променів на естетичну якість ігор є особливо захопливим, оскільки це, ймовірно, підніме загальну графічну точність до безпрецедентного рівня.

Вартість розробки ігор

Вартість розробки гри може суттєво варіюватися, починаючи приблизно від 35 000 доларів США до понад 600 000 доларів США. На цю велику різницю у вартості розробки впливає багато факторів, які впливають на загальну складність та обсяг проекту.

Прості 2D-ігри з обмеженим функціоналом часто мають менші витрати, тоді як 3D-ігри з насиченим сюжетом та складними механізмами вимагають вищого бюджету.

Деякими іншими факторами, що впливають на цей спектр витрат, є розмір та кваліфікація команди розробників, їхнє географічне розташування, жанр гри, обрана графіка та стиль малювання, час розробки, використані інструменти та технології, платформа, для якої розробляється гра, інтеграції (наприклад, покупки в додатку або підтримка багатокористувацької гри), залежності від сервісів або програмного забезпечення, звуковий дизайн, дизайн інтерфейсу користувача та вибір платформ та движків розробки.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів інтелектуального аркадного мультимедіа проекту на основі фрейворку Phaser. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем інтелектуального аркадного мультимедіа проекту на основі фрейворку Phaser.
- Досліджена система інтелектуального аркадного мультимедіа проекту на основі фрейворку Phaser.
- На основі отриманих результатів досліджень створена програмна реалізація системи інтелектуального аркадного мультимедіа проекту на основі фрейворку Phaser.

Розроблені алгоритми дозволяють успішно вирішувати завдання інтелектуального аркадного мультимедіа проекту на основі фрейворку Phaser. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Kuznetsov O., Frontoni E., Kuznetsova Y., Chevardin V., Smirnov O. «Architectural foundations for adaptive security in edge computing systems». *Cybersecurity Defensive Walls in Edge Computing*, 2025. pp. 21-61.
2. Вінтенко, Б.Ю., Миронець, І.В., Смірнов, О.А., Коваленко, О.В., Усік, П.С., Буравченко, К.О., Лисенко, І.А. «Логіко-структурна модель комп'ютерно-орієнтованої процедури системи підтримки оперативного персоналу АЕС». *Кібербезпека: освіта, наука, техніка*. 2025. Том 2 № 30. С. 413-427, 2025.
3. Смірнова, Т.В. «Дослідження методів, моделей та сучасних ІТ-рішень для підтримки технологічних процесів у критичній інфраструктурі держави». *Кібербезпека: освіта, наука, техніка*. 2025. Том 2 № 30. С.195-208, 2025.
4. Вінтенко Б., Смірнов О., Миронець І., Смірнова Т., Смірнов С. «Імітаційна модель шляхів вхідних даних комп'ютерної інтелектуальної системи підтримки оператора енергоблоку АЕС». *Комбінаторні конфігурації та їхні застосування: Матеріали XXVII Міжнародного науково-практичного семінару, присвяченого 125-річчю Національного університету «Запорізька політехніка» (Запоріжжя-Кропивницький-Київ, 4-6 червня 2025 р.)*. Запоріжжя: НУ «Запорізька політехніка», 2025. С.82-91.

5. Al-Azzeh, J., Ayyoub, B., Mesleh, A., Smirnova, T., Gnatyuk, S., Drieiev, O., Smirnov, O., Dorenskyi, O. «Cloud-Based Information System for Evaluating Caverns in the Process of Blasting Metal Surfaces of Details». *International Review on Modelling and Simulations* 18 (1), 2025. pp. 32-42.
6. Вінтенко Б.Ю., Смірнов О.А., Миронець І.В., Смірнова Т.В., Коваленко О.В., Мацуй А.М. «Модель шляхів отримання вхідних даних комп'ютерної інтелектуальної системи підтримки оперативного персоналу АЕС». *Центральноукраїнський науковий вісник. Технічні науки*. 2025. Вип. 11(42), ч. II. С.52-62.
7. Вінтенко Б.Ю., Смірнов О.А., Миронець І.В., Смірнова Т.В. «Методи забезпечення відмовостійкості інтелектуальних систем підтримки оператора». VIII міжнародна науково-практична конференція «Інформаційна безпека та комп'ютерні технології», м. Кропивницький. 24-25 квітня 2025 р. – Кропивницький: ЦНТУ. – С. 44-46.
8. Смірнов, О.А., Константинова, Л.В., Коноплицька-Слободенюк, О.К., Козірова, Н.В., Якименко, Н.М., Доренський, О.П., Буравченко, К.О. «Дослідження інструментів штучного інтелекту для роботи з базами даних та аналізу даних». *Кібербезпека: освіта, наука, техніка*. 2025. №3(27), С. 429–448.)
9. Smirnov O., Fedorov E., Neskoriadiya A., Neskoriadiya T. «Intellectual Classification method of Gymnastic Elements Based on Combinations of Descriptive and Generative Approache». *CEUR Workshop Proceedings Volume 3664*, 2024, Pages 11-23.
10. Вінтенко, Б., Миронець, І., Смірнов, О., Коваленко, А., Коноплицька-Слободенюк, О., Смірнова, Т., Константинова, Л. «Дослідження застосування систем підтримки оперативного персоналу об'єкту критичної інфраструктури при керуванні енергоблоком АЕС з реактором типу ВВЕР-1000». *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2024. № 2(26), С. 6-26.
11. Вінтенко, Б., Миронець, І., Смірнов, О., Кравчук, О., Козірова, Н., Савеленко, Г., Коваленко, А. «Дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». *Кібербезпека: освіта, наука, техніка*. 2024. №3(23), С. 111-131.
12. Kuznetsov O., Ilchenko O., Kryvinska N., Buravchenko K., Smirnov O., Savchenko Iu. «An Empirical Assessment of Leading Blockchain Financial Services». 2023 IEEE 1st Ukrainian Distributed Ledger Technology Forum (UADLTF), Kyiv, Ukraine, 2023, pp. 1-6,
13. Kuznetsov, O., Kryvinska, N., Ilchenko, O., Smirnova, T., Ulianovska, Y. «Comparative Analysis of Cryptocurrency Trading Platforms Using the Analytic Hierarchy Process». *CEUR Workshop Proceedings*, 2023, 3628, pp. 106-115.
14. Malyukov V., Bebesko B., Lakhno V., Smirnov O., Malyukova I., Mohylnyi H. «Managing the Purchase-Sale Process of Digital Currencies Under Fuzzy Conditions». *Lecture Notes in Networks and Systems*, 2023, 729 LNNS, pp. 104–112.
15. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». *Advanced Information Systems*, 2023, 7(2), pp. 49-56.
16. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchey, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». *CEUR Workshop Proceedings, Volume 3530*, 2023, pp. 256-265.
17. Smirnov, O., Odarchenko, R., Smirnova, T., Bondar, S., Volosheniuk, D. «Optimal Structure Construction of Private 5G Network for the Needs of Enterprises». *Lecture Notes on Data Engineering and Communications Technologies*, 2023, 178, pp. 208–223.
18. Вінтенко Б.Ю., Смірнов О.А., Коваленко А.С., Смірнов С.А., Буравченко К.О. «Дослідження вимог міжнародних стандартів IEC60880 та IEC62138 з розробки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». *Системи управління, навігації та зв'язку*, 2023, вип. 3(73), С. 155-166.
19. Вінтенко, Б., Миронець, І., Смірнов, О., Кравчук, О., Козірова, Н., Савеленко, Г., Коваленко, А. «Дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». *Кібербезпека: освіта, наука, техніка*. 2024. №3(23), С. 111-131.
20. Вінтенко Б.Ю., Смірнов О.А., Коваленко О.В., Смірнов С.А., Коваленко А.С. «Дослідження нормативних документів та галузевих стандартів розробки програмного забезпечення комп'ютерних систем управління АЕС, важливих для безпеки». *Системи управління, навігації та зв'язку*, 2023, вип. 2(72), С. 170-178.
21. Аль-Мудхафар Акіл Абдулхуссейн М., Смірнова Т.В., Буравченко К.О., Смірнов О.А. «Метод оцінки та підвищення користувальницького досвіду абонентів в програмно-конфігурованих мережах на основі використання машинного навчання». *Сучасні інформаційні системи*, 2023, том 7, № 2, С. 49-56.
22. Вінтенко Б.Ю., Смірнов О.А., Коваленко О.В., Смірнов С.А. «Дослідження нормативної документації та стандартів розробки програмного забезпечення комп'ютерних систем управління АЕС, важливих для безпеки». VI міжнародна науково-практична конференція «Інформаційна безпека та комп'ютерні технології», м. Кропивницький. 20-21 квітня 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 35-36.
23. Smirnov, O., Karapetyan, A., Fedorov, E., «Creating Neural Network and Single Solution Human-Based Metaheuristic Methods of Solving the Traveling Salesman Problem». *CEUR Workshop Proceedings, Volume 3312*, 2022, pp. 47-58.
24. Smirnov O., Kuznetsov A., Kryvinska N., Kiian A., Kuznetsova K. «Full Non-Binary Constant-Weight Codes». *SN Computer Science*, Vol 2, 337, 2021. <https://doi.org/10.1007/s42979-021-00739-w>.

25. Smirnov O., Kovalenko O., Kovalenko A., Kavun S. «Quantitative Risk Assessment Method Development in the Context of the SDLC-model». 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), 2021, pp. 203-208, doi: 10.1109/PICST54195.2021.9772143
26. Smirnova T., Gnatyuk S., Berdibayev R., Avkurova Zh., Iavich M. «Cloud-Based Cyber Incidents Response System and Software Tools». Communications in Computer and Information Science, 2021, vol 1486. Springer, Cham. pp 169-184.
27. Smirnov, O., Kuznetsov, A., Potii, O., Poluyanenko, N., Stelnyk, I., Mialkovsky, D. «Combining and filtering functions in the framework of nonlinear-feedback shift register». International Journal of Computing; 2020, Volume 19, Issue 2 – Research Institute for Intelligent Computer Systems – 2020. – P. 247-256.
28. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
29. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177.
30. Smirnov, O., Shekhanin, K., Kuznetsov, A., Krasnobayev, V. «Detecting Hidden Information in FAT». International Journal of Computer Network and Information Security (IJCNIS). Vol. 12, No. 3, 2020. PP.33-43.
31. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645.
32. Smirnov O. Kuznetsov A., Zaichenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019; Odessa; Ukraine; 9-13 September 2019. P.22-28.
33. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.
34. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019 . P.517-522.

УДК 004

А.Норов, магістр гр. КІ-24М,

Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ІОТ З ВИКОРИСТАННЯМ BLUETOOTH

У статті розроблено програмне забезпечення, яке призначено для системи ІоТ з використанням Bluetooth 6. Метою розробки є дослідження та принципи побудови системи ІоТ з використанням Bluetooth 6. Об'єктом дослідження є процес ІоТ з використанням Bluetooth 6. Предметом дослідження є методи ІоТ з використанням Bluetooth 6. Методи дослідження базуються на методах Інтернету речей, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи ІоТ з використанням Bluetooth 6. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

ІоТ, Bluetooth 6

Постановка проблеми. Інтернет речей (ІоТ) зазнав значного зростання за останні роки, а Bluetooth Low Energy (BLE) став ключовим засобом забезпечення низькоенергетичного та недорогого бездротового зв'язку. У рамках даного проекту зробимо огляд еволюції технології Bluetooth, зосереджуючись на ролі BLE в екосистемі ІоТ. Розглянемо поточний стан BLE, включаючи його застосування, проблеми, обмеження та останні досягнення в таких галузях, як безпека, управління живленням та mesh-мережі. Нещодавній випуск Bluetooth Low Energy версії 6.0 від Bluetooth Special Interest Group (SIG) підкреслює постійну еволюцію технології та зростаючу важливість в ІоТ. Однак цей швидкий розвиток висвітлює прогалину в сучасній літературі, відсутність комплексних, актуальних оглядів, які б повністю відображали сучасний ландшафт BLE в додатках ІоТ. У роботі проаналізуємо нові тенденції та майбутні напрямки розвитку BLE, включаючи інтеграцію штучного інтелекту, машинного навчання та аудіоможливостей. В аналізі також розглянемо узгодженість функцій BLE з Цілями сталого розвитку Організації Об'єднаних Націй (ЦСР), зокрема енергоефективністю, сталими містами та діями щодо зміни клімату. Розглядаючи розробку та впровадження технології BLE, ця робота має на меті надати уявлення про можливості та проблеми, пов'язані з її впровадженням у різних застосуваннях Інтернету речей, від розумних будинків та міст до промислової автоматизації та охорони здоров'я. Дана робота підкреслює значення еволюції BLE у формуванні майбутнього бездротового зв'язку та Інтернету речей, а також забезпечує основу для подальших досліджень та інновацій у цій галузі.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи ІОТ з використанням Bluetooth.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи ІоТ з використанням Bluetooth 6.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем ІоТ з використанням Bluetooth 6.
 - Дослідження системи ІоТ з використанням Bluetooth 6.
 - Програмна реалізація системи ІоТ з використанням Bluetooth 6.
- Об'єктом дослідження є процес ІоТ з використанням Bluetooth 6.*
Предметом дослідження є методи ІоТ з використанням Bluetooth 6.

Методи дослідження базуються на методах Інтернету речей, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Можливо, Bluetooth Low Energy – це технологія, яка «запустила» Інтернет речей. Проблема «класичного» Bluetooth полягала в тому, що він потребував постійного з'єднання, що, своєю чергою, означало досить обмежений час роботи від акумулятора, а отже, пристрої з живленням від акумулятора потребували частішої підзарядки. Це також обмежувало випадки використання, для яких його можна було легко розгорнути.

Технологія Bluetooth Low Energy вирішила ці проблеми, переводячи пристрої в режим сну між передачами, зберігаючи при цьому їхнє з'єднання. Вона також дозволяє легко здійснювати ad-hoc сполучення. Поряд з різними іншими технічними вдосконаленнями, це дозволило розгорнути велику кількість пристроїв з низьким енергоспоживанням, які обмінюються відносно невеликими обсягами даних, але водночас значно розширюють широке підключення.

Досі тенденція розвитку Wi-Fi була в іншому напрямку – в основному зосереджена на дедалі вищих швидкостях передачі даних, що дозволяють потокову передачу контенту високої чіткості та задоволення потреб «хмарних» обчислень. Споживання енергії не було головним фактором, як і питання спектру, які також не були головним занепокоєнням. Цільовим ринком була відносно невелика кількість великих потужних пристроїв, що передають багато даних.

Можна сказати, що Wi-Fi був як кувалда, а Bluetooth Low Energy – як скальпель – різні інструменти для різних завдань.

Нові розробки Bluetooth

Однак, нові розробки в обох технологіях починають спрямовувати їх у збіжних напрямках. Що стосується Bluetooth, швидкість передачі даних збільшилася з версією 4.2, а версія 5.2 представила можливості потокової передачі аудіо разом із новим кодеком. Це не зовсім відео високої чіткості, але це віддаляє Bluetooth Low Energy від його коріння, заснованого на даних Інтернету речей.

Wi-Fi 6 пропонує нові можливості

Що стосується Wi-Fi, то Wi-Fi 6 – це розробка, спрямована безпосередньо на покращення можливостей Wi-Fi для рішень Інтернету речей. Як згадувалося вище, попередні версії Wi-Fi були зосереджені на швидкості. Цього було досягнуто завдяки широкосмуговим каналам. Зворотний бік полягає в тому, що їх не може бути багато в обмеженому спектрі, виділеному для вільного використання. Це не має великого значення, якщо один чи два користувачі транслюють потокове відео з домашнього маршрутизатора, але, як знає кожен, хто користувався публічним Wi-Fi у жвавому районі, мережі можуть легко перенасичуватися.

Таким чином, Wi-Fi 6 запозичує кілька хитрощів зі світу стільникового зв'язку та розділяє спектр на піднесучі, що дозволяє більшій кількості користувачів передавати дані одночасно, хоча й з нижчою швидкістю передачі даних. Їх можна використовувати досить гнучко, тому різним користувачам може бути виділена різна кількість одиниць ресурсів протягом одного періоду часу, залежно від потреби.

Подальшим удосконаленням є реалізація «Цільового часу пробудження», завдяки якому пристрої можуть запитувати повторне пробудження після певного інтервалу часу та переходити в режим сну між ними. Це значною мірою спрямовано на зниження мінімального рівня споживання енергії, необхідного для пристрою Wi-Fi.

Для подальшого розширення можливостей Wi-Fi в щільних середовищах, антени MiMo включені на обох кінцях з'єднання, що дозволяє спільний доступ до мережі в просторі. Додаткові функції дозволяють ігнорувати мережі, що перекриваються, зі слабким сигналом.

Кросовер

Усе це міцно просуває Wi-Fi у сферу Інтернету речей – щільні мережі, гнучке використання даних, можливість використання обмежених обсягів даних пристроями з

живленням від батарей – все це дуже схоже на заяву, яку Bluetooth Low Energy зробив 10 років тому.

Bluetooth Low Energy та WiFi 6 – конкуренти?

Тож що ж це все разом дає? Чи є ці технології тепер «конкурентами», де одна «переможе», а інша «програє».

Не зовсім, я думаю. Очевидно, що є певний рух разом. Обидва більш чітко, ніж будь-коли, спрямовані на різноманітні програми Інтернету речей. Однак залишаються суттєві відмінності – Bluetooth Low Energy все ще пропонує набагато кращі характеристики низького енергоспоживання, ніж WiFi 6, а можливості швидкості передачі даних WiFi все ще значно перевершують Bluetooth. Технологія перебудови частоти Bluetooth все ще виявиться більш стійкою в шумному середовищі, а ad-hoc підключення все ще буде простішим за допомогою Bluetooth.

Можливо, краще було б сказати, що це конвергенція. Програми Інтернету речей стають все більш складними, і часто однієї радіотехнології недостатньо. Зворотним боком досягнень WiFi 6 є те, що маршрутизатор має стати ще складнішим пристроєм, ніж будь-коли, керуючи більшою кількістю з'єднань з різними вимогами. Стандарт домашньої автоматизації MATTER є гарним прикладом спроби керувати різними радіостандартами під одним дахом. Цей стандарт може передбачати використання WiFi для обміну великими обсягами даних та Bluetooth для локального налаштування пристроїв.

Примітно, що Nordic Semiconductor, лідер ринку Bluetooth Low energy, нещодавно випустив свій перший WiFi-пристрій. Тож можна очікувати, що незабаром з'явиться кілька пристроїв з подвійним радіозв'язком, які підтримуватимуть останнє покоління обох технологій.

Вибір для системних розробників

Для розробників систем, ймовірно, це буде не стільки питання вибору одного чи іншого, скільки в багатьох випадках питання того, які системні функції повинні використовувати яку бездротову технологію.

Можна провести аналогію з еволюцією мобільних телефонів – спочатку вони мали лише підключення до стільникової мережі, а з часом перетворилися на мультирадіопристрої, які ми носимо з собою сьогодні. Інтернет речей (IoT) розвивається тим самим шляхом, починаючи, як правило, з простого точка-точка з'єднання від пристрою до чогось, що діє як шлюз. Зараз у нас є багато різних архітектур рішень, включаючи мультирадіо, mesh-мережі, мережі для великих і малих відстаней та різні інші варіанти.

Суть у тому, що обидві технології додають можливості, і це просто робить більше речей можливими. Жодна з них навряд чи зникне в найближчому майбутньому.

Основна мета цього розділу – надати комплексний огляд еволюції технології Bluetooth, з особливим акцентом на BLE та її ключову роль в екосистемі Інтернету речей. Це включає відстеження розвитку технології Bluetooth від її зародження до сучасного стану, висвітлюючи ключові віхи та технологічні досягнення. Воно має на меті запропонувати детальний аналіз технічних характеристик, функцій та вдосконалень BLE порівняно з традиційною технологією Bluetooth. Крім того, воно визначає технічні проблеми, пов'язані з впровадженням BLE в Інтернеті речей, та досліджує рішення, розроблені для вирішення цих проблем. Нарешті, в опитуванні обговорюються нові тенденції та потенційні майбутні досягнення в технології BLE та її вплив на Інтернет речей. Дарруді та Гомес надали ранній огляд мереж BLE mesh, технології, яка з того часу стала вирішальною для масштабного розгортання Інтернету речей [3]. Зовсім недавно Наттуанатан та ін. дослідили сучасний стан BLE mesh, її застосування та міркування щодо впровадження [4]. Розуміння еволюції BLE в екосистемі Інтернету речей є критично важливим з кількох причин. Воно надає уявлення про те, як розвивалися технології бездротового зв'язку, що призвело до появи більш ефективних рішень з низьким енергоспоживанням, необхідних для пристроїв Інтернету речей. Роль BLE в Інтернеті речей підкреслює його значення у забезпеченні безперебійного, надійного та енергоефективного підключення між широким спектром пристроїв, від носимих

технологій до систем розумного дому. Комплексне опитування служить цінним ресурсом для дослідників, розробників та фахівців галузі, надаючи консолідовану базу знань, тим самим сприяючи прийняттю обґрунтованих рішень та стратегічному плануванню. Розуміння сучасних тенденцій та потенційних майбутніх напрямків BLE та Інтернету речей допомагає передбачити майбутні ринкові потреби та технологічні зрушення, гарантуючи, що поточні та майбутні рішення залишатимуться актуальними та ефективними. Висновки, отримані в результаті цього опитування, можуть бути корисними для багатьох дисциплін, окрім Інтернету речей, таких як охорона здоров'я, автомобільна промисловість та промислова автоматизація, де технологія BLE все частіше впроваджується. Хоча BLE стала домінуючою технологією в малопотужному зв'язку з низьким енергоспоживанням, важливо розглядати її в рамках ширшої екосистеми технологій, що забезпечують Інтернет речей. Раза та ін. [5] надали огляд малопотужних мереж широкого радіусу дії (LPWAN), які доповнюють BLE у сценаріях, що вимагають зв'язку на великі відстані. Оскільки BLE продовжує розвиватися та глибше інтегруватися в екосистеми Інтернету речей, виникатимуть нові виклики, особливо в сферах безпеки та конфіденційності. Цуй та ін. [6] висвітлили ці виклики в контексті розумних міст, області, де пристрої Інтернету речей з підтримкою BLE стають дедалі поширенішими. Вирішення цих проблем безпеки та конфіденційності матиме вирішальне значення для подальшого зростання та прийняття BLE в критичних додатках Інтернету речей.

На питання, яка система розумного дому вам підходить, не можна відповісти універсально, оскільки багато що залежить від вашої індивідуальної життєвої ситуації та потреб. Тому перше питання має бути таким: чи хочете ви модернізувати або модернізувати існуючу нерухомість, чи побудувати нову?

Існуючі будівлі можна легко та економічно ефективно модернізувати за допомогою систем голосового керування або бездротових рішень, що дозволяє розумно керувати окремими пристроями, такими як термостати опалення. Однак важливо зазначити, що витрати можуть швидко зростати при використанні різних окремих рішень, які можуть мати обмежений зв'язок один з одним. Бездротові системи використовують такі технології, як Wi-Fi або Bluetooth, або протоколи, такі як ZigBee або Z-Wave, для підключення різних зон або пристроїв у будинку. Модернізація існуючої нерухомості до шинного стандарту, такого як KNX, може стати складним проектом, що включає модифікацію стін та прокладання кабелів, але вона пропонує різні переваги, які ми розглянемо детальніше пізніше. Як варіант, для старих будівель є варіантом KNX-RF – бездротовий варіант шинної системи KNX, де керування розумними пристроями відбувається бездротово через діапазон частот 868 МГц, без необхідності структурних змін.

Перш ніж розпочинати проект модернізації, важливо з'ясувати, чи існують якісь нормативні обмеження, такі як вимоги щодо охорони спадщини, або чи потрібно консультуватися з орендодавцями для отримання дозволів на орендовану нерухомість.

Під час планування нового будівництва може бути доцільним прокласти кабелі, готові до шинної системи, з самого початку. Це дозволяє створити розгалужену мережу для сприяння інтелектуальному зв'язку між пристроями. Зазвичай ці кабелі прокладаються під час будівництва будівлі, що усуває необхідність подальшої модифікації стін.

Ролети, освітлення, побутова техніка, розваги чи системи безпеки – усе це можна взаємопов'язати, керувати індивідуально та налаштувати відповідно до ваших потреб. Сервер служить центральним вузлом, обмінюючись даними з елементами керування, такими як планшети, смартфони, сенсорні панелі або голосові помічники. Можливості різноманітні, і ви вирішуєте, які аспекти вашого дому ви хочете зробити розумними або інтелектуальними.

Якщо ви хочете лише автоматично вмикати або вимикати світло або опалення регулювати його самостійно, вам може не знадобитися повноцінна система домашньої автоматизації спочатку. Розумних розеток або вимикачів з дистанційним керуванням або без нього, або розумного термостата з дистанційним керуванням чи додатком може бути достатньо, щоб позначити ваш житловий простір як «розумний». Пристрої в розумних

будинках або квартирах зазвичай контролюються за допомогою інтернет-технологій, таких як мобільний додаток або голосові системи, такі як Amazon Alexa або Google Assistant. Однак побоювання щодо безпеки даних є поширеними.

Щойно пристрої або групи пристроїв об'єднані для забезпечення більшого комфорту, безпеки та енергоефективності вдома, і ви створюєте складніші розпорядки дня, ваше житлове середовище справді стає розумним. Наприклад, розумний будинок може автоматично знижувати температуру, коли нікого немає вдома, або піднімати сонцезахисні жалюзі та зовнішні віконниці, коли датчики виявляють сильний вітер. Управління енергією також стало важливим питанням, оскільки розумні будівлі, підключені до шинної системи, забезпечують самозабезпечення шляхом інтеграції опалення, фотоелектричних систем та настінних коробок з власноруч генерованою енергією для зниження витрат на енергію. Мережеве об'єднання та керування в інтелектуальних будівлях зазвичай здійснюється через сервер, а для візуалізації можна використовувати планшети або панелі керування. Однак є також постачальники, такі як PEAКnх, які поєднують сервери та панелі, причому панель керування діє як незалежний центр розумного дому.

Порівняння систем розумного дому

Багато систем розумного дому, представлених на ринку, мають схожий обсяг та роботу, а також підтримують деякі поширені пристрої. Однак є й помітні відмінності. Щоб допомогти вам зорієнтуватися на шляху до розумного дому, ми склали короткий огляд деяких систем розумного дому.

У процесі планування задайте собі такі питання:

1. Які пристрої та зони будуть підключені до системи розумного дому?

2. Які функції він повинен мати, і як вони повинні контролюватися?

3. Ви хочете створити логіку та процедури?

4. Наскільки ви хочете взяти на себе зобов'язання чи залишатися гнучкими? Чи повинна система бути розширюваною в майбутньому?

Також пам'ятайте, що в процесі планування у вас є вибір між:

— закриті системи з продукцією від одного виробника;

— частково відкриті системи для використання сумісних продуктів сторонніх виробників;

— відкриті системи, які можна вільно комбінувати як з продуктами певних виробників, так і з продуктами сторонніх виробників.

Якщо ви прагнете мати складну розумну будівлю з передовою домашньою автоматизацією, варто використовувати систему шин розумного дому. Шина являє собою лінію передачі даних, через яку інформація передається між взаємопов'язаними пристроями. Система шин забезпечує інтелектуальне з'єднання в межах кімнати або по всій будівлі.

Незалежно від того, яку систему шини розумного дому ви зрештою оберете, планування має бути комплексним та добре продуманим. Ви також можете прочитати нашу публікацію в блозі про те, як спланувати розумний будинок. Для початкового встановлення системи вам зазвичай потрібен системний інтегратор. Цей експерт знайомий зі специфічними методами встановлення кабелів, може виконати встановлення та налаштування системи, а також створити план встановлення, який включає всі компоненти, їх розміщення та місця розташування трубопроводів.

Вартість розумного дому не може бути універсально визначеною. Інформація станом на жовтень 2025 року показала, що витрати на систему розумного дому залежать від описаних систем та їхнього обсягу, дизайну та матеріалів, а також від використовуваних компонентів та їх функцій.

Залежно від розміру житлового простору, типу та обсягу обладнання, вартість «розумного будинку» може коливатися від двозначних сум у євро за окремі продукти, через пакети початкового рівня з кількома компонентами в тризначному діапазоні, до п'ятизначних сум у євро за повністю автоматизований та професійно встановлений

«розумного будинку», включаючи сенсорні панелі. Верхньої межі немає, а ціна зростає разом із комфортом, можливостями енергозбереження та функціями безпеки, які забезпечує система.

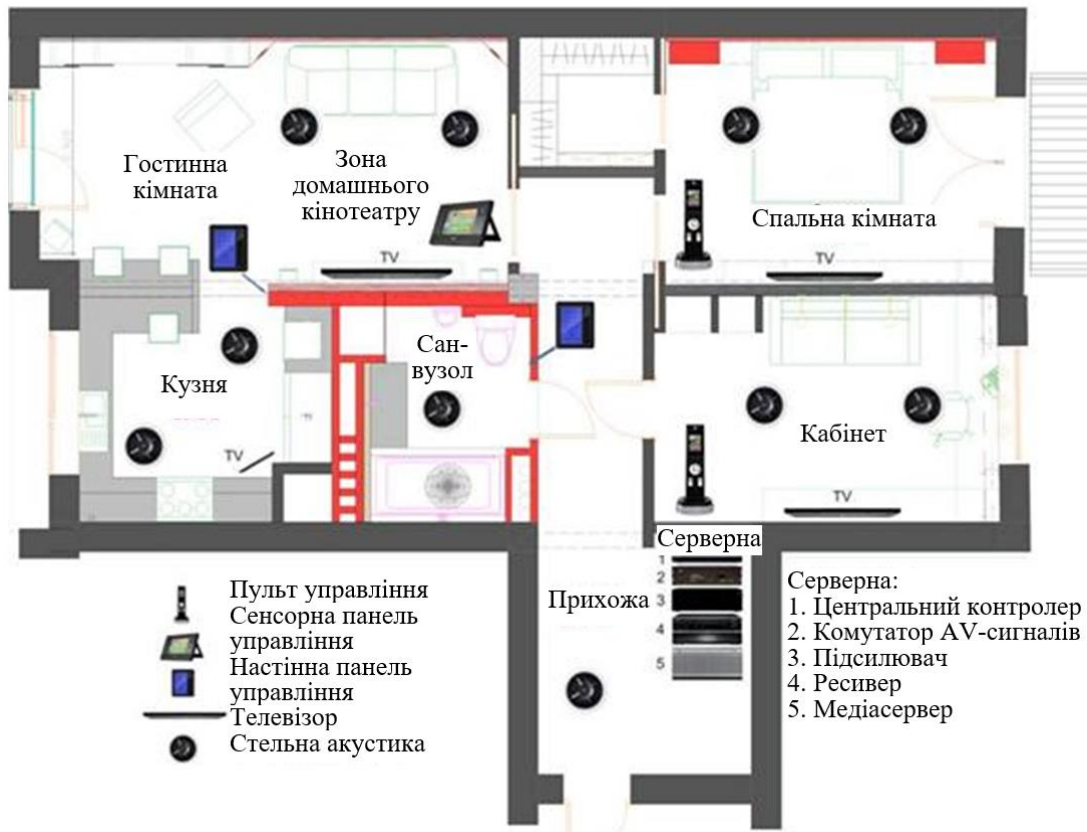


Рисунок 1 – Структурна схема системи

Бажано мати бюджетний план, заздалегідь зібрати інформацію про варіанти та провести порівняння витрат і вигод.

Системи розумного дому пропонують численні варіанти для безпечного, енергоефективного дому та комфортного повсякденного життя. Завдяки ретельному плануванню та врахуванню згаданих питань ви можете бути добре підготовлені до майбутнього розумного життя. Однак, не існує універсальної «найкращої» системи розумного дому; остаточне рішення залежить від індивідуальних життєвих ситуацій, потреб та бюджету.

Для деяких може бути доцільним використання індивідуальних або бездротових рішень. Серед систем розумного дому, запатентовані закриті системи зазвичай вважаються найбезпечнішими.

Для тих, хто бажає комплексної автоматизації з гнучкістю, безпекою та орієнтованим на майбутнє мережею пристроїв, варто розглянути системи розумного дому на основі шини. Системи для повної автоматизації будівель зазвичай мають високі стандарти безпеки.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів IoT з використанням Bluetooth 6. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем IoT з використанням Bluetooth 6.
- Досліджена система IoT з використанням Bluetooth 6.
- На основі отриманих результатів досліджень створена програмна реалізація системи IoT з використанням Bluetooth 6.

Розроблені алгоритми дозволяють успішно вирішувати завдання IoT з використанням Bluetooth 6. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія

яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Kuznetsov, O., Atzeni, G., Arnesano, M., Randieri, C., Smirnov, O. «Secure IoT-based smart wheelchair system: From implementation to security enhancement strategy». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 225–257.
2. Kuznetsov, O., Smirnov, O., Kuznetsova, T., Shaikhanova, A., Svatowsky, I. «Privacy-utility trade-offs in IoT networks: A comparative analysis of differential privacy mechanisms for sensor data aggregation». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 589–622.
3. Вінтенко Б., Смірнов О., Миронець І., Смірнова Т., Смірнов С. «Імітаційна модель шляхів вхідних даних комп'ютерної інтелектуальної системи підтримки оператора енергоблоку АЕС». Комбінаторні конфігурації та їхні застосування: Матеріали XXVII Міжнародного науково-практичного семінару, присвяченого 125-річчю Національного університету «Запорізька політехніка» (Запоріжжя-Кропивницький-Київ, 4-6 червня 2025 р.). Запоріжжя: НУ «Запорізька політехніка», 2025. С.82-91.
4. Al-Azzeh, J., Ayyoub, B., Mesleh, A., Smirnova, T., Gnatyuk, S., Drieiev, O., Smirnov, O., Dorenskyi, O. «Cloud-Based Information System for Evaluating Caverns in the Process of Blasting Metal Surfaces of Details». *International Review on Modelling and Simulations* 18 (1), 2025. pp. 32-42.
5. Вінтенко Б.Ю., Смірнов О.А., Миронець І.В., Смірнова Т.В., Коваленко О.В., Мацуй А.М. «Модель шляхів отримання вхідних даних комп'ютерної інтелектуальної системи підтримки оперативного персоналу АЕС». *Центральноукраїнський науковий вісник. Технічні науки*. 2025. Вип. 11(42), ч. II. С.52-62.
6. Вінтенко Б.Ю., Смірнов О.А., Миронець І.В., Смірнова Т.В. «Методи забезпечення відмовостійкості інтелектуальних систем підтримки оператора». VIII міжнародна науково-практична конференція «Інформаційна безпека та комп'ютерні технології», м. Кропивницький. 24-25 квітня 2025 р. – Кропивницький: ЦНТУ. – 2025. – С. 44-46.
7. Вінтенко, Б., Миронець, І., Смірнов, О., Коваленко, А., Коноплицька-Слободенюк, О., Смірнова, Т., Константинова, Л. «Дослідження застосування систем підтримки оперативного персоналу об'єкту критичної інфраструктури при керуванні енергоблоком АЕС з реактором типу ВВЕР-1000». *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2024. № 2(26), С. 6-26.
8. Смірнова Т.В., Коноплицька-Слободенюк О.К., Буравченко К.О., Смірнов С.А., Кравчук О.В., Козірова Н.Л., Смірнов О.А. «Дослідження технологій забезпечення кібербезпеки хмарних сервісів IaaS, PaaS та SaaS». *Кібербезпека: освіта, наука, техніка*. 2024. №4(24), С. 6-27.
9. Вінтенко, Б., Миронець, І., Смірнов, О., Кравчук, О., Козірова, Н., Савеленко, Г., Коваленко, А. «Дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». *Кібербезпека: освіта, наука, техніка*. 2024. №3(23), С. 111-131.
10. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». *Advanced Information Systems*, 2023, 7(2), pp. 49-56.
11. Kuznetsov, O., Kuznetsova, Y., Smirnov, O., Kostenko, O., Zvieriev, V. «Evaluating Hashing Algorithms in the Age of ASIC Resistance». *CEUR Workshop Proceedings*, 2023, 3628, pp. 93-105.
12. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchey, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». *CEUR Workshop Proceedings*, Volume 3530, 2023, pp. 256-265.
13. Smirnov, O., Odarchenko, R., Smirnova, T., Bondar, S., Volosheniuk, D. «Optimal Structure Construction of Private 5G Network for the Needs of Enterprises». *Lecture Notes on Data Engineering and Communications Technologies*, 2023, 178, pp. 208–223.
14. Вінтенко Б.Ю., Смірнов О.А., Коваленко А.С., Смірнов С.А., Буравченко К.О. «Дослідження вимог міжнародних стандартів IEC60880 та IEC62138 з розробки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». *Системи управління, навігації та зв'язку*, 2023, вип. 3(73), С. 155-166.
15. Аль-Мудхафар Акіл Абдулхуссейн М., Смірнова Т.В., Буравченко К.О., Смірнов О.А. «Метод оцінки та підвищення користувальницького досвіду абонентів в програмно-конфігурованих мережах на основі використання машинного навчання». *Сучасні інформаційні системи*, 2023, том 7, № 2, С. 49-56.
16. Smirnova, T., Gnatyuk, S., Yudin, O., Sydorenko, V., Polozhentsev, A., «The Model for Calculating the Quantitative Criteria for Assessing the Security Level of Information and Telecommunication Systems». *CEUR Workshop Proceedings Volume 3156*, 2022, Pages 390-399.
17. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». *Проблеми інформатизації та управління*, № 2(70). 2022. С. 28-37.
18. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля

криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 3(69). С. 93-98.

19. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Вісник Хмельницького національного університету. Серія: «Технічні науки», № 2 (307). С. 46-52. 2022.
20. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 1(67). С. 84-89.
21. Smirnova T., Gnatyuk S., Berdibayev R., Avkurova Zh., Iavich M. «Cloud-Based Cyber Incidents Response System and Software Tools». Communications in Computer and Information Science, 2021, vol 1486. Springer, Cham. pp 169-184.
22. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
23. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». Journal of theoretical and applied information technology Vol.98. No 21, 2020, P. 3334-3346.
24. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177.
25. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587.
26. Smirnov, O., Markovets, O. Vovk, N., Turchyn, Y., «Model of informational support for social network administrators' content creation». CEUR Workshop Proceedings Volume 2616, 2020, Pages 125-136.
27. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». CEUR Workshop Proceedings Volume 2616, 2020, Pages 366-379.
28. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645.
29. Smirnov O. Kuznetsov A., Zaichenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019; Odessa; Ukraine; 9-13 September 2019. P.22-28.
30. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.
31. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019 . P.517-522.

УДК 004

С.Олексієнко, магістр гр. КН-24М,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ КОМПЛЕКСНИХ ІНТЕЛЕКТУАЛЬНИХ РІШЕНЬ ДЛЯ ВІДЕОНАГЛЯДУ

У статті розроблено програмне забезпечення, яке призначено для системи комплексних інтелектуальних рішень для відеонагляду. Метою розробки є дослідження та принципи побудови системи комплексних інтелектуальних рішень для відеонагляду. Об'єктом дослідження є процес комплексних інтелектуальних рішень для відеонагляду. Предметом дослідження є методи комплексних інтелектуальних рішень для відеонагляду. Методи дослідження базуються на методах розпізнавання образів, методах великих даних, методах комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи комплексних інтелектуальних рішень для відеонагляду. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

інтелектуальне рішення, відеонагляд

Постановка проблеми. У кожній галузі платформи відеоспостереження стали важливими інструментами для забезпечення безпеки, моніторингу активів та підвищення операційної ефективності. Нещодавні технологічні досягнення збільшили попит на інтелектуальні, масштабовані та хмарні рішення для спостереження. Багато організацій зараз переходять на платформи на базі штучного інтелекту, які пропонують розширені можливості, такі як розпізнавання облич, виявлення об'єктів та складна аналітика даних. Новіші системи покращують виявлення загроз, прискорюють час реагування та мінімізують людські помилки завдяки автоматизації. Вибір нової платформи відеоспостереження являє собою значну інвестицію, яка має наслідки для організаційної безпеки та бізнес-аналітики. Індустрія відеоспостереження постійно розвивається, а штучний інтелект та хмарні обчислення відіграють вирішальну роль у сучасних рішеннях безпеки. Незалежно від того, чи шукаєте ви повністю хмарну систему на базі штучного інтелекту, чи простіше локальне рішення, варіанти відеонагляду задовольняють будь-які потреби безпеки. Вибір правильної платформи залежить від ваших конкретних вимог, бюджету та рівня інтеграції, який ви шукаєте для своєї інфраструктури спостереження.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи комплексних інтелектуальних рішень для відеонагляду.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи комплексних інтелектуальних рішень для відеонагляду.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем комплексних інтелектуальних рішень для відеонагляду.
- Дослідження системи комплексних інтелектуальних рішень для відеонагляду.
- Програмна реалізація системи комплексних інтелектуальних рішень для відеонагляду.

Об'єктом дослідження є процес комплексних інтелектуальних рішень для відеонагляду.

Предметом дослідження є методи комплексних інтелектуальних рішень для відеонагляду.

Методи дослідження базуються на методах розпізнавання образів, методах великих даних, методах комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Більшість систем безпеки містять камери відеоспостереження, які допомагають службам безпеки виявляти потенційні загрози. Однак, чим більшою та складнішою стає установка, тим складніше може бути забезпечити належне спостереження за всіма активними камерами та потоками спостереження.

З появою інтелектуальних технологій, таких як штучний інтелект та машинне навчання, сучасні системи спостереження можна запрограмувати на автоматичне виявлення аномальних подій та сигналів безпеки, що допомагає командам зосередити свої зусилля на подіях, що розгортаються, та питаннях негайної важливості.

Це основна передумова відеоаналітики. Ця передова технологія може самостійно аналізувати відеоконтент та отримувати з нього корисну інформацію для покращення прийняття рішень та підвищення ефективності реагування систем безпеки. Щоб дізнатися більше про практичні можливості аналітики відеоспостереження, нижче наведено повний посібник із застосування, можливостей та варіантів використання відеоаналітики.

Відеоаналітика – це передова технологія, яка автоматично аналізує контент, записаний відеокамерами. Інтелектуальні алгоритми обробляють відеодані в режимі реального часу, щоб генерувати інформацію про те, що відбувається, у серії зображень. Відеоаналітика для безпеки зазвичай використовується для виявлення та отримання інформації про рух об'єктів, людей та транспортних засобів на записах відеоспостереження.

Системи відеоаналітики спостереження пропонують більш практичний та ефективний спосіб перегляду та спостереження за записами з камер спостереження. Контент, знятий кількома камерами протягом кількох днів, може бути автоматично сортований за інтересами, допомагаючи співробітникам служби безпеки виявляти підозрілу активність та належним чином реагувати на неї в режимі реального часу та під час розслідувань.

Системи відеоаналітики обробляють відеопотоки за допомогою алгоритмів, розроблених для виявлення певних подразників. Захоплені зображення послідовно переглядаються спеціалізованими програмними інструментами, запрограмованими на перевірку певних подій або об'єктів, які можуть становити загрозу безпеці.

У простому сенсі, відеоаналітика шукає аномальні відмінності в послідовності зображень, а потім генерує дані про ці події за допомогою алгоритмів на основі правил. Наприклад, якщо відеокамера фіксує об'єкт, що рухається в її полі зору, відеоаналітика ставить запитання, щоб допомогти визначити об'єкт і вирішити, чи заслуговує його присутність на подальші дії.

Під поняттям відеоаналітики слід розуміти два основні типи систем:

– Традиційна відеоаналітика: Базові системи використовують алгоритми на основі правил для аналізу відеоконтенту. Якщо щось у серії зображень змінюється, програмне забезпечення задасть низку запитань типу «*якщо/тоді*», щоб звузити коло можливої зміни. Однак традиційні системи аналітики не можуть зберігати інформацію або навчатися на основі раніше зареєстрованих інцидентів.

– Відеоаналітика на основі штучного інтелекту: Відеоаналітика на основі штучного інтелекту також використовує процес на основі правил для отримання інформації про зображення. Однак їхні алгоритми використовують інструменти штучного інтелекту та машинного навчання, щоб навчатися на основі ширших даних. Простіше кажучи, глибоке навчання у відеоаналітиці дозволяє системам вивчати закономірності з історичних подій для підвищення точності виявлення.

Поширені типи відеоаналітики в системах відеоспостереження

Відеоаналітика в режимі реального часу дозволяє службам безпеки виявляти закономірності, аномальні події та підозрілу активність, які в іншому випадку могли б залишитися непоміченими. Камери відеоаналітики забезпечують постійне спостереження за

ключовими зонами, а різні алгоритми відеоаналітики спеціально розроблені для пошуку певних подразників. Нижче наведено деякі поширені типи аналітики.

Автоматичне розпізнавання номерних знаків (ALPR)

Камери ALPR використовують спеціальний тип відеоаналітики, який називається оптичним розпізнаванням символів (OCR), для зчитування інформації про номерні знаки транспортних засобів, що проїжджають повз. Технологію ALPR можна використовувати для підтримки операцій управління паркуванням та контролю доступу транспортних засобів, а також для спостереження за під'їзними дорогами та паркувальними зонами, щоб виявити наявність підозрілих транспортних засобів.

Виявлення натовпу

Алгоритми відеоаналітики, що використовуються для виявлення натовпу, запрограмовані на ідентифікацію людей та вимірювання щільності натовпу в полі зору камери. Аналітика виявлення натовпу використовується для підвищення безпеки на живих заходах, попередження команд про потенційні вузькі місця та порушення, які можуть потребувати додаткової уваги, а також для відстеження рівня заповненості та виявлення незвичайної активності.

Розпізнавання обличчя

Розпізнавання обличчя використовується для ідентифікації присутності людських облич у відеоконтенті, а також для порівняння облич з тими, що зберігаються в базах даних. Цей тип відеоаналітики може контролювати доступ до безпечних місць та покращувати безпеку периметра, попереджаючи команди про присутність відомих правопорушників та сторонніх осіб, які перебувають навколо приватних володінь.

Підрахунок людей

Системи відстеження людей аналізують різні типи біометричних показників, щоб краще зрозуміти дії людей у цільових зонах. Завдяки розпізнаванню обличчя, виявленню руху та поведінкових характеристик ці системи можуть ідентифікувати осіб та стежити за ними в приміщеннях, щоб покращити методи виявлення вторгнень та управління зайнятістю.

Відстеження об'єктів

Відеоаналітика для відстеження об'єктів контролює наявність та рух певних предметів у полі зору камери. Алгоритми можна налаштувати відповідно до різних випадків використання відеоаналітики. Наприклад, камери можуть бути запрограмовані для моніторингу посилок під час їхнього переміщення через пункти доставки та виконання замовлень або використовуватися для відстеження автомобілів для підтримки операцій з контролю дорожнього руху.

Виявлення руху

Алгоритми відеоаналітики, оптимізовані для виявлення руху, запрограмовані на безперервний пошук ознак руху в заданій області. Для цієї мети зазвичай використовується аналітика відеоспостереження з машинним навчанням. Системи можна навчити розуміти, як простори використовуються за нормальних умов, тому вони попереджають охоронців лише про рухи, які можуть становити проблему.

Виявлення предметів без нагляду

Системи відеоаналітики можна запрограмувати на моніторинг появи та руху статичних об'єктів у визначеному місці. Ці рішення добре впроваджуються в громадських місцях, таких як торгові центри, розважальні заклади та транспортні вузли, щоб допомогти співробітникам служби безпеки виявляти потенційні бомби та забезпечувати вільні аварійні виходи від перешкод.

Моніторинг зайнятості

Інструменти моніторингу заповнюваності підраховують кількість людей, які проходять через заздалегідь визначену зону протягом встановленого періоду часу. Цю технологію можна використовувати для забезпечення підтримки безпечного рівня заповнюваності та для збору даних про те, як використовуються приміщення. Наприклад, у

роздрібній торгівлі її можна використовувати для визначення того, коли послуги є найбільш популярними, та для вимірювання ефективності організаційних планів.

Переваги технології відеоаналітики

Вибір розробки та впровадження індивідуальних рішень для відеоаналітики може надати бізнесу та фахівцям з безпеки кілька суттєвих переваг. Завдяки інтелектуальному програмному забезпеченню, яке використовується для ефективного управління та отримання аналітичних даних з величезних обсягів, команди людей можуть покращити виконання ключових завдань, автоматично виділяючи високоякісну та релевантну аналітику.

1. Підвищена ефективність

Типова система безпеки містить багато IP-камер та моніторів, розташованих для охоплення ключових зон. Навіть найменша зміна в сигналі безпеки може свідчити про загрозу, що розгортається, але командам може бути важко ефективно спостерігати за всіма камерами безперервно.

Системи відеоаналітики безпеки можна навчити автоматично виявляти аномальні події та попереджати операторів про них, надсилаючи інформацію персоналу диспетчерської відеоспостереження та персоналу на місці через SMS або електронну пошту. Це допомагає забезпечити доведення до відома відповідного персоналу всіх підозрілих дій, а високоякісні записи подій миттєво генеруються для покращення розслідувань.

2. Покращене прийняття рішень

Поряд з виявленням аномальних подій, які можуть вимагати подальшого розслідування, системи відеоаналітики можуть розпізнати тип інциденту, який може розгорнутися. Завдяки ключовим типам відеоаналітики, таким як інструменти відстеження об'єктів та розпізнавання облич, персонал може бути попереджений про наявність вогнепальної зброї, сторонніх осіб або скупчення людей, що сприятиме обґрунтованому реагуванню на інциденти.

3. Зменшення кількості хибних тривог

Хоча традиційні системи безпеки можуть бути ефективними засобами стримування злочинів, оператори або центральні станції моніторингу повинні проводити додатковий аналіз, щоб зрозуміти причини активації. За оцінками, від 95% до 98% спрацьованих сигналів тривоги про крадіжку, паніку та пограбування є хибнопозитивними, що потенційно призводить до втрати часу та ресурсів, що може зробити організації вразливими до ширших ризиків.

Оскільки системи відеоаналітики безпеки розроблені для ідентифікації та розуміння конкретних подразників в унікальних умовах їхнього конкретного середовища, ризик хибних тривог можна суттєво зменшити. Це дозволяє персоналу швидко реагувати на ризики та скорочує час, витрачений на аналіз даних фізичної безпеки, щоб персонал міг зосередитися на важливих завданнях.

4. Потенційна економія коштів

Хоча початкові витрати на розробку систем відеоаналітики можуть бути високими, компанії, які впроваджують ці інструменти, можуть отримати довгострокову економію коштів. Перш за все, підвищена точність систем безпеки відеоаналітики може допомогти обмежити фінансовий вплив таких подій, як крадіжка та пошкодження майна, а додаткові переваги можна знайти в організаційних покращеннях.

Для аналізу, організації та реагування на дані безпеки знадобиться менше часу та ресурсів, що дозволить організаціям підвищити ефективність моніторингу відеоспостереження та процесів розслідування. Рішення для відеоаналітики також можуть бути впроваджені для спостереження за тим, як співробітники та гості взаємодіють з фізичними активами та інфраструктурою, допомагаючи підприємствам покращувати послуги та відповідати очікуванням клієнтів.

5. Постійні вдосконалення

Дані, зібрані та проаналізовані інструментами відеоаналітики, можна використовувати для постійного вдосконалення ширших аспектів діяльності бізнесу. Наприклад,

відеоаналітика в поєднанні з камерами зі штучним інтелектом може допомогти фахівцям зрозуміти типи загроз, до яких їхні організації найбільш вразливі, впливаючи на майбутні рішення щодо вдосконалення систем безпеки та внутрішніх політик.

Подібні принципи можна застосовувати до інших застосувань відеоаналітики. Системи, розгорнуті для спостереження за виробничими завданнями, можуть надавати інформацію щодо покращення виробництва. Аналітика ALPR може допомогти командам покращити операції з управління паркуванням, а поведінкова аналітика може сприяти покращенню обслуговування клієнтів у роздрібній торгівлі та готельному бізнесі.

Міркування щодо впровадження систем відеоаналітики

Системи безпеки відеоаналітики та управління бізнесом можуть забезпечити вимірні переваги лише за умови адаптації до унікальних потреб організації. Розробляючи індивідуальні рішення для відеоаналітики, власники бізнесу повинні враховувати такі фактори:

- **Обробка:** Аналітичне програмне забезпечення може обробляти дані на центральному сервері або на найближчому пристрої. Старіші камери зазвичай потребують серверних систем, які часто страждають від затримки під час обробки аналітики. Для порівняння, новіші IP- камери можуть використовувати периферійну аналітику для обробки даних та отримання аналітики про сам пристрій у режимі реального часу.

- **Точність виявлення:** Відеоаналітика з використанням машинного навчання та функцій штучного інтелекту може бути використана для розробки високоточних систем. Програмне забезпечення можна навчити розуміти нормальні умови роботи цільових зон та попереджати персонал про аномальні події.

- **Масштабованість:** Потреби в безпеці можуть змінюватися з часом, тому вкрай важливо вибрати рішення, яке можна масштабувати за потреби. Подумайте, наскільки легко та економічно ефективно може бути додавання нового обладнання та програмних функцій відеоаналітики до запропонованих інсталяцій.

- **Можливості інтеграції:** Аналітичні дані, отримані за допомогою інструментів відеоаналітики, можна використовувати для оптимізації роботи ширших систем безпеки. Перевірте, чи підтримують потрібні рішення конфігурації відкритого API та чи сумісні вони з існуючими пристроями безпеки для бізнесу.

Майбутні тенденції у відеоаналітиці

Зростаючий інтерес до технологій на основі штучного інтелекту призвів до збільшення впровадження штучного інтелекту в різних бізнес-секторах, причому з 2022 року цілих 72 % організацій впроваджують штучний інтелект для виконання принаймні однієї бізнес-функції. Оскільки штучний інтелект та алгоритми глибокого навчання стають дедалі більш досконалішими, все більше галузей готові отримати вигоду від інтелектуальних систем відеоаналітики.

Відеоаналітика на основі штучного інтелекту зараз є звичайним явищем у сучасних розумних містах та технологіях розумних будівель, а інструменти використовуються не лише для покращення безпеки, але й для підвищення енергоефективності, моніторингу навколишнього середовища та забезпечення належного обслуговування інфраструктури. Відеоаналітика, пов'язана з промисловим Інтернетом речей (IIoT), допомагає фахівцям виконувати ці завдання, дозволяючи автономно коригувати фізичну інфраструктуру у відповідь на високоякісні дані.

Інтерес до нових технологій штучного інтелекту, таких як відеоаналітика, поширюється також на малий бізнес та додатки, а дослідження, опубліковане у 2024 році, показало, що 98% малих підприємств зараз використовують інструменти на базі штучного інтелекту. Оскільки програмне забезпечення для відеоаналітики стає більш доступним та зручним у використанні, його впровадження в усіх галузях промисловості та середовищах, ймовірно, продовжуватиме зростати.

Відеоаналітика в режимі реального часу надає численні суттєві переваги підприємствам у більшості основних секторів, дозволяючи фахівцям отримувати практичну інформацію про важливі процеси безпеки, інфраструктури та організації. Використовуючи унікальні системи відеоаналітики, команди можуть покращити реагування на безпеку, отримати інформацію про бізнес-операції та допомогти працівникам-людям виконувати завдання безпечно та ефективно, що може бути корисним для сучасних підприємств будь-якого розміру.

Мережевий відеореєстратор (NVR) – це спеціалізований комп'ютер, який записує відео з камер безпеки в цифровому форматі на жорсткий диск. Оскільки NVR не має можливості відеозахоплення, відео зазвичай обробляється та кодується з IP-камери спостереження або камери CCTV і передається на NVR для зберігання через мережу Ethernet або Wi-Fi. NVR зазвичай використовуються в системах IP-відеоспостереження.

Мережеві відеореєстратори замінили застарілі цифрові відеореєстратори (DVR). Переваги включають:

- Запис відео та аудіо.
- Краща якість зображення.
- Гнучкість системи.
- Краще покриття огляду.
- Дротове або бездротове.
- Потрібен 1 кабель для відео, аудіо та живлення.
- Розпізнавання облич, номерних знаків тощо завдяки кращій якості зображення.

Функції мережевого відеореєстратора (NVR)

Функції NVR можуть включати:

- Відеоаналітику.
- Параметри режиму запису.
- Мережеві комутатори з живленням через Ethernet (PoE).
- Керування PTZ-камерою.
- Дистанційне налаштування.
- Тригери запису.
- Схеми стиснення відео.

Порівняння цифрових відеореєстраторів та мережевих відеореєстраторів

Цифровий відеореєстратор (DVR) записує відеозаписи з камер спостереження на локальні пристрої зберігання даних, найчастіше на жорсткий диск. DVR може записувати відео з аналогових джерел на місці або захоплювати відео з цифрового джерела. DVR можна підключити до аналогових камер за допомогою коаксіальних кабелів, що дозволяє отримати до них віддалений доступ. DVR пропонують розширені функції, такі як можливість пошуку записів за подіями або сортування за часом і датою. DVR можна налаштувати на автоматичну заміну старих записів після заповнення сховища.

Кожній камері безпеки потрібен центральний відеореєстратор для передачі та архівування записаного матеріалу. Відеоманітофони еволюціонували в моделі DVR, які потім були замінені технологією NVR, що дозволяє контролювати необмежену кількість камер, як в одному місці, так і по всьому світу.

Результати порівняння між відеореєстраторами та мережевими відеореєстраторами:

– Роздільна здатність записів. Відеореєстратори можуть записувати лише з роздільною здатністю 720p. З іншого боку, відеореєстратори пропонують можливості запису високої чіткості 1080p та неймовірну чіткість зображення. D1 – це стандартна якість відео, що використовується системами відеоспостереження замкнутого контуру, тоді як HD пропонує набагато чіткіше зображення з роздільною здатністю 1920×1080 пікселів деталізації.

– Підключення камери. Підключення аналогових систем відеоспостереження є досить складним, оскільки вони вимагають BNC-роз'ємів для кожної камери, підключеної до одного

пристрою, що означає прокладання великої кількості проводів між пристроями (або використання PoE). Це також обмежує кількість камер, які ви можете мати одночасно, перш ніж знадобиться ще один пристрій.

Відеореєстратори (NVR) – це сучасний погляд на цифровий відеореєстратор (DVR), який вирішує багато його проблем. NVR усуває ці проблеми, оскільки він підключений безпосередньо до однієї мережі, тоді як IP-камери передають свої кадри через інше з'єднання. Це робить масштабування NVR набагато доступнішим, ніж у випадку з системою DVR, яка вимагає складніших оновлень обладнання та процесів встановлення, щоб нові системи належним чином працювали разом.

Відеонаглядіві відеореєстратори (NVR) – це найпоширеніший спосіб зберігання та доступу до відео з IP-камер. Моделі з підтримкою Wi-Fi можуть передавати відео бездротовим способом без обмежень щодо близькості, якщо вони знаходяться в одній мережі. Однак, перед покупкою обладнання важливо знати про проблеми сумісності.

Гібридні відеореєстратори

Гібридні відеореєстратори (HVR) – це новітня технологія відеоспостереження. Вони можуть працювати як з аналоговими камерами, так і з IP-камерами, що дає їм перевагу над традиційними системами. Ця універсальність заощадить ваші кошти, коли справа доходить до купівлі нового обладнання.

Результати порівняння між відеореєстраторами та мережевими відеореєстраторами:

Підключення камери:

- Відеонаглядіві відеореєстратори (NVR) – це найпоширеніший спосіб зберігання та доступу до відеозаписів з IP-камер.
- NVR набагато масштабованіші, ніж DVR.

Роздільна здатність записів:

- Відеореєстратори можуть записувати лише з роздільною здатністю 720p. З іншого боку, відеореєстратори пропонують можливості запису високої чіткості 1080p та неймовірну чіткість зображення.

Гібридні відеореєстратори

- Може працювати як з аналоговими камерами, так і з IP-камерами.

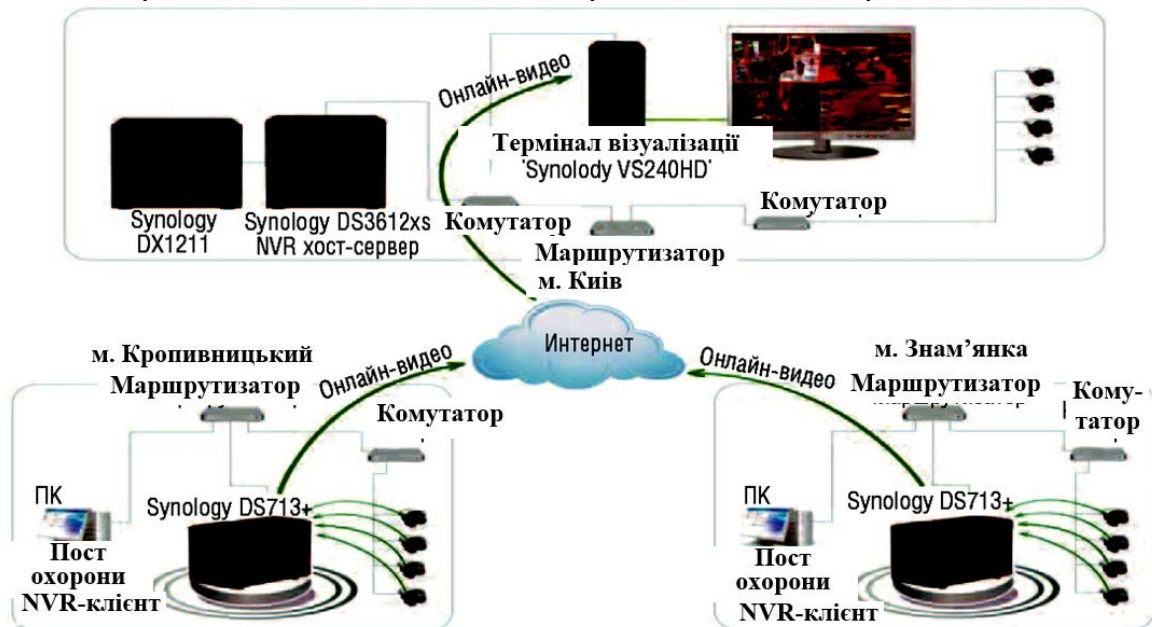


Рисунок 1 – Структурна схема системи

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів комплексних інтелектуальних рішень для відеонагляду. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем комплексних інтелектуальних рішень для відеонагляду.
- Досліджена система комплексних інтелектуальних рішень для відеонагляду.
- На основі отриманих результатів досліджень створена програмна реалізація системи комплексних інтелектуальних рішень для відеонагляду.

Розроблені алгоритми дозволяють успішно вирішувати завдання комплексних інтелектуальних рішень для відеонагляду. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Kuznetsov, O., Frontoni, E., Kryvinska, N., Chevardin, V., Smirnov, O. «Wireless Network Encryption Stream Ciphers, Computational Modeling, and Security Analysis». *Computational Modeling and Simulation of Advanced Wireless Communication Systems*, 2024, pp. 379–402.
2. Kuznetsov, O., Frontoni, E., Kryvinska, N., Smirnov, O., Imoize, G.L. «Computational Modeling of Enhanced Spread Spectrum Codes for Asynchronous Wireless Communication». *Computational Modeling and Simulation of Advanced Wireless Communication Systems*, 2024, pp. 403–447
3. Смірнова Т.В., Коноплицька-Слободенюк О.К., Буравченко К.О., Смірнов С.А., Кравчук О.В., Козірова Н.Л., Смірнов О.А. «Дослідження технологій забезпечення кібербезпеки хмарних сервісів IaaS, PaaS та SaaS». *Кібербезпека: освіта, наука, техніка*. 2024. №4(24), С. 6-27.
4. Батрак О., Смірнова Т., Гнатюк В., Одарченко Р., Смірнов О. «Дослідження показників ефективності функціонування та перспектив розвитку систем IP-телефонії». *Підводні технології*, 2024, № 13, с. 28-35.
5. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». *Advanced Information Systems*, 2023, 7(2), pp. 49-56.
6. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchey, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». *CEUR Workshop Proceedings, Volume 3530*, 2023, pp. 256-265.
7. Smirnov, O., Odarchenko, R., Smirnova, T., Bondar, S., Volosheniuk, D. «Optimal Structure Construction of Private 5G Network for the Needs of Enterprises». *Lecture Notes on Data Engineering and Communications Technologies*, 2023, 178, pp. 208–223.
8. Аль-Мудхафар Акіл Абдулхуссейн М., Смірнова Т.В., Буравченко К.О., Смірнов О.А. «Метод оцінки та підвищення користувальницького досвіду абонентів в програмно-конфігурованих мережах на основі використання машинного навчання». *Сучасні інформаційні системи*, 2023, том 7, № 2, С. 49-56.
9. Smirnov, O., Neskorodieva, T., Fedorov, E., Rudakov, K., Neskorodieva, A. «Method Detection Audit Data Anomalies on Basis Restricted Cauchy Machine» *CEUR Workshop Proceedings, Volume 3187*, 2022,
10. Smirnov O., Smirnova T., Anas M. Al-Oraiqat, Drieiev O., Polishchuk L., Sheraz Khan, Yassin M. Y. Hasan, Aladdein M. Amro, Hazim S. AlRawashdeh «Method for Determining Treated Metal Surface Quality Using Computer Vision Technology». *Sensors (Basel, Switzerland) Volume 22, Issue 16*, 6223, 2022.
11. Smirnov O., Kuznetsov A., Kryvinska N., Kiian A., Kuznetsova K. «Full Non-Binary Constant-Weight Codes». *SN Computer Science*, Vol 2, 337, 2021. <https://doi.org/10.1007/s42979-021-00739-w>
12. Smirnov O., Kuznetsov A., Zhora V., Onikiychuk A., Pieshkova O. «Hiding Messages in Audio Files Using Direct Spread Spectrum». *11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2021, Cracow, Poland, 22-25 September 2021*. P. 414-418.
13. Smirnov O., Kuznetsov A., Lokotkova I., Kuznetsova T., Florov S., Lebid O. «Using Orthogonal Signals to Hide Information in Images». *4 IEEE International Conference on Advanced Information and Communication Technologies (AICT) - 2021, Lviv, Ukraine, September 21-25, 2021*. P. 255-260.
14. Smirnov, O., Kuznetsov, A., Potii, O., Poluyanenko, N., Stelnyk, I., Mialkovsky, D. «Combining and filtering functions in the framework of nonlinear-feedback shift register». *International Journal of Computing*; 2020, Volume 19, Issue 2 – Research Institute for Intelligent Computer Systems – 2020. – P. 247-256.
15. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». *CEUR Workshop Proceedings. Volume 2740*, 2020, Pages 102-114.
16. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». *Journal of theoretical and applied information technology* Vol.98. No 21, 2020, P. 3334-3346.
17. Smirnov O., Kuznetsov A., Kovalchuk D., Kuznetsova T. «New technique for data hiding in cover images using adaptively generated pseudorandom sequences». *CEUR Workshop Proceedings Volume 2654*, 2020, Pages 1-14.
18. Smirnov O., Kuznetsov A., Onikiychuk A., Makushenko T., Anisimova O., Arischenko A. «Adaptive pseudo-random sequence generation for spread spectrum image steganography». *2020 IEEE 11th International Conference*

- on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 161-165.
19. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177.
 20. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587.
 21. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». CEUR Workshop Proceedings Volume 2616, 2020, Pages 366-379.
 22. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645.
 23. Smirnov, O., Kuznetsov, A., Gorbacheva, L., Babenko, V., «Hiding data in images using a pseudo-random sequence», CEUR Workshop Proceedings Volume 2608, 2020, Pages 646-660.
 24. Zhurakovskiy, B., Tsopa, N., Batrak, Y., Odarchenko, R., Smirnova, T «Comparative analysis of modern formats of lossy audio compression». Workshop Proceedings, 2020, 2654, стр. 315-327.
 25. Smirnov O. Kuznetsov A., Zaichenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019; Odessa; Ukraine; 9-13 September 2019. P.22-28.
 26. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.
 27. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019 . P.517-522.
 28. Smirnov, O., Krasnobayev, V., Yanko, A., Kuznetsova, T. «Methods of nulling numbers in the system of residual classes». CEUR Workshop Proceedings, Vol 2588, P. 90-106, 2019.
 29. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Averchev, A., Pastukhov, M., Kuznetsova, K., «Formation of Pseudorandom Sequences with Special Correlation Properties», 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT -2019/ Lviv, Ukraine, 2-6 July, 2019, P. 395-399.
 30. Smirnov, O., Kuznetsov, A., Kavun, S., Babenko, B., Nakisko, O., Kuznetsova, K., «Malware Correlation Monitoring in Computer Networks of Promising Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 347-352.
 31. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Pastukhov, M., Kuznetsova, K., Prokopovych-Tkachenko, D., «Discrete Signals with Special Correlation Properties», CEUR Workshop Proceedings Volume 2353, CEUR Workshop Proceedings 2019, Pages 618-629.

УДК 004

В.Онішук, магістр гр. КН-24М,*Центральноукраїнський національний технічний університет*

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ РИЗИКІВ БЕЗПЕКИ ПРИ ВИКОРИСТАНІ МІЖМЕРЕЖЕВИХ ЕКРАНІВ

У статті розроблено програмне забезпечення, яке призначено для системи інтелектуального аналізу ризиків безпеки при використанні міжмережевих екранів. Метою розробки є дослідження та принципи побудови системи інтелектуального аналізу ризиків безпеки при використанні міжмережевих екранів. Об'єктом дослідження є процес інтелектуального аналізу ризиків безпеки при використанні міжмережевих екранів. Предметом дослідження є методи інтелектуального аналізу ризиків безпеки при використанні міжмережевих екранів. Методи дослідження базуються на методах аналізу даних, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи інтелектуального аналізу ризиків безпеки при використанні міжмережевих екранів. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

інтелектуальний аналіз, ризик безпеки, міжмережеві екрани

Постановка проблеми. У сучасну цифрову епоху як організації, так і окремі особи сильно залежать від веб-додатків для широкого кола діяльності. Однак ця залежність від Інтернету також відкриває можливості для зловмисників використовувати слабкі місця безпеки, присутні в цих додатках. Брандмауери веб-додатків (WAF), як правило, є першою лінією захисту, захищаючи веб-додатки шляхом фільтрації та моніторингу HTTP-трафіку. Однак, якщо ці брандмауери не налаштовані належним чином, зловмисники можуть обійти їх або скомпрометувати. Зростаюча кількість атак, спрямованих на веб-додатки, підкреслює нагальну потребу в підвищенні їхньої безпеки. Дана робота пропонує поглиблений огляд існуючих досліджень з оцінки вразливостей веб-додатків та тестування на проникнення (VAPT).

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи інтелектуального аналізу ризиків безпеки при використанні міжмережевих екранів.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи інтелектуального аналізу ризиків безпеки при використанні міжмережевих екранів.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем інтелектуального аналізу ризиків безпеки при використанні міжмережевих екранів.
- Дослідження системи інтелектуального аналізу ризиків безпеки при використанні міжмережевих екранів.
- Програмна реалізація системи інтелектуального аналізу ризиків безпеки при використанні міжмережевих екранів.

Об'єктом дослідження є процес інтелектуального аналізу ризиків безпеки при використанні міжмережевих екранів.

Предметом дослідження є методи інтелектуального аналізу ризиків безпеки при використанні міжмережевих екранів.

Методи дослідження базуються на методах аналізу даних, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Оцінка ризиків – це необхідна діяльність, яку необхідно проводити регулярно, щоб побачити загальний стан навколишнього середовища.

Ця оцінка є важливим процесом, який використовується для виявлення потенційних ризиків або небезпек у певній ситуації чи діяльності, а також для оцінки ймовірності та потенційних наслідків цих ризиків.

Існує кілька причин, чому важливо проводити оцінку ризиків.

Це може включати запобігання нещасним випадкам і травмам, дотримання правил, репутацію тощо.

Що стосується оцінки ризиків брандмауера, то це процес оцінки ефективності заходів безпеки брандмауера організації.

Оцінка ризиків брандмауера включає оцінку конфігурації, правил та політик брандмауера, щоб визначити, чи вони належним чином налаштовані та підтримуються для захисту мережі організації від зовнішніх загроз.

Метою оцінки ризиків брандмауера є виявлення потенційних слабких місць у заходах безпеки брандмауера та рекомендація кроків для покращення безпеки мережі організації.

Орієнтовно проводить оцінку ризиків брандмауера на основі найкращих галузевих практик, яка охоплює такі теми, як рівень дозволеності правила, використання кластера, використання IPS тощо. Детальні елементи перелічені як категорії тем наступним чином:

- Рівень вседозволеності правила.
- Правила доступу до периметра.
- Стан журналу брандмауера та кожного правила.
- Небезпечний доступ до послуг.
- Конфлікт корпоративної політики.
- Стан кластера брандмауера.
- Використання правила або об'єкта.
- Використання IPS.

Постійне розслідування цих елементів у режимі реального часу надаватиме інформацію про стан ризику в режимі реального часу, яку можна буде постійно переглядати на системних панелях, і відповідно вживати заходів. Крім того, для подальшого аналізу будуть створюватися звіти про оцінку ризиків для кожного брандмауера або системи.

Брандмауер – це пристрій мережевої безпеки, апаратний або програмний, який контролює весь вхідний та вихідний трафік і, на основі визначеного набору правил безпеки, приймає, відхиляє або відкидає цей конкретний трафік. Він діє як охоронець, який допомагає захистити ваш цифровий світ від небажаних відвідувачів та потенційних загроз.

Брандмауер:

- Прийняти: дозволити трафік.
- Відхилити: заблокувати трафік, але відповісти повідомленням «помилка недоступності».
- Відмова: блокування трафіку без відповіді.

Потреба в брандмауері

Брандмауер є важливим, оскільки мережі постійно піддаються впливу як безпечного, так і шкідливого трафіку з Інтернету чи інших мереж. Без брандмауера ваші системи не матимуть захисту від небажаного доступу, шкідливої діяльності чи випадкових витоків даних.

1. Запобігання несанкціонованому доступу

Уявіть, що двері вашого будинку завжди відчинені. Будь-хто, хто переходить повз, може зайти та забрати ваші речі. Брандмауер – це як замкнені двері з охоронцем, які впускають лише перевірених людей і не пускають незнайомих.

2. Блокування шкідливого трафіку

Подумайте про свою поштову скриньку електронної пошти. Без спам-фільтра ви б отримували шахрайські та спам-повідомлення. Брандмауер працює як цей спам-фільтр, він блокує шкідливі дані, перш ніж вони досягнуть вас.

3. Захист конфіденційної інформації

Це як зберігати свій банківський PIN-код у сейфі, а не залишати його на столі, де будь-хто може його побачити. Брандмауер гарантує, що ваші особисті та бізнес-дані залишаються прихованими від кіберзлочинців.

4. Запобігання кібератак

Якщо ви залишите свій автомобіль незамкненим на парковці, злодії можуть його вкрати. Брандмауер блокує вашу мережу, щоб зловмисники не могли її викрати.

5. Контроль використання мережі

Так само, як батьки встановлюють батьківський контроль, щоб діти не могли відвідувати небезпечні веб-сайти, брандмауери контролюють, де вашим комп'ютерам дозволено підключатися.

Робота брандмауера

Брандмауер працює як охоронець вашої мережі, стоячи між вашими внутрішніми системами, такими як комп'ютери, сервери та пристрої, та зовнішнім світом, таким як Інтернет чи інші мережі. Він ретельно перевіряє всі дані, що входять або виходять, щоб забезпечити проходження лише безпечного трафіку.

- Коли дані намагаються увійти до вашої мережі або вийти з неї, вони спочатку проходять через брандмауер.

- Брандмауер перевіряє пакети даних (невеликі фрагменти інформації) за допомогою заздалегідь визначених правил.

- Правила можна визначити на брандмауері на основі необхідності та політик безпеки організації.

- Брандмауер дозволяє приймати рішення, такі як: Дозволити → Якщо пакет відповідає правилам безпеки, або Блокувати → Якщо пакет підозрілий, походить з чорного списку джерела або містить шкідливий код.

- Брандмауер реєструє заблокований або незвичний трафік для перевірки командами безпеки.

- Сповіщення можуть надсилатися в режимі реального часу, якщо виявлено серйозну загрозу.

Політика за замовчуванням: Дуже важко чітко охопити всі можливі правила на брандмауері. З цієї причини брандмауер завжди повинен мати політику за замовчуванням. Політика за замовчуванням складається лише з дій (прийняти, відхилити або видалити). Припустимо, що на брандмауері не визначено жодного правила щодо SSH-підключення до сервера. Отже, він дотримуватиметься політики за замовчуванням. Якщо політика за замовчуванням на брандмауері встановлена на прийняття, то будь-який комп'ютер за межами вашого офісу може встановити SSH-підключення до сервера. Тому встановлення політики за замовчуванням як "відхилити" (або "скинути") завжди є гарною практикою.

Типи брандмауерів

1) Розміщення в мережі:

- Брандмауер фільтрації пакетів.
- Брандмауер з перевіркою стану.
- Проксі-брандмауер (рівень програми).
- Шлюз на рівні схеми.
- Брандмауер веб-застосунків (WAF).
- Брандмауер наступного покоління (NGFW).

2) Захищені системи:

- Мережевий брандмауер.
- Брандмауер на базі хоста.

3) Метод фільтрації даних:

- Периметральний брандмауер.
- Внутрішній брандмауер.
- Розподілений брандмауер.

4) Форм-фактори:

- Апаратний брандмауер.
- Програмний брандмауер.

Важливість брандмауерів

Мережевий брандмауер – це ваша перша лінія захисту в кібербезпеці. Він відстежує, фільтрує та контролює дані, що передаються в вашу мережу та з неї.

– Мережі вразливі до будь-якого трафіку, який намагається отримати доступ до ваших систем, незалежно від того, чи є він шкідливим, чи ні. Саме тому вкрай важливо перевіряти весь мережевий трафік.

– Коли ви підключаєте персональні комп'ютери до інших ІТ-систем або Інтернету, це відкриває багато переваг, таких як співпраця, спільний доступ до ресурсів та творчість. Але це також наражає вашу мережу та пристрої на ризики, такі як злом, крадіжка особистих даних, шкідливе програмне забезпечення та онлайн-шахрайство.

– Як тільки зловмисник знайде вашу мережу, він зможе легко отримати до неї доступ та створювати до неї загрозу, особливо за умови постійного підключення до Інтернету.

– Використання брандмауера є важливим для проактивного захисту від цих ризиків. Він допомагає користувачам захистити свої мережі від найгірших небезпек.

Брандмауер служить бар'єром безпеки для мережі, звужуючи поверхню атаки до однієї точки контакту. Замість того, щоб кожен пристрій у мережі був підданий доступу до Інтернету, весь трафік спочатку має пройти через брандмауер. Таким чином, брандмауер може фільтрувати та блокувати недозволений трафік, незалежно від того, чи він входить, чи виходить. Крім того, брандмауери допомагають створювати облік спроб підключень, підвищуючи обізнаність про безпеку.

Брандмауери регулюють як вхідний, так і вихідний трафік, захищаючи мережу від:

– Зовнішні загрози, такі як віруси, фішингові електронні листи, атаки типу «відмова в обслуговуванні» (DoS) та бекдори. Брандмауери фільтрують вхідний трафік, запобігаючи несанкціонованому доступу до конфіденційних даних та запобігаючи потенційним зараженням шкідливим програмним забезпеченням.

– Внутрішні загрози, такі як відомі зловмисники або ризиковані програми. Брандмауер може застосовувати правила та політики для обмеження певних типів вихідного трафіку, що допомагає виявляти підозрілу активність та запобігати витоку даних.

Брандмауери можуть захищати від різноманітних загроз, моніторячи та контролюючи вхідний і вихідний мережевий трафік. Ось основні загрози, від яких вони допомагають захиститися:

– Проникнення зловмисників: Брандмауери можуть блокувати підозрілі з'єднання, запобігаючи прослуховуванню та розширеним постійним загрозам (APT).

– Батьківський контроль: Батьки можуть використовувати брандмауери, щоб заборонити своїм дітям доступ до відвертого веб-контенту.

– Обмеження перегляду веб-сторінок на робочому місці: Роботодавці можуть обмежити працівників у використанні мережі компанії для доступу до певних сервісів та веб-сайтів, таких як соціальні мережі.

– Національно контрольована інтрамережа: Уряди можуть блокувати доступ до певного веб-контенту та послуг, які суперечать національній політиці чи цінностям.

Дозволяючи власникам мережі встановлювати певні правила, брандмауери пропонують настроюваний захист для різних сценаріїв, підвищуючи загальну безпеку мережі.

Практики безпеки брандмауера**Тримайте брандмауер увімкненим**

Ніколи не вимикайте брандмауер лише для підключення до пристрою чи мережі. Натомість налаштуйте правила брандмауера та додайте довірені пристрої до списку дозволених пристроїв.

Будьте в курсі подій

Регулярно оновлюйте програмне забезпечення брандмауера або операційну систему, щоб виправляти вразливості та запобігати новим загрозам безпеці.

Підключення до VPN

VPN шифрує ваш інтернет-трафік, додаючи ще один рівень захисту поряд із вашим брандмауером. Тільки обов'язково налаштуйте правила брандмауера, якщо виникне конфлікт.

Відхилити невідомі запити

Якщо ви отримаєте підозрілий запит на доступ, негайно його заблокуйте. Розслідуйте це пізніше, перш ніж вносити будь-які постійні зміни.

Додайте додаткові інструменти безпеки

Брандмауери не блокують усі загрози, особливо шкідливі програми, які ви встановлюєте самостійно. Використовуйте перевірене антивірусне або антивірусне програмне забезпечення для повного захисту.

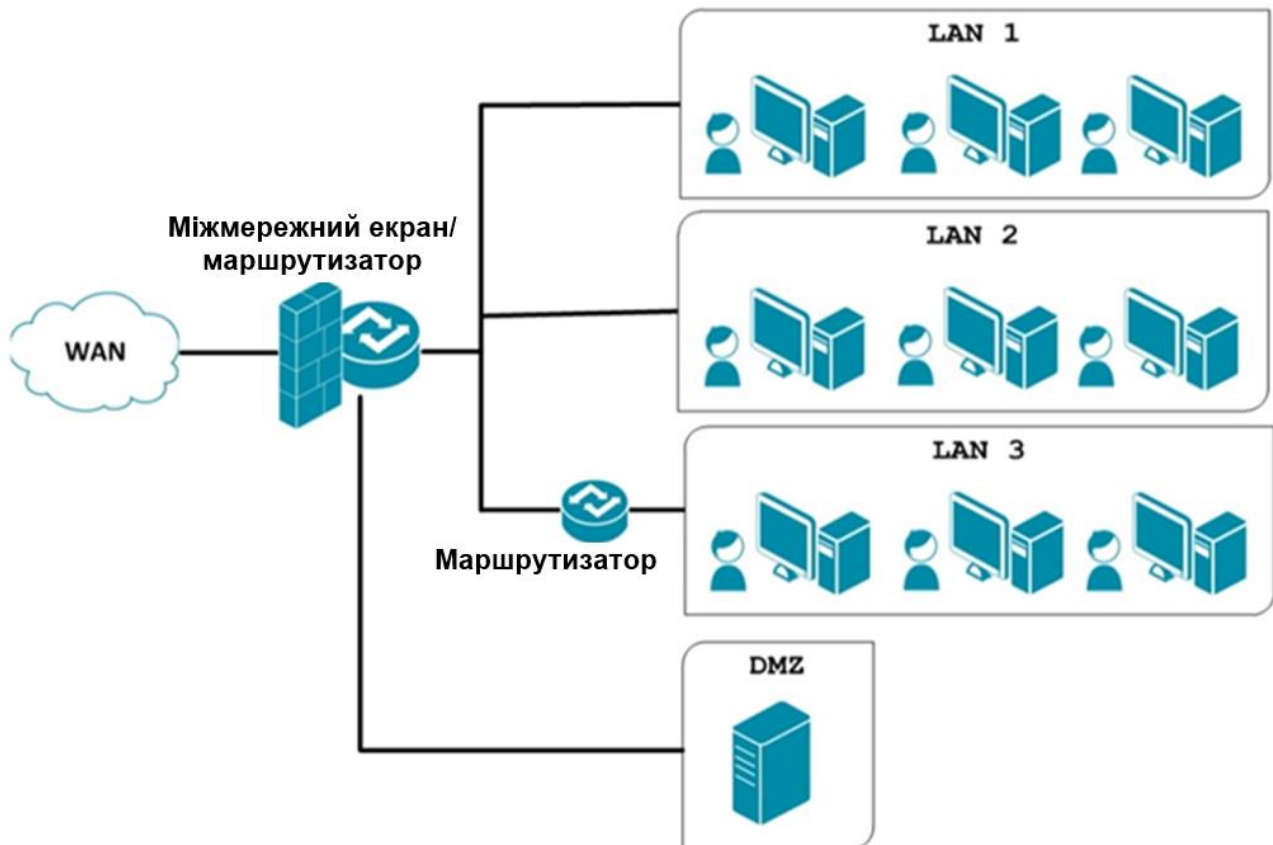


Рисунок 1 – Структурна схема системи

Брандмауер – це механізм безпеки, який може бути апаратним або програмним, здебільшого призначений для забезпечення безпеки. Його основна мета – забезпечити доступ до комп'ютера або мережі лише уповноваженим особам. Він виступає посередником між приватною мережею та публічним Інтернетом для регулювання доступу до трафіку відповідно до заданої політики безпеки.

Апаратні брандмауери діють як фізичні бар'єри між мережею та Інтернетом, тоді як програмні брандмауери – це додаткові програми для ПК або мережевих комп'ютерів.

Брандмауер можна уявити як охоронця, який стоїть між приватною мережею та публічним Інтернетом і дозволяє перетинати цей бар'єр лише такому трафіку.

Брандмауери функціонують, аналізуючи потоки мережевих пакетів або пакетів даних, що циркулюють у мережі. Вони визначають, чи пропускати пакет чи ні, залежно від встановлених параметрів безпеки. Це може включати аналіз джерела та пункту призначення пакета, використовуваного протоколу зв'язку та вмісту повідомлення.

Існують різні типи брандмауерів, зокрема:

- Фільтрація пакетів Брандмауер.
- Брандмауер проксі-сервісу.
- Брандмауер з перевіркою стану.
- Шлюзи рівня каналу Брандмауер.
- Брандмауер наступного покоління (NGFW).
- Програмні брандмауери.
- Апаратні брандмауери.
- Хмарні брандмауери.

Тепер перейдемо до функцій брандмауера, щоб зрозуміти, як вони допомагають компаніям та окремим особам створювати безперебійні та безпечні мережі.

Головна функція брандмауера – забезпечення безпеки. Ці системи пропонують численні цілі, які безпосередньо покращують безпеку, керованість та продуктивність мережі. Нижче ми пояснили деякі інші функції брандмауера.

Моніторинг мережевого трафіку

Важливою функцією брандмауера є регулювання руху трафіку між приватною мережею та публічним Інтернетом. Брандмауери аналізують кожен пакет інформації, який хоче ввійти або вийти через брандмауер, перевіряючи адресу джерела та призначення, а також використовуваний протокол. Цей пакет порівнюється з попередньо встановленими правилами безпеки; якщо брандмауер схвалює, пакет пропускається; в іншому випадку він блокується.

Контроль доступу

Брандмауери допомагають регулювати, хто може отримувати доступ до вашої мережі та який рівень свободи в ній є. Використовуючи правила доступу, ви можете вирішувати, хто або що може підключатися до вашої мережі. Наприклад, ви можете дозволити переглядати деякі дані лише певним користувачам, а іншим – заборонити.

Контроль доступу описується як список дозволів для вашої мережі, відомий як Список контролю доступу. Так само, як двері будинку зачинені для людей, яких ви не знаєте або не є вашими родичами, брандмауер дозволяє перебувати всередині мережі лише тим, кому дозволено.

Фільтрація пакетів

Фільтрація пакетів використовується в брандмауерах для перевірки мережевого трафіку на рівні пакетів. Брандмауери аналізують пакети, спочатку перевіряючи їх на рівні заголовка, який складається з інформації, що передається з кожним пакетом; він містить IP-адреси джерела та призначення. Потім брандмауери аналізують протокол зв'язку та номери портів, що використовуються.

Представлені тут пакетні дані можуть використовуватися брандмауерами та пов'язаними з ними системами для фільтрації та подальшого вжиття заходів, тобто «дозволу» або «заборони» різних типів трафіку відповідно до політик безпеки. Наприклад, брандмауер можна налаштувати так, щоб він забороняв підключення всього трафіку на стандартному веб-порті 80, щоб запобігти доступу хакерів до хостів на веб-серверах.

Фільтрація на рівні програм

Окрім фільтрації на рівні пакетів, сучасні брандмауери розширюють свою функціональність, фільтруючи на рівні програм. Брандмауери роблять це, розглядаючи вміст повідомлення та контекст мережевого трафіку, а не лише заголовок. Це також дозволяє їм

контролювати та забороняти або дозволяти певні програми чи служби, такі як перегляд веб-сторінок, електронна пошта або протокол передачі файлів.

Фільтрація на рівні програм через брандмауери забезпечує дотримання політик безпеки, таких як запобігання доступу до певних веб-сайтів або використання певних програм.

Фільтрація контенту

Ще однією важливою функцією брандмауерів є те, що їх також можна запрограмувати на фільтрацію контенту на основі різних критеріїв. Ця функція дозволяє організації або окремій особі заборонити будь-якій IP-адресі доступ до певних сайтів або контенту, доступного в Інтернеті та визнаного забороненим або небезпечним.

Фільтрація контенту схожа на батьківський контроль. Так само, як ви б налаштували батьківський контроль на телевізорі чи Інтернеті для своїх дітей, фільтрація контенту робить те саме для всієї мережі.

Система виявлення вторгнень та система запобігання вторгненням

Брандмауери також можуть виконувати роль IDPS, скорочення від intrusion detection and prevention systems (систем виявлення та запобігання вторгненням). Таким чином, вони можуть шукати ознаки, що вказують на зловмисну активність, таку як мережева атака, спроба несанкціонованого доступу або будь-яка дивна активність у мережі. Коли йдеться про загрози безпеці, брандмауери можуть діяти ефективно та запобігати атаці або пом'якшувати її наслідки, якщо така є.

Ця функція виявлення та запобігання вторгненням допомагає захистити мережу та підключені до неї пристрої від багатьох видів кіберзагроз, таких як DDoS, мережеве шкідливе програмне забезпечення та незаконний доступ.

Підтримка віртуальної приватної мережі (VPN)

Сучасні брандмауери пропонують VPN-рішення як у своєму списку функцій, так і в основному наборі функцій. У випадку VPN-з'єднання, формування безпечного та зашифрованого тунелю між користувачем та мережею здійснюється за допомогою VPN, щоб користувач міг безпечно підключатися до мережі віддалено.

Брандмауери, що підтримують VPN, можуть допомогти організації розширити периметр своєї мережі та задовольнити потреби користувачів, яким доводиться або які бажають працювати віддалено в сучасному бізнес-середовищі.

Трансляція мережевих адрес (NAT)

Ще однією важливою функцією брандмауерів є те, що вони містять функції NAT, які дозволяють їм перетворювати одну схему мережевих адрес в іншу. Це особливо актуально, коли приватна мережа використовує інший набір IP-адрес, ніж публічна мережа.

Коли брандмауери виконують NAT, внутрішня фактична топологія мережі залишається прихованою від глобальної мережі, що робить її безпечнішою. Це може допомогти мінімізувати прямий доступ до внутрішніх пристроїв з Інтернету, тим самим зменшуючи ймовірність атаки.

Ведення журналів та звітність

Брандмауери зазвичай мають функції реєстрації та звітності, що дозволяють їм записувати та аналізувати мережевий трафік і події безпеки. Цю інформацію можна використовувати для різних цілей, таких як:

- Моніторинг та аудит мережевої активності.
- Виявлення та розслідування інцидентів безпеки.
- Створення звітів для цілей дотримання вимог та регулювання.
- Оптимізація конфігурацій брандмауера та політик безпеки.

Ось деякі з основних функцій брандмауера, які допомагають захистити вашу приватну мережу та пристрої.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів інтелектуального аналізу ризиків безпеки при використанні міжмережевих екранів. Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем інтелектуального аналізу ризиків безпеки при використанні міжмережевих екранів.

– Досліджена система інтелектуального аналізу ризиків безпеки при використанні міжмережевих екранів.

– На основі отриманих результатів досліджень створена програмна реалізація системи інтелектуального аналізу ризиків безпеки при використанні міжмережевих екранів.

Розроблені алгоритми дозволяють успішно вирішувати завдання інтелектуального аналізу ризиків безпеки при використанні міжмережевих екранів. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Kuznetsov O., Frontoni E., Kuznetsova Y., Chevardin V., Smirnov O. «Architectural foundations for adaptive security in edge computing systems». *Cybersecurity Defensive Walls in Edge Computing*, 2025. pp. 21–61.
2. Chulinda L., Smirnov O., Shapenko L., Ustynova I., Bohatiuk I., Kelyp S. «The role of innovation in ensuring the safety of international civil aviation». *Ceur Workshop Proceedings*, 2025, 4024, pp. 530–542.
3. Петрик В.М., Присяжнюк М.М., Аль-Файюмі Халед та ін. «Системи інформаційної зброї та технології інформаційної війни»: підручник / Петрик В.М., Присяжнюк М.М., Аль-Файюмі Халед, Жарков Я.М., Смірнов О.А., Буравченко К.О., Давидюк А.В., Кононович В.Г., Корчинський В.В., Кудирко В.М., Фесенко А.О.; за заг. ред. В.М. Петрика, М.М. Присяжнюка.– К.: Видавничий центр “Кафедра”, 2025.– 320 с.
4. Усік, П.С., Смірнова, Т.В., Буравченко, К.О., Смірнов, О.А., Улічев, О.С., Смірнов, С.А. «Дослідження технологій забезпечення кібербезпеки банківських систем з використанням штучного інтелекту». *Кібербезпека: освіта, наука, техніка*. 2025. Том 1 № 29. С.704–716, 2025
5. Kuznetsov, O., Frontoni, E., Kuznetsova, K., Arnesano, M., Smirnov, O. «A secure biometric authentication architecture for blockchain-driven cyber-physical systems». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 193–224.
6. Kuznetsov, O., Atzeni, G., Arnesano, M., Randieri, C., Smirnov, O. «Secure IoT-based smart wheelchair system: From implementation to security enhancement strategy». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 225–257.
7. Kuznetsov, O., Smirnov, O., Kuznetsova, T., Shaikhanova, A., Svatowsky, I. «Privacy-utility trade-offs in IoT networks: A comparative analysis of differential privacy mechanisms for sensor data aggregation». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 589–622.
8. Lakhno, V., Malyukov, V., Smirnov, O., Bebesko, B., Chubaievskiy, V., Zhumadilova, M., Malyukova, I., Smirnov, S. «Multifactorial Model for Targeted Attacks Counteracting Within the Framework of a Multi-Step Quality Game with Fuzzy Information». *8th International Symposium on Intelligent Informatics, ISI 2023*, 2025. vol 389. pp 377–389. Springer, Singapore.
9. Kuznetsov O., Frontoni E., Kuznetsova Y., Smirnov O., Moskovchenko I. «Trust-Based Security Architecture for Edge Computing: A Simulation Study of Dynamic Trust Evolution and Attack Detection». *CEUR Workshop Proceedings*, 2024, 3909, pp. 227–241.
10. Kuznetsov, O., Frontoni, E., Kryvinska, N., Chevardin, V., Smirnov, O. «Wireless Network Encryption Stream Ciphers, Computational Modeling, and Security Analysis». *Computational Modeling and Simulation of Advanced Wireless Communication Systems*, 2024, pp. 379–402.
11. Kuznetsov, O., Frontoni, E., Kryvinska, N., Smirnov, O., Imoize, G.L. «Computational Modeling of Enhanced Spread Spectrum Codes for Asynchronous Wireless Communication». *Computational Modeling and Simulation of Advanced Wireless Communication Systems*, 2024, pp. 403–447.
12. Ткаченко, О., Ільченко, А., Улічев, О., Мелешко, Є., Смірнов, О. «Правові засади поширення інформаційних впливів в соціальних мережах». *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2024. № 2(26), С. 170–188.
13. Смірнова Т.В., Коноплицька-Слободенюк О.К., Буравченко К.О., Смірнов С.А., Кравчук О.В., Козірова Н.Л., Смірнов О.А. «Дослідження технологій забезпечення кібербезпеки хмарних сервісів IaaS, PaaS та SaaS». *Кібербезпека: освіта, наука, техніка*. 2024. №4(24), С. 6–27.
14. Вінтенко, Б., Миронець, І., Смірнов, О., Кравчук, О., Козірова, Н., Савеленко, Г., Коваленко, А. «Дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». *Кібербезпека: освіта, наука, техніка*. 2024. №3(23), С. 111–131.
15. Батрак О., Смірнова Т., Гнатюк В., Одарченко Р., Смірнов О. «Дослідження показників ефективності функціонування та перспектив розвитку систем IP-телефонії». *Підводні технології*, 2024, № 13, с. 28–35.
16. Kuznetsov, O., Kryvinska, N., Ilchenko, O., Smirnova, T., Ulianova, Y. «Comparative Analysis of Cryptocurrency Trading Platforms Using the Analytic Hierarchy Process». *CEUR Workshop Proceedings*, 2023,

3628, pp. 106-115.

17. Akhalaia, G., Iavich, M., Iashvili, G., Prysiazhnyy, D., Smirnova, T. «Secure Encrypted Connection on Georgian Website». *CEUR Workshop Proceedings*, 2023, 3550, pp. 313-320.
18. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». *Advanced Information Systems*, 2023, 7(2), pp. 49-56
19. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchey, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». *CEUR Workshop Proceedings*, Volume 3530, 2023, pp. 256-265.
20. Kuznetsov, O., Kandy, S., Frontoni, E., Smirnov, O. «Trade-offs in Post-Quantum Cryptography: A Comparative Assessment of BIKE, HQC, and Classic McEliece». *CEUR Workshop Proceedings*, Volume 3504, 2023, pp. 1-11.
21. Smirnov, O., Lakhno, V., Akhmetov, B., Chubaievskyi, V., Khorolska, K., Bebesko, B. «Selection of a Rational Composition of Information Protection Means Using a Genetic Algorithm». In: Rajakumar, G., Du, KL., Vuppapapati, C., Beligiannis, G.N. (eds) *Intelligent Communication Technologies and Virtual Mobile Networks. Lecture Notes on Data Engineering and Communications Technologies*, vol 131. 2023. Springer, Singapore. pp. 21-34.
22. Смірнова Т.В., Гнатюк С.О., Бердибаєв Р.Ш., Сидоренко В.М., Жигаревич О.К., «Система корелювання подій та управління інцидентами кібербезпеки на об'єктах критичної інфраструктури». *Кібербезпека: освіта, наука, техніка*, №3(19), 2023, С. 176-196.
23. Смірнов О.А. Козлов Я.О., Смірнова Т.В. «Дослідження застосування SIEM-систем для забезпечення кібербезпеки та захисту інформації». II Міжнародна науково-практична Інтернет-конференція «Інновації та перспективні шляхи розвитку інформаційних технологій (ІПШРІТ-2023)» м.Черкаси 6 грудня 2023 року – Черкаси: ЧДТУ.– 2023. – С.251-252.
24. Козлов Я.О., Смірнова Т.В., Смірнов О.А. «Дослідження SIEM-систем для забезпечення кібербезпеки». VII міжнародна науково-практична конференція “Інформаційна безпека та комп’ютерні технології” до 30-ти річчя кафедри кібербезпеки та програмного забезпечення, м. Кропивницький. 1 листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 26.
25. Козлов Я.О., Козірова Н.Л., Смірнов О.А. «Дослідження структури та принципу роботи SIEM-системи». VII міжнародна науково-практична конференція “Інформаційна безпека та комп’ютерні технології” до 30-ти річчя кафедри кібербезпеки та програмного забезпечення, м. Кропивницький. 1 листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 59.
26. Вінтенко Б.Ю., Смірнов О.А., Коваленко О.В., Смірнов С.А., Коваленко А.С. «Дослідження нормативних документів та галузевих стандартів розробки програмного забезпечення комп’ютерних систем управління АЕС, важливих для безпеки». *Системи управління, навігації та зв’язку*, 2023, вип. 2(72), С. 170-178.
27. Smirnov, O., Neskrodieva, T., Fedorov, E., Rudakov, K., Neskrodieva, A. «Method Detection Audit Data Anomalies on Basis Restricted Cauchy Machine» *CEUR Workshop Proceedings*, Volume 3187, 2022,
28. Smirnov O.A., Al-Oraiqat A.M., Ulichev O.S., Meleshko Ye.V., Al-Rawashdeh H.S., Polishchuk L.I. «Modeling strategies for information influence dissemination in social networks». *Journal of Ambient Intelligence and Humanized Computing* Volume 13, Issue 5. Springer, Cham. 2022, pp. 2463-2477.
29. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». *Проблеми інформатизації та управління*, № 2(70). 2022. С. 28-37.
30. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» *Системи управління, навігації та зв’язку*, 2022, № 3(69). С. 93-98.
31. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» *Вісник Хмельницького національного університету. Серія: «Технічні науки»*, № 2 (307). С. 46-52. 2022.

УДК 004

О.Осуський, магістр гр. КІ-24М,

Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ МЕРЕЖЕВОГО УПРАВЛІННЯ КОРПОРАТИВНИМИ ВІДЕОРЕСУРСАМИ НА ОСНОВІ ТЕХНОЛОГІЇ EVRP

У статті розроблено програмне забезпечення, яке призначено для системи мережевого управління корпоративними відеоресурсами на основі технології EvRP. Метою розробки є дослідження та принципи побудови системи мережевого управління корпоративними відеоресурсами на основі технології EvRP. Об'єктом дослідження є процес мережевого управління корпоративними відеоресурсами на основі технології EvRP. Предметом дослідження є методи мережевого управління корпоративними відеоресурсами на основі технології EvRP. Методи дослідження базуються на методах теорії інформації, теорії побудови комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи мережевого управління корпоративними відеоресурсами на основі технології EvRP. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

управління корпоративними відеоресурсами, EvRP

Постановка проблеми. Корпоративна відеоплатформа (EvRP) – це централізована система, яка займається управлінням відео для різних підприємств. Вона відповідає за створення, керування, зберігання та доставку високоякісного відеоконтенту співробітникам компанії або клієнтам за її межами. Основні функції цих відеоплатформ включають керування прямими трансляціями, відеоаналітику, безпеку, контроль доступу, відеохостинг та високоякісні можливості інтеграції.

EvRP діють як система керування контентом (CMS) для відео, здатна створювати захопливий відеоконтент для бізнес-функцій, таких як навчання співробітників, комунікація, маркетинг, підтримка клієнтів тощо. Зрештою, корпоративна відеоплатформа – це ефективне бізнес-рішення, яке може допомогти компаніям керувати величезними обсягами даних, підвищити продуктивність, покращити комунікацію та співпрацю з мінімальними витратами.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи мережевого управління корпоративними відеоресурсами на основі технології EvRP.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи мережевого управління корпоративними відеоресурсами на основі технології EvRP.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем мережевого управління корпоративними відеоресурсами на основі технології EvRP.

- Дослідження системи мережевого управління корпоративними відеоресурсами на основі технології EvRP.

- Програмна реалізація системи мережевого управління корпоративними відеоресурсами на основі технології EvRP.

Об'єктом дослідження є процес мережевого управління корпоративними відеоресурсами на основі технології EvRP.

Предметом дослідження є методи мережевого управління корпоративними відеоресурсами на основі технології EvRP.

Методи дослідження базуються на методах теорії інформації, теорії побудови комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Корпоративні відеоплатформи є важливими для підтримки бізнесу, який прагне залишатися конкурентоспроможним та інноваційним. Кілька тенденцій вимагають встановлення та впровадження централізованої системи онлайн-керування відео, де цифровий контент може куруватися та використовуватися для покращення віддаленої співпраці, комунікації, маркетингової прибутковості тощо, щоб досягти кращих бізнес-результатів. Тепер, коли ви знаєте важливість виконавчих віцепрезидентів (EvRP), давайте обговоримо конкретні переваги встановлення такої системи у вашій компанії.

Переваги корпоративної відеоплатформи

Впровадження добре оснащеної системи корпоративної відеоплатформи для задоволення потреб вашої компанії у відеозв'язку може запропонувати вам багато переваг.

Ознайомтеся з деякими з цих переваг:

- Централізоване керування відео: EvRP пропонують безпечний та організований спосіб зберігання, керування та розповсюдження відеоконтенту по всій організації.
- Аналітика та огляди відео: Виконавчі візитні картки (EvRP) надають цінні дані про те, хто що дивиться, рівень залученості та загальні показники ефективності відео.
- Безпека контенту: EvRP пропонують надійні функції безпеки, такі як контроль доступу, шифрування та управління цифровими правами (DRM), для захисту конфіденційного відеоконтенту від несанкціонованого доступу та забезпечення дотримання правил захисту даних.
- Покращена комунікація: Виконавчі віцепрезиденти сприяють безперебійній комунікації в організаціях за допомогою таких функцій, як прямі трансляції, відеоконференції та контент на вимогу, покращуючи співпрацю між командами незалежно від географічного розташування.

Варіанти використання корпоративних відеоплатформ

Корпоративні відеоплатформи можуть задовольнити потреби управління відео в організаціях з різних напрямків.

Деякі з найпоширеніших випадків використання систем EvRP є наступними:

- Корпоративні комунікації: Виконавчі віце-президенти ефективно вдосконалюють внутрішні та зовнішні комунікаційні стратегії організації, надсилаючи оголошення, оновлення тощо.
- Розвиток та навчання людських ресурсів: Виконавчі віце-президенти можуть створювати захопливий та ефективний відеоконтент для навчання співробітників, зменшуючи витрати, пов'язані з проведенням виїзних сесій. Наприклад, вони можуть використовувати відео для роз'яснення складних тем, таких як пояснення переваг EOR, що полегшує співробітникам розуміння цих переваг.
- Маркетингові стратегії: відеоконтент, такий як демонстрації продуктів, відгуки клієнтів, контент для соціальних мереж та рекламні відео, є ключовим для маркетингової кампанії компанії. Виконавчі віце-президенти контролюють усі ці елементи.
- Заходи та конференції: Виконавчі віце-президенти в основному відповідають за ефективну віддалену співпрацю, проводячи прямі трансляції та відеоконференції, в яких учасники з різних місць можуть збиратися разом та брати участь.

Функції, які слід враховувати при виборі корпоративних відеоплатформ

Найкращі відеоплатформи пропонують різні функції, адаптовані до конкретних бізнес-вимог. Щоб отримати максимальну віддачу від своїх інвестицій, вам потрібно добре знати можливості ваших систем EvRP.

Ось список головних функцій, на які слід звернути увагу під час вибору гідної платформи для корпоративного відео.

- Функції створення та керування відео: Виконавчий віце-президент повинен вміти створювати та редагувати відео. Зверніть увагу на такі важливі інструменти, як запис екрана, обрізання та кадрування відео, візуальні ефекти, налаштування звуку тощо.

- Можливості відеохостингу: Платформа повинна бути добре оснащена такими функціями, як зберігання відео, категоризація та тегування для ефективного хостингу.

- Підтримка прямих трансляцій: Платформа повинна мати можливість проводити прямі трансляції, конференції та події, а також керувати ними та планувати їх.

- Функції безпеки та доступу: Система повинна бути максимально захищена, зокрема шифруванням та захистом паролем. Крім того, повинні бути присутніми функції контролю доступу, щоб запобігти несанкціонованому доступу до відео.

- Інструменти аналітики та відстеження: інструменти для відстеження показників відео, таких як перегляди, залученість та рівень утримання, повинні бути присутніми, щоб дозволити компаніям вимірювати ефективність своїх відеостратегій.

- Налаштування: Платформа повинна бути налаштовуваною для передачі брендових повідомлень та адаптації інтерфейсу до бізнес-цілей.

- Сумісність з мобільними пристроями: відеоплатформа також має бути сумісною зі смартфонами Android та iOS, щоб зробити її доступнішою для співробітників.

- Можливості інтеграції: Відеоплатформа має бути сумісною з іншими корпоративними системами та системами управління контентом для максимальної ефективності.

Кожна компанія, що виробляє онлайн-відеоконтент, хоче транслювати його як у приватному, так і в колективному просторі.

Для цього ось список функцій платформи відеохостингу для професіоналів.

Багато компаній хочуть узгодити свою платформу з іміджем свого бренду.

На корпоративній платформі ви маєте можливість мати:

- Відеоплеєр HTML5 у white label. Ви можете додати свій логотип на відеоплеєр для більш професійного результату, який ідеально відповідає іміджу вашого бренду. Важливо, щоб ваша аудиторія могла переглядати ваші відео у найкращій можливій роздільній здатності HD. Для цього на корпоративній відеоплатформі, такій як Videas, Vimeo або Wistia, доступний відеоплеєр HTML5.

- Персоналізована відеоплатформа. Ви креативні та хочете персоналізувати свою платформу. Ви маєте можливість узгодити графічний статут вашої компанії на відеоплатформі Enterprise. «Приватний YouTube», який вам підходить!

- Відеотека. Ідеально підходить для розміщення великої кількості відео. Це також дозволяє звільнити місце на вашому комп'ютері. Більше того, ви можете легко переміщатися по відеотеці, і, звичайно ж, завдяки багатьом функціям:

- Класифікувати.
- Для індексу.
- Для анотації.
- Перейменувати.
- Щоб шукати відео.
- Щоб створити списки відтворення.
- Налаштовувана сторінка спільного доступу.

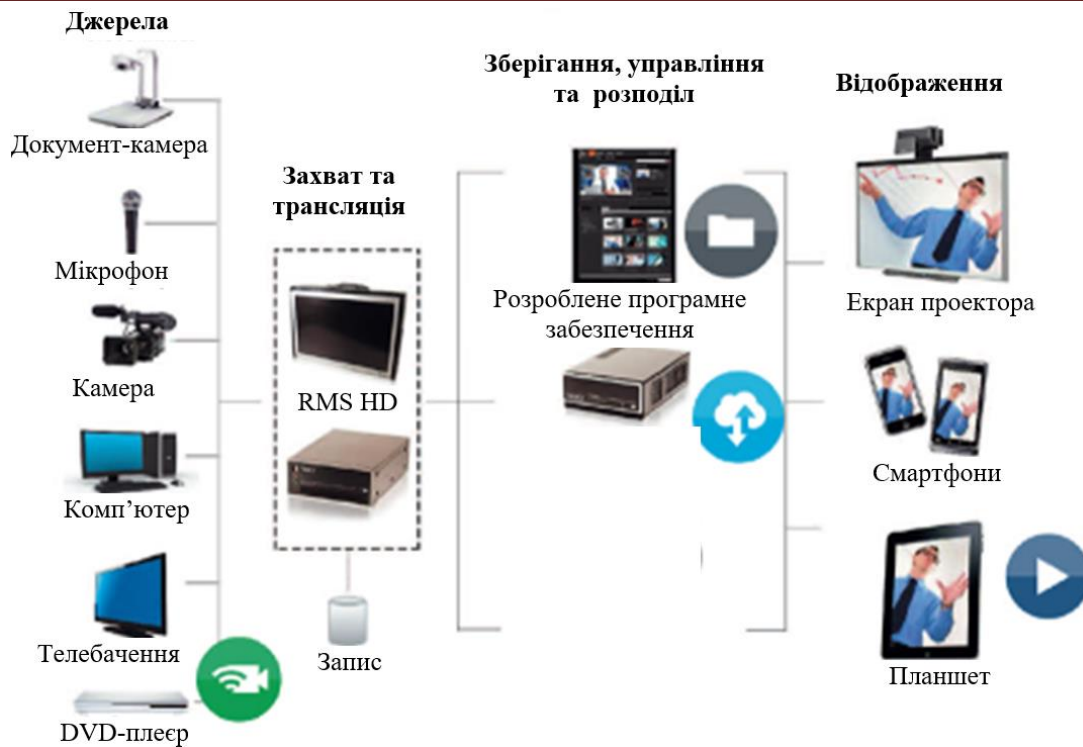


Рисунок 1 – Структурна схема системи

Коли ми ділимося відео на YouTube, ми можемо лише скопіювати посилання для поширення, щоб поділитися ним у ваших соціальних мережах, електронною поштою або текстовим повідомленням. Навпаки, корпоративні платформи дозволяють вам підкреслити свою оригінальність. Наприклад, ми надаємо вам можливість персоналізувати вашу сторінку спільного доступу. Для професійного результату ви можете додати свій логотип та персоналізувати кольори.

– Посилена безпека. Ваша конфіденційність поважається по-різному на корпоративній відеоплатформі:

- Ваші відео та посилання для поширення захищені паролями.
- Щоб ви могли легко та швидко входити в систему, приватна платформа може бути узгоджена з вашою системою єдиного входу.
- Для більшої конфіденційності ваша аудиторія обмежена. Таким чином, ви можете керувати правами доступу, вибираючи осіб, які можуть переглядати ваші відео.
- Простір для співпраці. Ідеально підходять для компаній, платформи EvRP дозволяють вам об'єднувати ваші відео у відеотеці. Якщо ви хочете об'єднати свої відео зі своїми колегами, ця платформа створена для вас!

Крім того, ви можете ділитися своїми внутрішніми відео зі своїми колегами завдяки персоналізованому корпоративному веб-телебаченню, яке ми пропонуємо на нашій приватній відеоплатформі.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів мережевого управління корпоративними відеоресурсами на основі технології EvRP. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем мережевого управління корпоративними відеоресурсами на основі технології EvRP.
- Досліджена система мережевого управління корпоративними відеоресурсами на основі технології EvRP.

– На основі отриманих результатів досліджень створена програмна реалізація системи мережевого управління корпоративними відеоресурсами на основі технології EvRP.

Розроблені алгоритми дозволяють успішно вирішувати завдання мережевого управління корпоративними відеоресурсами на основі технології EvRP. Проведено аналіз

предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Kuznetsov, O., Frontoni, E., Kryvinska, N., Smirnov, O., Imoize, G.L. «Computational Modeling of Enhanced Spread Spectrum Codes for Asynchronous Wireless Communication». *Computational Modeling and Simulation of Advanced Wireless Communication Systems*, 2024, pp. 403–447
2. Смірнова Т.В., Коноплицька-Слободенюк О.К., Буравченко К.О., Смірнов С.А., Кравчук О.В., Козірова Н.Л., Смірнов О.А. «Дослідження технологій забезпечення кібербезпеки хмарних сервісів IaaS, PaaS та SaaS». *Кібербезпека: освіта, наука, техніка*. 2024. №4(24), С. 6-27.
3. Батрак О., Смірнова Т., Гнатюк В., Одарченко Р., Смірнов О. «Дослідження показників ефективності функціонування та перспектив розвитку систем IP-телефонії». *Підводні технології*, 2024, № 13, с. 28-35.
4. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». *Advanced Information Systems*, 2023, 7(2), pp. 49-56.
5. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchey, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». *CEUR Workshop Proceedings*, Volume 3530, 2023, pp. 256-265.
6. Smirnov, O., Odarchenko, R., Smirnova, T., Bondar, S., Volosheniuk, D. «Optimal Structure Construction of Private 5G Network for the Needs of Enterprises». *Lecture Notes on Data Engineering and Communications Technologies*, 2023, 178, pp. 208–223.
7. Аль-Мудхафар Акіл Абдулхуссейн М., Смірнова Т.В., Буравченко К.О., Смірнов О.А. «Метод оцінки та підвищення користувальницького досвіду абонентів в програмно-конфігурованих мережах на основі використання машинного навчання». *Сучасні інформаційні системи*, 2023, том 7, № 2, С. 49-56.
8. Smirnov, O., Neskoroedieva, T., Fedorov, E., Rudakov, K., Neskoroedieva, A. «Method Detection Audit Data Anomalies on Basis Restricted Cauchy Machine» *CEUR Workshop Proceedings*, Volume 3187, 2022,
9. Smirnov O., Smirnova T., Anas M. Al-Oraiqat, Drieiev O., Polishchuk L., Sheraz Khan, Yassin M. Y. Hasan, Aladdein M. Amro, Hazim S. AlRawashdeh «Method for Determining Treated Metal Surface Quality Using Computer Vision Technology». *Sensors (Basel, Switzerland)* Volume 22, Issue 16, 6223, 2022.
10. Smirnov O., Kuznetsov A., Kryvinska N., Kiian A., Kuznetsova K. «Full Non-Binary Constant-Weight Codes». *SN Computer Science*, Vol 2, 337, 2021. <https://doi.org/10.1007/s42979-021-00739-w>
11. Smirnov O., Kuznetsov A., Zhora V., Onikiychuk A., Pieshkova O. «Hiding Messages in Audio Files Using Direct Spread Spectrum». 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2021, Cracow, Poland, 22-25 September 2021. P. 414-418.
12. Smirnov O., Kuznetsov A., Lokotkova I., Kuznetsova T., Florov S., Lebid O. «Using Orthogonal Signals to Hide Information in Images». 4 IEEE International Conference on Advanced Information and Communication Technologies (AICT) - 2021, Lviv, Ukraine, September 21-25, 2021. P. 255-260.
13. Smirnov, O., Kuznetsov, A., Potii, O., Poluyanenko, N., Stelnyk, I., Mialkovsky, D. «Combining and filtering functions in the framework of nonlinear-feedback shift register». *International Journal of Computing*; 2020, Volume 19, Issue 2 – Research Institute for Intelligent Computer Systems – 2020. – P. 247-256.
14. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». *CEUR Workshop Proceedings*. Volume 2740, 2020, Pages 102-114.
15. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». *Journal of theoretical and applied information technology* Vol.98. No 21, 2020, P. 3334-3346.
16. Smirnov O., Kuznetsov A., Kovalchuk D., Kuznetsova T. «New technique for data hiding in cover images using adaptively generated pseudorandom sequences». *CEUR Workshop Proceedings* Volume 2654, 2020, Pages 1-14.
17. Smirnov O., Kuznetsov A., Onikiychuk A., Makushenko T., Anisimova O., Arischenko A. «Adaptive pseudorandom sequence generation for spread spectrum image steganography». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 161-165.
18. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177.
19. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) *Data-Centric Business and Applications*. *Lecture Notes on Data Engineering and Communications Technologies*, vol 48. Springer, Cham. 2021. pp 557-587.
20. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». *CEUR Workshop Proceedings* Volume 2616, 2020, Pages 366-379.

21. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645.
22. Smirnov, O., Kuznetsov, A., Gorbacheva, L., Babenko, V., «Hiding data in images using a pseudo-random sequence», CEUR Workshop Proceedings Volume 2608, 2020, Pages 646-660.
23. Zhurakovskiy, B., Tsopa, N., Batrak, Y., Odarchenko, R., Smirnova, T «Comparative analysis of modern formats of lossy audio compression». Workshop Proceedings, 2020, 2654, стр. 315-327.
24. Smirnov O. Kuznetsov A., Zaichenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019; Odessa; Ukraine; 9-13 September 2019. P.22-28.
25. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.
26. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019 . P.517-522.
27. Smirnov, O., Krasnobayev, V., Yanko, A., Kuznetsova, T. «Methods of nulling numbers in the system of residual classes». CEUR Workshop Proceedings, Vol 2588, P. 90-106, 2019.
28. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Averchev, A., Pastukhov, M., Kuznetsova, K., «Formation of Pseudorandom Sequences with Special Correlation Properties», 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT -2019/ Lviv, Ukraine, 2-6 July, 2019, P. 395-399.
29. Smirnov, O., Kuznetsov, A., Kavun, S., Babenko, B., Nakisko, O., Kuznetsova, K., «Malware Correlation Monitoring in Computer Networks of Promising Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 347-352.
30. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Pastukhov, M., Kuznetsova, K., Prokopovych-Tkachenko, D., «Discrete Signals with Special Correlation Properties», CEUR Workshop Proceedings Volume 2353, CEUR Workshop Proceedings 2019, Pages 618-629.
31. Smirnov A.A., Kuznetsov A.A., Danilenko D.A., Berezovsky A., «The statistical analysis of a network traffic for the intrusion detection and prevention systems», Telecommunications and Radio Engineering. – Volume 74, Issue 1. – Begel House Inc. – 2015. – P. 61-78.

УДК 004

В.Павлюхін, магістр гр. КІ-24М,*Центральноукраїнський національний технічний університет*

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ КОНТЕЙНЕРНОЇ ВІРТУАЛІЗАЦІЇ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ДЛЯ ХОСТИНГУ

У статті розроблено програмне забезпечення, яке призначено для системи контейнерної віртуалізації мережевої інфраструктури для хостингу. Метою розробки є дослідження та принципи побудови системи контейнерної віртуалізації мережевої інфраструктури для хостингу. Об'єктом дослідження є процес контейнерної віртуалізації мережевої інфраструктури для хостингу. Предметом дослідження є методи контейнерної віртуалізації мережевої інфраструктури для хостингу. Методи дослідження базуються на методах побудови комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи контейнерної віртуалізації мережевої інфраструктури для хостингу. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

контейнерна віртуалізація, мережева інфраструктура, хостинг

Постановка проблеми. З появою контейнеризації 10 років тому ми побачили компактний, зручний та портативний спосіб запуску програм безпосередньо одночасно з віртуалізацією. Основна відмінність полягає в архітектурі. Контейнери мають те саме ядро, що й гостьова система, і тому не віртуалізують низькорівневі компоненти, такі як центральний процесор (ЦП).

З одного боку, вони легші та гнучкіші, ніж віртуальні машини (VM). З іншого боку, VM можуть точніше задовольняти потреби низькорівневих компонентів і є повністю автономними системами. Яка архітектура найкраще підходить для розробки програми сьогодні?

У даній магістерській роботі ми вивчимо два основні віртуальні методи розгортання. Ми порівняємо обидва методи за кількома критеріями: сумісність на основі користувацького досвіду та простота встановлення/розгортання, масштабованість на основі автоматичної еластичності робочого навантаження та енергоефективність з точки зору енергії та комп'ютерних ресурсів. Після тестів ми розробимо програмну реалізацію системи контейнерної віртуалізації мережевої інфраструктури для хостингу.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи контейнерної віртуалізації мережевої інфраструктури для хостингу.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи контейнерної віртуалізації мережевої інфраструктури для хостингу.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем контейнерної віртуалізації мережевої інфраструктури для хостингу.
- Дослідження системи контейнерної віртуалізації мережевої інфраструктури для хостингу.
- Програмна реалізація системи контейнерної віртуалізації мережевої інфраструктури для хостингу.

Об'єктом дослідження є процес контейнерної віртуалізації мережевої інфраструктури для хостингу.

Предметом дослідження є методи контейнерної віртуалізації мережевої інфраструктури для хостингу.

Методи дослідження базуються на методах побудови комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Віртуалізація – це процес використання програмного забезпечення для створення віртуального ресурсу, який працює на окремому рівні від фізичного обладнання. Найпоширенішим випадком використання віртуалізації є хмарні обчислення.

Ви можете запускати кілька віртуальних машин на одному комп'ютері за допомогою віртуалізації. Ці віртуальні машини є незалежними системами, але мають спільну фізичну ІТ-інфраструктуру та керуються гіпервізором.

Віртуалізація набула величезного значення в останній галузі програмного забезпечення. Очікується, що до 2026 року світовий ринок віртуалізації додатків становитиме 5,76 мільярда доларів. Це пояснюється тим, що віртуалізація дозволяє користувачам отримувати доступ до додатків і функцій без їх встановлення на комп'ютер.

Ця хмарна технологія економить гроші, час і місце для зберігання, пропонуючи всі можливості хмарних обчислень. Від неї вигоду отримують як великі підприємства, так і малий бізнес. Деякі з переваг віртуалізації:

- Доступність усіх ресурсів ОС для програм.
- Добре налагоджена функціональність.
- Кращі інструменти та засоби контролю безпеки.
- Надійні інструменти управління.
- Економія коштів та висока ефективність.
- Централізоване робоче навантаження без накладних витрат.

VirtualBox, VMware Workstation Player та Microsoft Hyper-V є найпопулярнішими постачальниками віртуальних машин.

Обмеження віртуалізації

Віртуалізація – це потужна технологія, яка має багато переваг, але також має кілька обмежень, про які слід знати. Деякі з основних обмежень віртуалізації включають:

- Для роботи кількох операційних систем та віртуальної копії обладнання потрібні значні ресурси оперативної пам'яті та процесора.
- Перехід між приватними та публічними хмарами та центрами обробки даних ускладнює життєвий цикл розробки програмного забезпечення.
- Він монолітний і запускає програми як окремі великі файли.
- Додає обчислювальні ресурси та дуже швидко циклічно перезавантажується/завантажується.
- Він не запускає деякі програми належним чином.
- Деякі старіші або спеціалізовані програми можуть бути несумісними з програмним забезпеченням для віртуалізації або можуть вимагати додаткового налаштування для належної роботи.

– Віртуалізовані середовища можуть бути не такими простими в масштабуванні, як фізичні, особливо коли йдеться про додавання додаткових апаратних ресурсів.

Контейнери – це засіб ізоляції програми від її оточення шляхом інкапсуляції її залежностей та конфігурацій в одному блоці. Після цього цей блок можна перенести в інші середовища, такі як приватні хмари, публічні хмари та центри обробки даних.

Контейнери є легшими та гнучкішими, коли справа доходить до віртуалізації вашого середовища без гіпервізора. Вони дозволяють DevOps зосередитися на розробці та розгортанні коду, що забезпечує швидше надання ресурсів. Контейнеризований додаток поводить себе послідовно в середовищах розробки, тестування та виробництва.

Як згадувалося раніше, контейнеризація – це процес пакування кожного компонента, необхідного для запуску програми або мікросервісу, включаючи пов'язані бібліотеки. Кожен

контейнер складається з коду, залежностей та самої ОС. Це дозволяє програмам працювати однаково на різних платформах.

Контейнеризація – це форма віртуалізації ОС, яка використовує можливості операційної системи для ізоляції процесів та контролю їх доступу до пам'яті, дискового простору та процесорів.

Поширення контейнеризації розпочалося з Docker, платформи з відкритим кодом для створення, розгортання та управління контейнерними додатками. З її появою у 2013 році технологія та екосистема контейнерів зазнали значного розвитку.

Деякі переваги контейнеризації:

- Зменшення завантаженості ресурсів управління ІТ.
- Вимоги до меншого розміру.
- Швидше завантаження та спрощені оновлення безпеки.
- Менше коду для міграції, перенесення або завантаження робочих навантажень.
- Швидша доставка.
- Легше управління.

Контейнеризація працює шляхом спільного використання ядра хост-ОС з іншими контейнерами як ресурсу лише для читання. Ви можете розгорнути кілька контейнерів на одному сервері або віртуальній машині, оскільки вони легкі та масштабовані.

Таким чином, ви підтримуєте лише одну ОС і не присвячуєте цілий сервер одній програмі. Контейнеризація є відповіддю на кілька проблем DevOps. Саме тому багато підприємств застосовують цей підхід для міграції керованих сервісів у хмару.

Контейнери дозволяють розбивати програми на найменші компоненти або мікросервіси. Ці сервіси розробляються та розгортаються незалежно, що усуває монолітність.

Наприклад, якщо ви підтримуєте кілька кнопок дій на своєму веб-сайті, збій однієї з них не впливає на продуктивність інших. Це зменшує час простою, навантаження на обслуговування та залежність.

Обмеження контейнеризації

Як і віртуальні машини, контейнери також мають деякі обмеження.

- Усі контейнери повинні працювати на схожих операційних системах.
- Якщо контейнери базуються на іншій ОС, їм потрібен інший хост.
- Вони можуть створювати вразливості безпеки в ядрі ОС, оскільки всі контейнери на хост-машині використовують цю ОС.
- Це рішення все ще розробляється та вдосконалюється, тому його впровадження може бути складнішим.

Контейнеризація та віртуалізація мають свої сильні та слабкі сторони. Вони використовуються незалежно для задоволення потреб вашого бізнесу. Їх також можна використовувати разом для створення ефективної ІТ-інфраструктури для DevOps.

1. Ізоляція

Контейнери та віртуальні машини забезпечують різні ступені ізоляції. Контейнерній системі потрібна базова ОС для надання базових послуг усім контейнеризованим програмам. З іншого боку, гіпервізор запускає віртуальні машини зі своєю ОС, яка використовує апаратну підтримку.

В результаті, контейнерні системи мають менші накладні витрати, ніж віртуальні машини, і зазвичай орієнтовані на середовища з тисячами контейнерів. Вони забезпечують ізоляцію сервісів між контейнерами, тоді як віртуальна машина забезпечує повністю ізольоване середовище. Це призводить до обмеженого доступу до ресурсів для контейнерних сервісів, таких як файлові системи.

Щоб поєднати можливості контейнеризації та віртуалізації, можна обрати паравіртуалізацію. Вона ізолює програми завдяки підтримці віртуальної пам'яті та вимагає спеціальних драйверів пристроїв у віртуальній машині, підключеній до ОС через гіпервізор.

Простіше кажучи, віртуальні машини, якими керують гіпервізори, використовують обладнання віртуальної машини, тоді як контейнерні системи надають служби ОС від базового хоста для ізоляції програм за допомогою обладнання віртуальної пам'яті.

2. Операційна система

Контейнери та віртуальні машини суттєво відрізняються з точки зору автономності ОС. Контейнери дотримуються віртуалізації ОС, що означає, що вони використовують ресурси хост-ОС. З іншого боку, кожен екземпляр у віртуальній машині є повноцінною гостьовою ОС сам по собі.

Таким чином, віртуальна машина містить гостьову ОС, віртуальну копію обладнання для її запуску, програму, її бібліотеки та залежності. Вона може запускати різні операційні системи на одному фізичному сервері. Оскільки контейнери віртуалізують ОС, вони містять лише програму з її бібліотеками та залежностями.

Оскільки екземпляр віртуальної машини віртуалізує всю ОС, він зрештою додає компоненти, не пов'язані з вашою програмою. Однак, незалежно від типу операційної системи, контейнери ізолюють лише ресурси, від яких залежить ваша програма. Тому вони мають більшу гнучкість ОС, ніж віртуальні машини.

Віртуалізація ОС дозволяє перенести вашу програму на іншу систему, не впливаючи на її розробку та розгортання. Це відповідає потребам багатохмарних та гібридних рішень, зменшуючи ризики прив'язки до постачальника та забезпечуючи плавний перехід з незначними накладними витратами.

3. Сумісність з гостями

Віртуальні машини сумісні майже з усіма операційними системами на хості, тоді як контейнери сумісні лише з версією операційної системи, подібною до версії хоста. Хоча віртуальні машини з'явилися раніше та широко використовувалися протягом багатьох років, контейнери зараз є найкращим вибором для DevOps у багатьох відношеннях.

Нові технології та інновації зазвичай створюються для контейнерних середовищ. Крім того, доступно багато образів контейнерів з відкритим кодом, попередньо зібраних та налаштовуваних. Попередньо зібрані образи для віртуальних машин також доступні, але їх важко налаштувати та забезпечити сумісність.

4. Контейнеризація проти віртуалізації: розгортання

У цьому відношенні контейнеризація також пропонує більшу гнучкість. Існує лише кілька кроків для розгортання програми за допомогою віртуальної машини.

1. Збірка та налаштування віртуальної машини.
2. Встановлення програми на основі цільової ОС.
3. Опублікуйте додаток на платформі на ваш вибір.

Але цей процес тривалий та ресурсомісткий.

Щоб розгорнути контейнеризований застосунок, ви можете отримати образ та розгорнути його на будь-якій сумісній платформі. Це швидкий процес, який не такий ресурсомісткий, як віртуальна машина.

5. Постійне зберігання

Контейнери та віртуальні машини відрізняються тим, як їм потрібна інфраструктура зберігання даних та як вона використовується. Це впливає на проектування вашої ІТ-інфраструктури та допомагає максимізувати цінність середовища застосунків.

Контейнери є тимчасовими, тобто вони запускаються та зупиняються автоматично. Це не стосується віртуальних машин. Однак, обом потрібен доступ до постійного сховища у виробничому середовищі. Без цього доступу контейнер завершує роботу, і дані стають недоступними.

Якщо ви використовуєте контейнеризацію корпоративного рівня, вам потрібно налаштувати постійне середовище зберігання, яке підтримує контейнери.

6. Балансування навантаження

Балансування навантаження віртуальних машин передбачає переміщення запущених віртуальних машин на інші вузли для відмовостійкого кластера. З іншого боку, контейнери

можуть автоматично запускатися або зупинятися на вузлах кластера залежно від змін навантаження.

У цьому випадку змінюється лише доступність, але самі контейнери не переміщуються.

7. Нетворкінг

Контейнери використовують ізольований вигляд віртуального мережевого адаптера для легкої віртуалізації, оскільки вони спільно використовують брандмауер хоста. Віртуальні машини використовують повну віртуалізацію з VNA.

Контейнеризація проти віртуалізації: що підходить саме вам?

Як контейнери, так і віртуальні машини (VM) мають свої переваги. Вам слід обрати контейнеризацію, щоб максимізувати кількість програм на мінімальних серверах. Це також правильний вибір для розгортання хмарних програм, упаковки мікросервісів та переміщення масштабованих програм між ІТ-середовищами з однією й тією ж ОС.

Як варіант, віртуальні машини можуть виконувати більше операцій і найкраще підходять для монолітних робочих навантажень, що вимагають повної функціональності ОС. Вибирайте віртуальні машини, якщо ваш застосунок не потребує портативності, і ви хочете розміщувати застарілі застосунки, ізолювати ризиковані середовища розробки та виділити ІТ-ресурси, такі як сервери, сховища та мережі.

Ви також можете використовувати контейнери та віртуальні машини разом для оптимізації ємності та використання сервера. Інтеграція контейнерів у віртуальні машини дозволяє командам DevOps підвищити ефективність фізичного сервера та зменшити кількість збоїв.

Гіпервізор працює в такий спосіб: операційна система хоста емулює апаратне забезпечення, поверх якого вже запускаються гостьові операційні системи. Це означає, що взаємозв'язок між гостьовою й хостовою операційними системами треба «залізній» парадигмі: усе, що «уміє» робити встаткування, повинне бути доступно гостьовий ОС із боку хостової. Навпроти, контейнери – це віртуалізація на рівні операційної системи, а не встаткування, тобто кожна гостьова ОС використовує те ж саме ядро (а в деяких випадках – і інші частини ОС), що й хостова. Це дає контейнерам велику перевагу: вони менше й компактніше гіпервізорних гостьових середовищ, оскільки в них з хостом набагато більше загального.



Рисунок 1 – Структурна схема системи

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів контейнерної віртуалізації мережевої інфраструктури для хостингу. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем контейнерної віртуалізації мережевої інфраструктури для хостингу.
- Досліджена система контейнерної віртуалізації мережевої інфраструктури для хостингу.
- На основі отриманих результатів досліджень створена програмна реалізація системи контейнерної віртуалізації мережевої інфраструктури для хостингу.

Розроблені алгоритми дозволяють успішно вирішувати завдання контейнерної віртуалізації мережевої інфраструктури для хостингу. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Smirnov O., Smirnova T., Anas M. Al-Oraiqat, Drieiev O., Polishchuk L., Sheraz Khan, Yassin M. Y. Hasan, Aladdein M. Amro, Hazim S. AlRawashdeh «Method for Determining Treated Metal Surface Quality Using Computer Vision Technology». Sensors (Basel, Switzerland) Volume 22, Issue 16, 6223, 2022.
2. Smirnov O., Kuznetsov A., Kryvinska N., Kiian A., Kuznetsova K. «Full Non-Binary Constant-Weight Codes». SN Computer Science, Vol 2, 337, 2021. <https://doi.org/10.1007/s42979-021-00739-w>
3. Smirnov O., Kuznetsov A., Zhora V., Onikiychuk A., Pieshkova O. «Hiding Messages in Audio Files Using Direct Spread Spectrum». 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2021, Cracow, Poland, 22-25 September 2021. P. 414-418.
4. Smirnov O., Kuznetsov A., Lokotkova I., Kuznetsova T., Florov S., Lebid O. «Using Orthogonal Signals to Hide Information in Images». 4 IEEE International Conference on Advanced Information and Communication Technologies (AICT) - 2021, Lviv, Ukraine, September 21-25, 2021. P. 255-260.
5. Smirnov, O., Kuznetsov, A., Potii, O., Poluyanenko, N., Stelnyk, I., Mialkovsky, D. «Combining and filtering functions in the framework of nonlinear-feedback shift register». International Journal of Computing; 2020, Volume 19, Issue 2 – Research Institute for Intelligent Computer Systems – 2020. – P. 247-256.
6. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
7. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». Journal of theoretical and applied information technology Vol.98. No 21, 2020, P. 3334-3346.
8. Smirnov O., Kuznetsov A., Kovalchuk D., Kuznetsova T. «New technique for data hiding in cover images using adaptively generated pseudorandom sequences». CEUR Workshop Proceedings Volume 2654, 2020, Pages 1-14.
9. Smirnov O., Kuznetsov A., Onikiychuk A., Makushenko T., Anisimova O., Arischenko A. «Adaptive pseudorandom sequence generation for spread spectrum image steganography». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 161-165.
10. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177.
11. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587.
12. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». CEUR Workshop Proceedings Volume 2616, 2020, Pages 366-379.
13. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645.
14. Smirnov, O., Kuznetsov, A., Gorbacheva, L., Babenko, V., «Hiding data in images using a pseudo-random sequence», CEUR Workshop Proceedings Volume 2608, 2020, Pages 646-660.
15. Zhurakovskiy, B., Tsopa, N., Batrak, Y., Odarchenko, R., Smirnova, T «Comparative analysis of modern formats of lossy audio compression». Workshop Proceedings, 2020, 2654, стр. 315-327.
16. Smirnov O. Kuznetsov A., Zaichenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete

- Signals with Special Correlation Properties». International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019; Odessa; Ukraine; 9-13 September 2019. P.22-28.
17. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.
 18. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019 . P.517-522.
 19. Smirnov, O., Krasnobayev, V., Yanko, A., Kuznetsova, T. «Methods of nulling numbers in the system of residual classes». CEUR Workshop Proceedings, Vol 2588, P. 90-106, 2019.
 20. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Averchev, A., Pastukhov, M., Kuznetsova, K., «Formation of Pseudorandom Sequences with Special Correlation Properties», 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT -2019/ Lviv, Ukraine, 2-6 July, 2019, P. 395-399.
 21. Smirnov, O., Kuznetsov, A., Kavun, S., Babenko, B., Nakisko, O., Kuznetsova, K., «Malware Correlation Monitoring in Computer Networks of Promising Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 347-352.
 22. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Pastukhov, M., Kuznetsova, K., Prokopovych-Tkachenko, D., «Discrete Signals with Special Correlation Properties», CEUR Workshop Proceedings Volume 2353, CEUR Workshop Proceedings 2019, Pages 618-629.
 23. Smirnov A.A., Kuznetsov A.A., Danilenko D.A., Berezovsky A., «The statistical analysis of a network traffic for the intrusion detection and prevention systems», Telecommunications and Radio Engineering. – Volume 74, Issue 1. – Beggel House Inc. – 2015. – P. 61-78.
 24. Smirnov O., Kuznetsov A., Kovalchuk D., Kuznetsova T. «New Technique for Hiding Data in Cover Images Using Adaptively Generated Pseudorandom Sequences». CEUR Workshop Proceedings Volume 2732, 2020, Pages 214-227.
 25. Т.В. Смірнова, О.М. Дреєв, О.А. Смірнов «Хмарна інформаційна система оцінювання шорсткості з використанням дискретного частотного аналізу макротографій». IV міжнародна науково-практична конференція “Інформаційна безпека та комп’ютерні технології”, м. Кропивницький. 15-16 квітня 2021р. – Кропивницький: ЦНТУ. – 2021. – С. 30.
 26. О.А. Смірнов, П.С. Усік, «дослідження перспектив використання технологічних рішень в мережах 5g» у Кібербезпека та інформаційні технології: монографія. – Х. : ТОВ «ДІСА ПЛЮС», 2020.С. 122-135.
 27. О.А.Смірнов, Т.В.Смірнова, Л.І. Поліщук, К.О. Буравченко, А.О.Макевнін, «Дослідження хмарних технологій як сервісів», Кібербезпека: освіта, наука, техніка. № 3(7). С. 43-62. 2020.
 28. Смірнов О.А., Дреєва Г.М., Дреєв О.М., Смірнова Т.В. «Фрактальний аналіз генератора самоподібного трафіку на основі ланцюга Маркова». Центральнотрапінський науковий вісник. Технічні науки. № 2(33). с. 161-172, 2019.
 29. О. Смірнов, Є. Деменко, О. Онікійчук, А. Арищенко, Л. Горбачова, «Формування псевдовипадкових послідовностей для приховування даних в зображеннях» Комп’ютерні науки та кібербезпека. № 4. С. 30-37. 2019.
 30. Смірнов О.А., Коноплицька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В. Поліщук Л.І. Проектування комп’ютерних систем та мереж. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2019. – 264 с.
 31. Smirnov, O., Kuznetsov, A., Kuznetsova, K. Synthesis of Discrete Signals with Improved Correlation Properties. Монографія: In.: ISCI’2019: Information Security in Critical Infrastructures. Collective monograph. Edited by Ivan D. Gorbenko and Alexandr A. Kuznetsov, ASC Academic Publishing, USA, 2019, pp. 281-299. – ISBN: 978-0-9989826-8-7 (Hardback), ISBN: 978-0-9989826-9-4 (Ebook).

УДК 004

О.Бершадський, магістр гр. КІ-24М,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ЕМУЛЯТОРА ПЕРЕТВОРЕННЯ ЛОГІЧНОЇ АДРЕСИ В ЛІНІЙНУ ТА ЛІНІЙНОЇ У ФІЗИЧНУ ДЛЯ НАВЧАЛЬНИХ ЦІЛЕЙ

У статті розроблено програмне забезпечення, яке призначено для системи емулятора перетворення логічної адреси в лінійну та лінійної у фізичну для навчальних цілей. Метою розробки є дослідження та принципи побудови системи емулятора перетворення логічної адреси в лінійну та лінійної у фізичну для навчальних цілей. Об'єктом дослідження є процес емулятора перетворення логічної адреси в лінійну та лінійної у фізичну для навчальних цілей. Предметом дослідження є методи емулятора перетворення логічної адреси в лінійну та лінійної у фізичну для навчальних цілей. Методи дослідження базуються на методах комп'ютерної логіки, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи емулятора перетворення логічної адреси в лінійну та лінійної у фізичну для навчальних цілей. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

Емулятор, перетворення логічної адреси в лінійну та лінійної у фізичну, навчальні цілі

Знання обчислювальних пристроїв, включаючи реалізацію програмного забезпечення на машинному рівні. Кілька курсів у навчальних програмах з інформатики розглядають ці низькорівневі деталі, такі як архітектура комп'ютера та мови асемблера. Для таких курсів є переваги у вивченні реальних архітектур замість спрощених прикладів. Однак реальні архітектури та набори інструкцій вносять складність, що ускладнює їх опанування в рамках одного семестру. Методи візуалізації можуть допомогти полегшити це навантаження, на жаль, існуючі інструменти часто важко використовувати, а отже, важко впроваджувати в курсі, де час вже обмежений. Щоб вирішити цю проблему, у даній роботі розробляється програмне забезпечення емулятора перетворення логічної адреси в лінійну та лінійної у фізичну для навчальних цілей. Дане програмне забезпечення графічно ілюструє ключові відмінності між знайомими мовами високого рівня та незнайомими мовами низького рівня, а також ілюструє, як знайомі програми високого рівня поведуться на реальних архітектурах. Ключем до цього інструменту є те, що ми використовуємо простий веб-інтерфейс, який не потребує налаштування, що полегшує перешкоди для впровадження курсу. Ми також включаємо кілька функцій, які ще більше підвищують його корисність в умовах класу. Ці функції включають графічні зв'язки між кодом високого рівня та машинним кодом, чітко проілюстровані покрокові переходи станів машини, кольорове кодування для зрозумілості поведінки інструкцій та ілюстрацію вказівників.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи емулятора перетворення логічної адреси в лінійну та лінійної у фізичну для навчальних цілей.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи емулятора перетворення логічної адреси в лінійну та лінійної у фізичну для навчальних цілей.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем емулятора перетворення логічної адреси в лінійну та лінійної у фізичну для навчальних цілей.
- Дослідження системи емулятора перетворення логічної адреси в лінійну та лінійної у фізичну для навчальних цілей.
- Програмна реалізація системи емулятора перетворення логічної адреси в лінійну та лінійної у фізичну для навчальних цілей.

Об'єктом дослідження є процес емулятора перетворення логічної адреси в лінійну та лінійної у фізичну для навчальних цілей.

Предметом дослідження є методи емулятора перетворення логічної адреси в лінійну та лінійної у фізичну для навчальних цілей.

Методи дослідження базуються на методах комп'ютерної логіки, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Проблема підготовки висококваліфікованих фахівців дуже гостро постала у середині двохтисячних років минулого сторіччя, коли на ринку вакансій стали з'являтися усе більше і більше оголошень з потребою у кваліфікованих програмістів, саме фахівців, а не досвідчених користувачів.

На сьогоднішній день, ринок висококваліфікованих фахівців стабілізувався, але все одно кадрові агентства шукають по всій країні вузькоспеціалізованих комп'ютерних фахівців за замовленням приватних підприємців і комп'ютерних фірм.

В процесі навчання у вищих навчальних закладах виникає гостра потреба в добре організованих і детально розроблених навчальних системах.

У даній магістерській дипломній роботі, зроблена спроба реалізувати навчальну систему емулятора перетворення логічної адреси в лінійну та лінійної у фізичну для навчальних цілей.

Коли студент починає вивчати внутрішню будову персонального комп'ютера, він в першу чергу стикається з перетворенням логічної адреси в лінійну та лінійної у фізичну для навчальних цілей.

У рамках архітектури ПК існує й розвивається ряд мікроархитектур. Раніше було показано, що поняття архітектури комп'ютера ієрархично й що існують загальні й індивідуальні властивості архітектури. У контексті обговорення архітектури процесорів Intel має сенс також позиціонувати різні їхні архітектурні властивості й принципи як загальні й індивідуальні.

До індивідуальних архітектурних властивостей і принципів можна віднести існуючі в рамках різних мікроархитектур. Що стосується загальних архітектурних властивостей і принципів IA-64, то до них відносяться ті, які мають місце для всіх процесорів Intel або, принаймні, існують поза рамками конкретної мікроархитектури для великої кількості моделей процесорів. В зв'язку з тим, що процесор в основному визначає логіку роботи комп'ютера, то й назви більшості загальних архітектурних властивостей і принципів IA-64 збігаються з назвами аналогічних властивостей і принципів комп'ютера: номенклатура програмно-доступних регістрів; організація й способи адресації пам'яті; номенклатура режимів роботи процесорів; організація й розрядність зовнішніх інтерфейсів ЕОМ; способи подання й формати даних; набір і формати машинних команд ЕОМ; порядок обробки переривань. Практично всі ці загальні архітектурні властивості й принципи становлять програмну модель процесора, що буде розглянута надалі.

Емулятор процесора – це програмне забезпечення, яке імітує апаратний центральний процесор. Емулятори широко використовуються комп'ютерними фахівцями для різних видів діяльності (наприклад, налагодження, профілювання та аналізу шкідливих програм). Хоча жодні теоретичні обмеження не заважають розробити емулятор, який точно емулює фізичний процесор, написання повнофункціонального емулятора є дуже складним та схильним до помилок завданням. Сучасні архітектури CISC мають дуже багатий набір інструкцій, деяким інструкціям бракує належних специфікацій, а інші можуть мати невизначені ефекти в крайніх випадках. У цій статті представлено методологію тестування,

специфічну для емуляторів процесорів, засновану на фаззингу. Емулятор «навантажується» спеціально створеними тестовими випадками, щоб перевірити, чи правильно емульовано процесор. Неправильна поведінка емулятора виявляється шляхом одночасного запуску одного й того ж тестового випадку на емульованому та на фізичному процесорах та порівняння їх стану після виконання. Різниця в кінцевому стані свідчить про дефекти в коді емулятора.

Варіанти мікроархітектури процесорів Intel

Зовнішня програмна модель (логічна) 64-розрядних процесорів змінювалася тільки у бік розвитку, у той час як їх виконавча (фізична) частина могла бути зроблена різною. Поняття мікроархітектури орієнтоване на опис особливостей виконавчої частини процесорів, тобто того, якими способами і якими засобами процесор виконує обробку машинного коду (рис. 1). На сьогоднішній день у рамках IA-64 існує дві мікроархітектури процесорів Intel: P6 і NetBurst

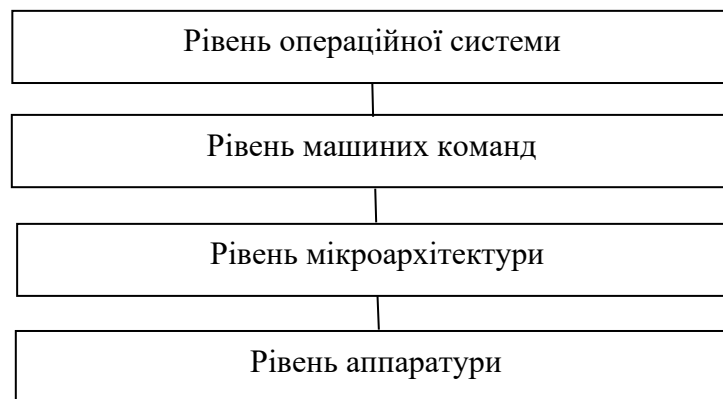


Рисунок 1 – Подання комп'ютера у вигляді рівнів

Мікроархітектура NetBurst. Реалізована в процесорі Pentium IV, є розвитком ідей мікроархітектури P6. Відзначимо найбільш важливі властивості нової мікроархітектури.

- Швидка виконавча частина процесора. АЛП процесора працює на подвоєній частоті процесора.

- Гіперконвеєрна технологія. Гіперконвеєр Pentium IV складається з 20 щаблів. Ціль збільшення довжини конвеєра – спрощення завдань, реалізованих кожної з його щаблів, і, як наслідок, спрощення відповідної апаратної логіки.

- Поліпшена технологія динамічного виконання завдяки більш глибокій «довільності» у порядку виконання коду й удосконаленій системі пророкування переходів.

- Нова підсистема кешування. Відсутній кеш команд першого рівня. Замість нього введений кеш трас. Трасами називаються послідовності мікрооперацій, у які були декодовані раніше обрані команди. Структурна схема процесора Pentium IV показана на рисунку 2.

Мікроархітектура NetBurst підтримує ще одну нову технологію – HyperThreading. Дана технологія дозволяє на базі одного фізичного процесора Pentium IV моделювати декілька логічних, кожний з яких має власний архітектурний простір IA-64. Під архітектурним простором IA-64 розуміється сукупність регістрів даних, сегментних регістрів, системних регістрів і регістрів MSR. Кожний логічний процесор має також власний контролер переривань APIC.

Розглянувши структурну схему процесора перейдемо до розгляду структурної схеми ПЕОМ. При розробці структурної схеми відштовхнемося від внутрішньої архітектурної будови персонального комп'ютера. Структурна схема персонального комп'ютера складається:

- шина PCI (Peripheral Component Interconnect) – шина з'єднання периферійних компонентів, займає особливе місце в PC-архітектурі, є містком між локальною шиною процесора і шиною введення-виведення ISA/EISA чи MCA;

- шина ISA – являє собою паралельну шину, створену на базі шини пам'яті і введення/виведення IBM PC/AT;
- контролер клавіатури – взаємодія з клавіатурою в PC AT базується на двох мікропроцесорах Intel 8042. Один мікропроцесор знаходиться в системному блоці, другий – в клавіатурі.
- контролера прямого доступу в пам'ять – прямий доступ до пам'яті (DMA);
- контролер переривань – в архітектурі PC AT підсистема апаратних переривань складається з двох контролерів 8259A. Вони об'єднані таким чином, що можуть обслужити 15 запитів на переривання;
- послідовний інтерфейс – послідовний інтерфейс RS-232 (KP580BB51);
- паралельний інтерфейс – паралельний порт використовується для підключення принтера до комп'ютера. Також принтер можливо підключити через асинхронний адаптер і USB порт;
- контролер USB – швидкий, двонаправлений, ізохронний, дешевий, послідовний інтерфейс;
- системний таймер – архітектура використовує підсистему трьохканального 16-розрядного таймера 8254, як системний таймер;
- енергонезалежна пам'ять і годинник реального часу – основне призначення енергонезалежної пам'яті – збереження найбільш важливих параметрів системи при відключенні живлення комп'ютера;
- контролер гнучких дисків (Floppy Disk Controller, FDC) – Керування гнучкими дисками здійснюється мікросхемою (контролером) 8272A;
- контролер твердих дисків з інтерфейсами IDE, EIDE і SCSI;
- робота AGP – спеціалізована надбудова над шиною PCI.

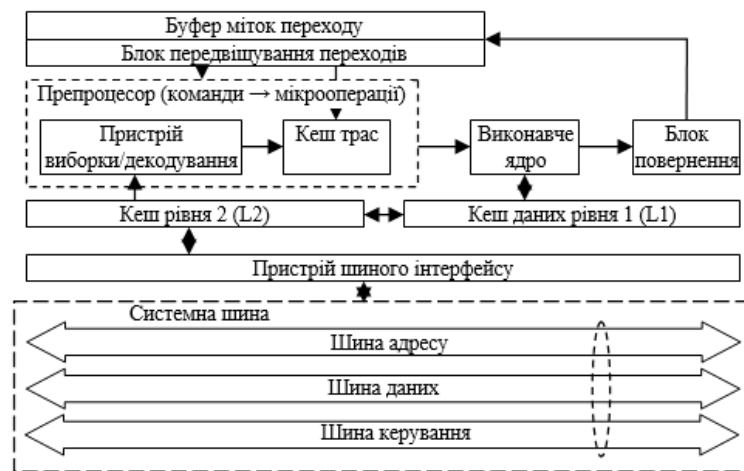


Рисунок 2 – Структурна схема процесора Pentium IV

На рис. 3 зображено розроблену структурну схему системи. Розглянемо її роботу детально.

Користувач через головне вікно ПЗ має можливість перейти до довідкової системи з подальшим переглядом документації та проведенням тестування пройденого матеріалу, перейти до модуля налаштування параметрів роботи ПЗ, налаштувати параметри роботи емулятора перетворення.

З блоку емулятора перетворення ми можемо запуснути моделювання та провести моделювання крок за кроком з виведення інформації кроку на екран. Емулятор дозволяє наявно подивитись як відбувається перетворення логічної адреси в лінійну та лінійної у фізичну для навчальних цілей.

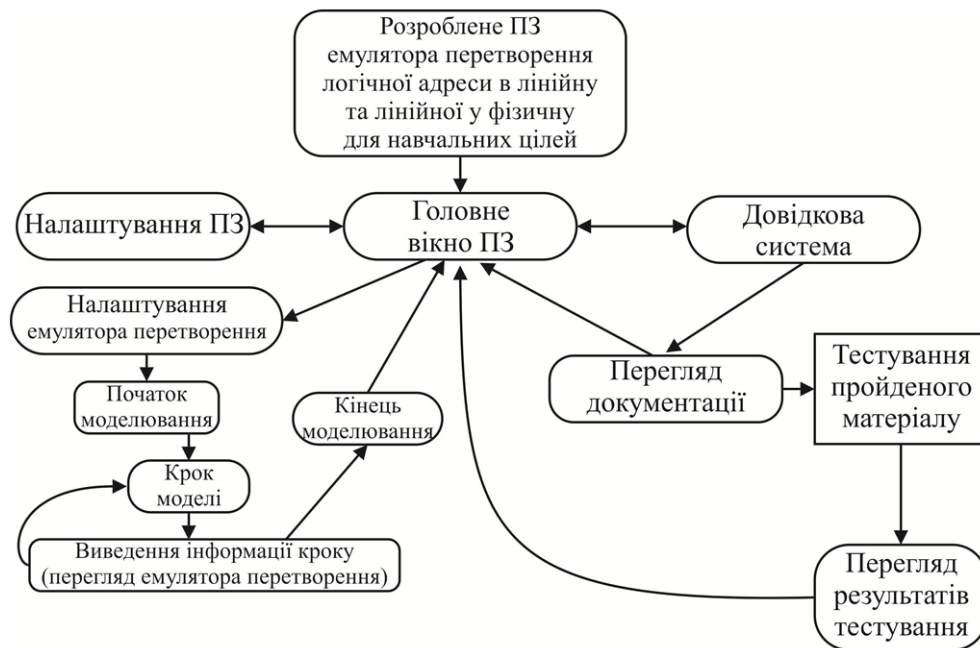


Рисунок 3 – Структурна схема системи

Після кількох важких років, що характеризувалися втратою позицій у сфері штучного інтелекту, зростаючим конкурентним тиском та зменшенням важливості деяких своїх основних продуктів, Intel увійшла у 2025 рік у режимі відновлення. Виробник чіпів робить ставку на нову хвилю ПК зі штучним інтелектом та чіткішу стратегічну спрямованість на відновлення своєї актуальності в нову еру обчислювальної техніки.

Штучний інтелект був провідною силою для всього технологічного сектору, і дуже мало компаній вдавалося дотримуватися своїх принципів без певного впливу ШІ. Intel, більше ніж більшість, була змушена змиритися з власними обмеженнями в цій галузі та переорієнтувати свою діяльність, щоб стати гравцем на ринку ШІ.

Повністю інтегрований чіпсет штучного інтелекту

Компанія агресивно просуває категорію ПК зі штучним інтелектом, спираючись на архітектуру інтегрованого нейронного процесора (NPU) Core Ultra, вперше представлену у 2023 році, та поширюючи своє твердження про те, що робочі навантаження зі штучним інтелектом повинні виконуватися локально на звичайних настільних комп'ютерах та ноутбуках.

Це було ключовим акцентом на виставці CES 2026, де Intel представила Core Ultra Series 3, побудований на новій архітектурі Panther Lake та виробничому процесі вузлів Intel 18A. Продукт об'єднує кілька проектів Intel.

Panther Lake – це спроба зробити свої процесори масштабованими для ширшого спектру ноутбуків, потенційно будучи варіантом для всього, від легких ноутбуків до високопродуктивних настільних комп'ютерів.

Водночас, вузол 18A був частиною плану колишнього генерального директора Пета Гелсінгера щодо значних витрат на ливарні виробництва та дослідження та розробки, щоб знову зробити Intel найкращим у своєму класі у виробництві чіпів.

Схоже, це було певним успіхом, оскільки Intel повідомляє про високий попит на свої чіпи штучного інтелекту та оголосила на CES, що вони вже інтегровані в 200 моделей ноутбуків.

Ранні тести та огляди Core Ultra Series 3 є дуже позитивними завдяки вражаючій ефективності чіпів та покращеній інтеграції з Microsoft Copilot та іншими моделями штучного інтелекту.

Intel вважає, що ринок ПК зі штучним інтелектом, ймовірно, поглине звичайний ринок, прогножуючи, що половина всіх ПК, проданих у 2026 році, матиме вбудовану обробку на базі штучного інтелекту у вигляді нейронних процесорів (NPU).

Intel залишається домінуючим постачальником інтегрованих чіпсетів для ноутбуків і настільних комп'ютерів, тому більшість цих ПК із підтримкою штучного інтелекту працюватимуть на її кремнієвих процесорах.

Ще однією ознакою зміни стратегії Intel є нещодавнє партнерство із SambaNova, яка, як повідомлялося, була метою придбання Intel наприкінці 2025 року.

Дві компанії оголосили про стратегічну багаторічну співпрацю, а також про інвестиції Intel у розмірі від 100 до 150 мільйонів доларів у SambaNova в рамках раунду фінансування на суму 350 мільйонів доларів.

Співпраця передбачатиме інтеграцію SambaNova кремнієвих технологій Intel у архітектуру свого центру обробки даних зі штучним інтелектом, що забезпечить Intel швидкозростаючий стартап у цій галузі.

Штучний інтелект більше не є змаганням у створенні найбільшої моделі. Справжня гонка полягає в тому, хто зможе оновити цілі центри обробки даних за допомогою агентів ШІ, які реагують миттєво, ніколи не зупиняються та роблять це за ціною, яка перетворює ШІ з експерименту на найприбутковіший двигун у хмарі.

SambaNova є прямим конкурентом Intel та NVIDIA у сфері апаратного забезпечення штучного інтелекту, зокрема в робочих навантаженнях логічного виводу та корпоративних рішеннях.

Блок реконфігурованого потоку даних стартапу та оптимізована для потоку даних архітектура чудово підходять для щоденної роботи чат-бота на основі штучного інтелекту або генератора зображень, оскільки вони, як було показано, працюють ефективніше, ніж стандартні графічні процесори, у виконанні рутинних завдань.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів емулятора перетворення логічної адреси в лінійну та лінійної у фізичну для навчальних цілей. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем емулятора перетворення логічної адреси в лінійну та лінійної у фізичну для навчальних цілей.
- Досліджена система емулятора перетворення логічної адреси в лінійну та лінійної у фізичну для навчальних цілей.
- На основі отриманих результатів досліджень створена програмна реалізація системи емулятора перетворення логічної адреси в лінійну та лінійної у фізичну для навчальних цілей. Розроблені алгоритми дозволяють успішно вирішувати завдання емулятора перетворення логічної адреси в лінійну та лінійної у фізичну для навчальних цілей. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Kuznetsov O., Frontoni E., Kuznetsova Y., Chevardin V., Smirnov O. «Architectural foundations for adaptive security in edge computing systems». Cybersecurity Defensive Walls in Edge Computing, 2025. pp. 21-61.
2. Вінтенко, Б.Ю., Миронець, І.В., Смірнов, О.А., Коваленко, О.В., Усік, П.С., Буравченко, К.О., Лисенко, І.А. «Логіко-структурна модель комп'ютерно-орієнтованої процедури системи підтримки оперативного персоналу АЕС». Кібербезпека: освіта, наука, техніка. 2025. Том 2 № 30. С. 413-427, 2025.
3. Смірнова, Т.В. «Дослідження методів, моделей та сучасних ІТ-рішень для підтримки технологічних процесів у критичній інфраструктурі держави». Кібербезпека: освіта, наука, техніка. 2025. Том 2 № 30. С.195-208, 2025.
4. Вінтенко Б., Смірнов О., Миронець І., Смірнова Т., Смірнов С. «Імітаційна модель шляхів вхідних даних комп'ютерної інтелектуальної системи підтримки оператора енергоблоку АЕС». Комбінаторні конфігурації та їхні застосування: Матеріали XXVII Міжнародного науково-практичного семінару, присвяченого 125-річчю Національного університету «Запорізька політехніка» (Запоріжжя-Кропивницький-Київ, 4-6 червня

- 2025 р.). Запоріжжя: НУ «Запорізька політехніка», 2025. С.82-91.
5. Al-Azzeh, J., Ayoub, B., Mesleh, A., Smirnova, T., Gnatyuk, S., Driev, O., Smirnov, O., Dorenskyi, O. «Cloud-Based Information System for Evaluating Caverns in the Process of Blasting Metal Surfaces of Details». *International Review on Modelling and Simulations* 18 (1), 2025. pp. 32-42.
 6. Вінтенко Б.Ю., Смірнов О.А., Миронець І.В., Смірнова Т.В., Коваленко О.В., Мацуй А.М. «Модель шляхів отримання вхідних даних комп'ютерної інтелектуальної системи підтримки оперативного персоналу АЕС». *Центральноукраїнський науковий вісник. Технічні науки*. 2025. Вип. 11(42), ч. II. С.52-62.
 7. Вінтенко Б.Ю., Смірнов О.А., Миронець І.В., Смірнова Т.В. «Методи забезпечення відмовостійкості інтелектуальних систем підтримки оператора». VIII міжнародна науково-практична конференція «Інформаційна безпека та комп'ютерні технології», м. Кропивницький. 24-25 квітня 2025 р. – Кропивницький: ЦНТУ. – 2025. – С. 44-46.
 8. Смірнов, О.А., Константинова, Л.В., Коноплицька-Слободенюк, О.К., Козірова, Н.В., Якименко, Н.М., Доренський, О.П., Буравченко, К.О. «Дослідження інструментів штучного інтелекту для роботи з базами даних та аналізу даних». *Кібербезпека: освіта, наука, техніка*. 2025. №3(27), С. 429–448.)
 9. Smirnov O., Fedorov E., Neskoriy A., Neskoriy T. «Intellectual Classification method of Gymnastic Elements Based on Combinations of Descriptive and Generative Approache». *CEUR Workshop Proceedings Volume 3664*, 2024, Pages 11-23.
 10. Вінтенко, Б., Миронець, І., Смірнов, О., Коваленко, А., Коноплицька-Слободенюк, О., Смірнова, Т., Константинова, Л. «Дослідження застосування систем підтримки оперативного персоналу об'єкту критичної інфраструктури при керуванні енергоблоком АЕС з реактором типу ВВЕР-1000». *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2024. № 2(26), С. 6-26.
 11. Вінтенко, Б., Миронець, І., Смірнов, О., Кравчук, О., Козірова, Н., Савеленко, Г., Коваленко, А. «Дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». *Кібербезпека: освіта, наука, техніка*. 2024. №3(23), С. 111-131.
 12. Kuznetsov O., Ilchenko O., Kryvinska N., Buravchenko K., Smirnov O., Savchenko Iu. «An Empirical Assessment of Leading Blockchain Financial Services». *2023 IEEE 1st Ukrainian Distributed Ledger Technology Forum (UADLTF)*, Kyiv, Ukraine, 2023, pp. 1-6,
 13. Kuznetsov, O., Kryvinska, N., Ilchenko, O., Smirnova, T., Ulianovska, Y. «Comparative Analysis of Cryptocurrency Trading Platforms Using the Analytic Hierarchy Process». *CEUR Workshop Proceedings*, 2023, 3628, pp. 106-115.
 14. Malyukov V., Bebesko B., Lakhno V., Smirnov O., Malyukova I., Mohylnyi H. «Managing the Purchase-Sale Process of Digital Currencies Under Fuzzy Conditions». *Lecture Notes in Networks and Systems*, 2023, 729 LNNS, pp. 104–112.
 15. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». *Advanced Information Systems*, 2023, 7(2), pp. 49-56.
 16. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchov, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». *CEUR Workshop Proceedings, Volume 3530*, 2023, pp. 256-265.
 17. Smirnov, O., Odarchenko, R., Smirnova, T., Bondar, S., Volosheniuk, D. «Optimal Structure Construction of Private 5G Network for the Needs of Enterprises». *Lecture Notes on Data Engineering and Communications Technologies*, 2023, 178, pp. 208–223.
 18. Вінтенко Б.Ю., Смірнов О.А., Коваленко А.С., Смірнов С.А., Буравченко К.О. «Дослідження вимог міжнародних стандартів IEC60880 та IEC62138 з розробки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». *Системи управління, навігації та зв'язку*, 2023, вип. 3(73), С. 155-166.
 19. Вінтенко, Б., Миронець, І., Смірнов, О., Кравчук, О., Козірова, Н., Савеленко, Г., Коваленко, А. «Дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». *Кібербезпека: освіта, наука, техніка*. 2024. №3(23), С. 111-131.
 20. Вінтенко Б.Ю., Смірнов О.А., Коваленко О.В., Смірнов С.А., Коваленко А.С. «Дослідження нормативних документів та галузевих стандартів розробки програмного забезпечення комп'ютерних систем управління АЕС, важливих для безпеки». *Системи управління, навігації та зв'язку*, 2023, вип. 2(72), С. 170-178.
 21. Аль-Мудхафар Акіл Абдулхуссейн М., Смірнова Т.В., Буравченко К.О., Смірнов О.А. «Метод оцінки та підвищення користуальницького досвіду абонентів в програмно-конфігурованих мережах на основі використання машинного навчання». *Сучасні інформаційні системи*, 2023, том 7, № 2, С. 49-56.
 22. Вінтенко Б.Ю., Смірнов О.А., Коваленко О.В., Смірнов С.А. «Дослідження нормативної документації та стандартів розробки програмного забезпечення комп'ютерних систем управління АЕС, важливих для безпеки». VI міжнародна науково-практична конференція «Інформаційна безпека та комп'ютерні технології», м. Кропивницький. 20-21 квітня 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 35-36.
 23. Smirnov, O., Karapetyan, A., Fedorov, E., «Creating Neural Network and Single Solution Human-Based Metaheuristic Methods of Solving the Traveling Salesman Problem». *CEUR Workshop Proceedings, Volume 3312*, 2022, pp. 47-58.
 24. Smirnov O., Kuznetsov A., Kryvinska N., Kiian A., Kuznetsova K. «Full Non-Binary Constant-Weight Codes».

- SN Computer Science, Vol 2, 337, 2021. <https://doi.org/10.1007/s42979-021-00739-w>.
25. Smirnov O., Kovalenko O., Kovalenko A., Kavun S. «Quantitative Risk Assessment Method Development in the Context of the SDLC-model». 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), 2021, pp. 203-208, doi: 10.1109/PICST54195.2021.9772143
 26. Smirnova T., Gnatyuk S., Berdibayev R., Avkurova Zh., Iavich M. «Cloud-Based Cyber Incidents Response System and Software Tools». Communications in Computer and Information Science, 2021, vol 1486. Springer, Cham. pp 169-184.
 27. Smirnov, O., Kuznetsov, A., Potii, O., Poluyanenko, N., Stelnyk, I., Mialkovsky, D. «Combining and filtering functions in the framework of nonlinear-feedback shift register». International Journal of Computing; 2020, Volume 19, Issue 2 – Research Institute for Intelligent Computer Systems – 2020. – P. 247-256.
 28. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
 29. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177.
 30. Smirnov, O., Shekhanin, K., Kuznetsov, A., Krasnobayev, V. «Detecting Hidden Information in FAT». International Journal of Computer Network and Information Security (IJCNIS). Vol. 12, No. 3, 2020. PP.33-43.
 31. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645.

УДК 004

В.Плужник, магістр гр. КІ-24М,

Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ ТА ДОСТУПОМ ДО МЕРЕЖЕВИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

У статті розроблено програмне забезпечення, яке призначено для системи управління ідентифікацією та доступом до мережових інформаційних ресурсів. Метою розробки є дослідження та принципи побудови системи управління ідентифікацією та доступом до мережових інформаційних ресурсів. Об'єктом дослідження є процес управління ідентифікацією та доступом до мережових інформаційних ресурсів. Предметом дослідження є методи управління ідентифікацією та доступом до мережових інформаційних ресурсів. Методи дослідження базуються на методах захисту інформації, методах теорії побудови комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи управління ідентифікацією та доступом до мережових інформаційних ресурсів. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

управління ідентифікацією та доступом, мережеві інформаційні ресурси

Постановка проблеми. Інструменти мережевої безпеки спрямовані на запобігання несанкціонованому доступу до даних, крадіжці особистих даних та кіберзагрозам до пристроїв, технологій та процесів.

Мережева безпека запобігає несанкціонованому доступу до інформації або зловживанню мережею організації. Вона включає апаратні та програмні технології, розроблені для захисту безпеки та надійності мережі та даних.

Інструменти мережевої безпеки є важливими для захисту мережі вашої організації та запобігання кільком загрозам, які можуть пошкодити систему та мережу. Вони допомагають контролювати мережу та запобігати витокам даних.

Інструмент мережевої безпеки може аналізувати весь трафік у мережі. Моніторинг трафіку допомагає організації проактивно виявляти проблеми та загрози, перш ніж вони завдадуть їй значної шкоди. Інструменти мережевої безпеки надсилають сповіщення в режимі реального часу про будь-яку незвичайну поведінку, щоб запобігти будь-яким порушенням.

Деякі переваги інструментів мережевої безпеки:

- Інструменти мережевої безпеки мінімізують бізнес- та фінансовий вплив будь-якого порушення, оскільки вони допомагають вам дотримуватися правил та запобігати порушенням.

- Мережева безпека допомагає вашому бізнесу дотримуватися вимог і забезпечує кілька рівнів безпеки, щоб розширити масштаби вашого бізнесу та запропонувати краще робоче місце для ваших співробітників.

- Це забезпечує захист будь-якої конфіденційної інформації та даних, що передаються по мережі.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи управління ідентифікацією та доступом до мережових інформаційних ресурсів.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи управління ідентифікацією та доступом до мережевих інформаційних ресурсів.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем управління ідентифікацією та доступом до мережевих інформаційних ресурсів.

- Дослідження системи управління ідентифікацією та доступом до мережевих інформаційних ресурсів.

- Програмна реалізація системи управління ідентифікацією та доступом до мережевих інформаційних ресурсів.

Об'єктом дослідження є процес управління ідентифікацією та доступом до мережевих інформаційних ресурсів.

Предметом дослідження є методи управління ідентифікацією та доступом до мережевих інформаційних ресурсів.

Методи дослідження базуються на методах захисту інформації, методах теорії побудови комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Автентифікація – це процес перевірки особи користувача або системи. Повернімося до нашого прикладу зі спортзалом. Адміністратор у спортзалі приймає лише передплатників. Як це досягається в аналоговому світі? Вони можуть попросити вас надати вашу картку члена спортзалу (якщо припустити, що спортзал надає її кожному передплатнику). У вас повинна бути картка члена спортзалу з вашою фотографією та відповідними даними про передплату. Адміністратор може підтвердити вашу особу, перевібивши вашу картку; проблема автентифікації вирішена (якщо хтось не знайде спосіб підробити картку, але це вже інша проблема).

Автентифікація та ідентифікація є основними компонентами будь-якої інформаційної системи та мережі. Важливо розуміти різницю між автентифікацією та ідентифікацією.

Під час ідентифікації користувач (або система чи процес) заявляє про певну (унікальну) особу у відповідних налаштуваннях. Автентифікація – це підтвердження особи користувача (або системи чи процесу). Цей процес зазвичай здійснюється одним із таких способів:

- Щось тобі відомо.

- Щось у тебе є.

- Щось, що ти є.

Використовуються ще два методи, хоча й у меншій мірі:

- Деся ви знаходитесь (логічне/фізичне місцезнаходження).

- Щось, що ви робите (поведінка).

Опишемо кожен із трьох основних механізмів автентифікації.

Щось, що ти знаєш

«Щось, що ви знаєте», стосується чогось, що ви знаєте або запам'ятали. Приклади включають наступне:

- Паролі, такі як 4SNoPawKkdFiCdnmi%WAdWi-;4,mxRMQB.

- Парольні фрази, такі як «Judge Battle Advise Pain 9» та «Baggage Protection Dissatisfy Barrel 8».

- PIN-код (персональний ідентифікаційний номер), такий як 25063та6285.

Більшість мобільних телефонів автоматично блокуються протягом кількох хвилин бездіяльності. Залежно від початкової конфігурації, користувач може розблокувати їх, ввівши правильний PIN-код, пароль або графічний ключ. Хоча графічний ключ і намальований, він нічим не відрізняється від PIN-коду, тобто чогось, що запам'ятовується.

Розглянемо випадок, коли ви входите в TryHackMe. Ви повинні ідентифікувати себе за допомогою імені користувача або електронної пошти та автентифікувати свою особу за допомогою пароля. (Якщо ви входите в TryHackMe через Google, ви надасте свої облікові

дані для входу Google, і Google підтвердить вашу особу TryHackMe.) Ім'я користувача та електронна пошта є унікальними для вас; отже, ідентифікація може бути здійснена без жодної двозначності. Вважається, що пароль відомий лише вам, що доводить, що ви є власником облікового запису.

Щось у тебе є

«Щось, що у вас є» стосується об'єкта, зазвичай фізичного, який у вас є. Це може бути як телефон, так і ключ безпеки.

Наприклад, коли ви хочете зареєструватися в деяких додатках для обміну миттєвими повідомленнями, вас просять надати номер телефону, зазвичай номер мобільного телефону. Цей номер телефону є вашою ідентифікатором у цьому додатку. Як ви можете довести, що це справді ваш номер телефону? Один із способів – надіслати вам код через SMS або зателефонувати вам на цей номер і повідомити код. Прочитання SMS протягом кількох хвилин або отримання дзвінка на цей номер доведе, що у вас є цей номер телефону. У випадку номера мобільного телефону, цього буде достатньо, щоб підтвердити, що у вас є SIM-картка (або eSIM).

Апаратний ключ безпеки достатньо малий, щоб його можна було носити на зв'язці ключів або в гаманці. Ви можете використовувати ключ безпеки для автентифікації, підключивши його до порту USB або USB C або піднісши його до зчитувача NFC (Near-Field Communication). Прикладами апаратних ключів безпеки є, наприклад, Yubico, Titan Security Key, Nitrokey та Thetis.

Щось, що ти є

«Щось, чим ви є», стосується біометричних зчитувачів. Прикладами є зчитувачі відбитків пальців, сканери розпізнавання обличчя, сканери сітківки ока та розпізнавання голосу.

Ви, найімовірніше, стикалися з автентифікацією за допомогою зчитувача відбитків пальців під час спроби розблокувати телефон. Багато сучасних мобільних телефонів дозволяють користувачеві автентифікуватися за допомогою відбитка пальця, зберігаючи пароль/PIN-код/графічний ключ як резервний варіант на випадок, якщо автентифікація за відбитком пальця не вдасться.

Розпізнавання обличчя також стає популярним у сучасних смартфонах. З роками біометричні зчитувачі та сканери стають не тільки надійнішими, але й доступнішими. Ця технологія вигідна як компаніям, які вимагають високого рівня безпеки, так і споживачам.

Багатофакторна автентифікація (MFA)

Багатофакторна автентифікація (MFA) означає використання двох або більше з перерахованих вище механізмів (щось, що ви знаєте/маєте/є). Мета полягає в тому, щоб забезпечити додатковий захист у разі порушення одного з механізмів автентифікації.

Якщо ви хочете скористатися банкоматом банку, вставте свою кредитну/дебетову картку та введіть свій PIN-код. Ця процедура є одним із найперших прикладів двофакторної автентифікації (2FA). Очевидна корисність полягає в тому, що зловмиснику недостатньо просто отримати вашу картку, оскільки йому також потрібно знати ваш PIN-код.

Багато домашніх сейфів, доступних сьогодні, використовують 2FA, не обов'язково рекламуючи це. Вони вимагають від власника вставити ключ і ввести правильний PIN-код, щоб сейф відкрився. Вам потрібно знати PIN-код і мати ключ, щоб його відкрити. Отже, якщо комусь іншому вдасться отримати ключ від сейфа, він все одно не зможе відкрити сейф, не знаючи PIN-коду.

У другому випадку двофакторна автентифікація (2FA) вимагає двох механізмів автентифікації та підпадає під більш загальну багатофакторну автентифікацію (MFA), яка вимагає двох або більше факторів автентифікації. Ця вимога може значно покращити безпеку та захистити від різних атак, таких як ті, що використовують слабкі паролі.

Після автентифікації користувачеві має бути надано належний рівень доступу. Авторизація визначає, до чого має бути дозволено автентифікованому користувачеві отримувати доступ та що робити. Повертаючись до нашого прикладу зі спортзалом, ми

очікуємо, що платний учасник спортзалу матиме право доступу до будь-якого тренувального обладнання протягом встановленого робочого часу. Абонент не може позичати та брати бігову доріжку додому протягом місяця. Спортзал – це не бібліотека! Механізми контролю доступу забезпечать належне виконання авторизації. Якщо в спортзалі є належний механізм контролю доступу, хтось помітить, як ви намагаєтеся перенести та винести бігову доріжку.

Розглянемо ще один нетехнічний приклад: Віка забронювала номер у готелі на один тиждень. Завдяки цьому бронюванню Віка повинна мати право доступу до свого готельного номера, серед інших громадських приміщень, протягом усього перебування. Хоча їй дозволено доступ до призначеного їй номера, їй не дозволено, наприклад, доступ до інших номерів. Як це можна забезпечити? Знову ж таки, авторизація забезпечується механізмами контролю доступу.

У прикладі з готелем Віці надають ключ, який надає їй доступ до призначеного їй номера. Відповідно, контроль доступу здійснюється за допомогою замків та ключів. Більш вишуканий готель може використовувати смарт-картки та електронні зчитувачі карток для відмикання дверей номера. У будь-якому випадку існує механізм, який би забезпечив авторизацію.

Розглянемо технічний приклад. Як частина команди з продажу, Ігор повинен мати доступ до всіх файлів, пов'язаних із продажами, які необхідні для ефективного та результативного виконання його роботи. Наприклад, команді з продажу не потрібно мати доступ до документів, що стосуються, наприклад, управління персоналом та бухгалтерського обліку. У цьому випадку контроль доступу можна забезпечити, встановивши відповідні дозволи доступу до файлів та бази знань компанії.

Коротко кажучи, авторизація визначає, до чого користувач повинен мати доступ, тоді як контроль доступу забезпечує дотримання встановленої політики. Наприклад, після входу до свого облікового запису електронної пошти ви повинні мати можливість читати свої електронні листи та надсилати нові. Однак за замовчуванням ви не повинні мати доступу до поштової скриньки жодного зі своїх колег. Поштовий сервер має бути розроблений таким чином, щоб дозволяти користувачеві доступ до своєї поштової скриньки та забороняти йому доступ до поштових скриньок інших користувачів.

Авторизація проти контролю доступу

– Авторизація – етап прийняття рішення – визначає, який доступ слід надавати кому, на основі ролей або політик.

Вирішення, що секретар може надсилати електронні листи від імені менеджера.

– Контроль доступу – механізм забезпечення дотримання правил – реалізує правила, визначені на етапі авторизації.

Запобігання зміні документа користувачами шляхом забезпечення доступу лише для читання.

Підзвітність та ведення журналу

Підзвітність гарантує, що користувачі несуть відповідальність за дії, які вони виконують у системі. Іншими словами, після автентифікації своєї особи та отримання дозволу на доступ до системи вони можуть нести відповідальність за свої дії. Підзвітність можлива, якщо у нас є можливості аудиту, які зазвичай вимагають належного функціонування журналювання.

Почнемо з нетехнічного прикладу: спортзал. У вас є абонемент у спортзал, і ви відвідуєте його тричі на тиждень. Тепер, коли ви стали його постійним клієнтом, адміністратор впізнає вас і не просить пред'являти вашу картку члена. Це ніби ви завжди «залогінені» в спортзалі! Ви помічаєте, що всі, хто має «доступ» до спортзалу, дотримуються певних правил. Наприклад, ніхто не розбиває настінне дзеркало, якщо незадоволений швидкістю свого прогресу. Якщо вони це зроблять, їхнє членство буде анульовано, і вони сплатять усі збитки. Іншими словами, кожен несе *відповідальність* за свої дії. Ця модель забезпечує зручність для всіх для безпечних тренувань.

Розглянемо більш технічний приклад, наприклад, касира банку. Такий працівник може переглядати та проводити різні операції на рахунок клієнта. Як ми можемо гарантувати, що недобросовісний працівник не зловживатиме такими повноваженнями? Нам потрібно безпечно реєструвати всі транзакції та відповідні деталі. Ми повинні мати можливість перевіряти всі проведені транзакції та перевіряти, хто що зробив. Без такої можливості ми не можемо ні покладатися на таку систему, ні довіряти їй.

Ведення журналу

Критичним аспектом підзвітності є ведення журналу. Вedenня журналу – це процес запису подій, що відбуваються в системі. Цей процес включає дії користувачів, системні події та помилки. Реєструючи дії користувачів, організація може вести облік того, хто і коли отримував доступ до якої інформації. Цей запис життєво важливий для дотримання нормативних вимог, реагування на інциденти та судово-медичних розслідувань.

Завдяки комплексній системі реєстрації, організація може відстежувати дії будь-якого користувача, виявляти будь-які аномалії або несанкціонований доступ і вживати відповідних заходів. Наприклад, якщо неавторизований користувач намагається отримати доступ до конфіденційних даних, система реєстрації може генерувати сповіщення для сповіщення персоналу служби безпеки.

Ведення журналів також може допомогти організаціям виявляти інциденти безпеки та реагувати на них. Аналізуючи дані журналів, команди безпеки можуть виявляти закономірності підозрілої активності, такі як повторні невдалі спроби входу або незвичайні моделі доступу. Цю інформацію потім можна використовувати для розслідування потенційних загроз безпеці та реагування на них.

Оскільки підзвітність є ключовим компонентом будь-якої безпечної інфраструктури, слід належним чином подбати про те, щоб ведення журналу відбувалося належним чином та безпечно. Крім того, залежно від вимог безпеки, журнали повинні бути захищеними від несанкціонованого доступу. Причина полягає в тому, що ви не хочете, щоб зловмисник видаляв або змінював журнали та приховував свої дії в мережі. Ось чому гарною практикою є налаштування окремого сервера журналювання з одним завданням: безпечне отримання та зберігання журналів. Звідси й переадресація журналів.

Пересилання журналів – це процес надсилання даних журналів з однієї системи до іншої. Цей процес часто об'єднує дані журналів з кількох джерел у централізоване місце для кращого аналізу та керування. Пересилання журналів також може використовуватися для надсилання даних журналів до хмарного сервісу для зберігання та аналізу.

Пересилання журналів має кілька переваг. Централізуючи дані журналів, організації можуть легше аналізувати та співвідносити події журналів з різних систем для виявлення потенційних загроз безпеці. Це підводить нас до управління інформацією та подіями безпеки (SIEM).

Ведення журналу та SIEM

Управління інформацією та подіями безпеки (SIEM) – це технологія, яка об'єднує дані журналів з кількох джерел та аналізує їх на наявність ознак загроз безпеці. Рішення SIEM можуть допомогти організаціям виявляти аномалії, потенційні інциденти безпеки та надавати сповіщення командам безпеки.

Інтегруючи логуювання та SIEM, організації можуть краще розуміти активність своїх систем та мереж, а також контролювати потенційні загрози. Ця інтеграція дозволяє організаціям ефективніше виявляти загрози безпеці та реагувати на них.

Крім того, інтеграція ведення журналу та SIEM забезпечує додаткові переваги, такі як звітність про відповідність вимогам та судово-медичні розслідування. Звітність про відповідність вимогам є важливою частиною системи безпеки будь-якої організації, а ведення журналу допомагає організаціям виконувати вимоги до звітності, збираючи дані, необхідні для аудитів. Судово-медичні розслідування мають вирішальне значення для визначення джерела та причини інциденту безпеки. Рішення для ведення журналу та SIEM

дозволяють організаціям проводити судово-медичні розслідування, надаючи детальну історію активності системи та мережі.

Управління ідентифікацією

Керування ідентифікацією (IdM) включає всі необхідні політики та технології для ідентифікації, автентифікації та авторизації. IdM має на меті забезпечити, щоб уповноважені особи мали доступ до активів та ресурсів, необхідних для їхньої роботи, тоді як неавторизованим особам доступ заборонено. IdM вимагає, щоб кожному користувачеві або пристрою було призначено цифрову ідентифікацію.

IdM допомагає організаціям захищати конфіденційні дані та підтримувати дотримання нормативних вимог. Це також дозволяє організаціям оптимізувати процеси доступу користувачів, зменшувати витрати, пов'язані з управлінням ідентифікацією, та покращувати взаємодію з користувачами. Впроваджуючи ефективну стратегію IdM, організації можуть гарантувати, що їхні користувачі автентифіковані та авторизовані для безпечного доступу до необхідних їм ресурсів.

Деякі джерела використовують IdM та керування ідентифікацією та доступом (IAM) як взаємозамінні. Інші джерела вважають, що IdM більше зосереджений на питаннях безпеки, пов'язаних з ідентифікацією користувача, таких як автентифікація та дозволи. Вони стверджують, що IdM займається управлінням атрибутами та дозволами користувачів, пристроїв та груп, тоді як IAM більше займається оцінкою атрибутів та дозволів і наданням або заборонною доступу відповідно до політики компанії. У цьому завданні ми представляємо їх як різні, хоча межа між ними, як правило, розпливчаста.

Управління ідентифікацією (IdM)

Управління цифровими ідентифікаторами (IdM) – це важливий компонент кібербезпеки, що стосується процесу управління та контролю цифрових ідентифікацій. Він включає управління ідентифікаторами користувачів, їхню автентифікацію, авторизацію та контроль доступу. Головна мета IdM – забезпечити доступ до певних ресурсів та інформації лише уповноваженим особам. Системи IdM використовуються для керування ідентифікаторами користувачів у мережі організації.

Системи IdM використовують централізовану базу даних для зберігання ідентифікаційних даних користувачів та прав доступу. Вони також надають функціональні можливості для керування та моніторингу доступу користувачів до ресурсів. Системи IdM зазвичай включають такі функції, як надання користувачів, автентифікація та авторизація. Надання користувачів стосується процесу створення та керування обліковими записами користувачів, тоді як автентифікація та авторизація стосуються перевірки особи користувача та надання доступу до певних ресурсів.

Системи IdM є критично важливими в організаціях, де існує кілька систем і програм, що потребують контролю доступу. Вони допомагають спростити управління ідентифікацією користувачів, зменшуючи ризик несанкціонованого доступу до ресурсів. Крім того, системи IdM забезпечують єдину точку відліку для управління ідентифікацією користувачів, що спрощує для організацій управління правами доступу користувачів.

Керування ідентифікацією та доступом (IAM)

IAM – це більш комплексне поняття, ніж IdM. Воно охоплює всі процеси та технології для управління цифровими ідентифікаторами та правами доступу, а також їх захисту. Системи IAM включають різноманітні функції, такі як надання користувачам доступу, контроль доступу, управління ідентифікаторами та управління відповідністю. Системи IAM гарантують, що лише авторизовані користувачі мають доступ до певних ресурсів і даних, а їхній доступ моніториться та контролюється.

Системи IAM пропонують комплексне рішення для керування та захисту доступу до ресурсів в організації. Вони інтегруються з кількома системами та програмами, забезпечуючи централізоване уявлення про ідентифікаційні дані користувачів та права доступу. Системи IAM використовують різні технології для керування доступом, включаючи контроль доступу на основі ролей, багатофакторну автентифікацію та єдиний вхід.

Системи IAM допомагають організаціям дотримуватися нормативних вимог, таких як HIPAA, GDPR та PCI DSS. Вони надають функції для керування життєвим циклом ідентифікації користувачів, включаючи адаптацію, видалення та скасування доступу. Крім того, системи IAM дозволяють організаціям відстежувати та перевіряти активність користувачів, що допомагає запобігти порушенням безпеки та забезпечити дотримання галузевих норм.

IdM та IAM є важливими компонентами кібербезпеки. Вони гарантують, що лише уповноважені особи мають доступ до певних ресурсів та інформації. Системи IdM керують ідентифікаторами користувачів, тоді як системи IAM охоплюють ширші функції для управління та захисту цифрових ідентифікаторів та прав доступу.

Атаки проти автентифікації

Це завдання охоплюватиме приклади атак на наївний протокол автентифікації. Мета полягає в тому, щоб дати уявлення про важливість використання існуючих та перевірених протоколів замість створення протоколу та його використання без ретельного тестування одноранговими користувачами.

Автентифікація в аналоговому світі

Припустимо, ви належите до кінного клубу. Клуб резервує місцевий ресторан для щотижневих зустрічей. Ви можете поспілкуватися про свої пригоди, насолоджуючись улюбленою стравою. Охоронець біля входу знає не всіх членів клубу. Тож ви розробляєте схему автентифікації, щоб охоронець міг вирішити, чи відчиняти двері.

Одна з найпростіших ідей, яка спадає на думку, – це використання загальної секретної фрази. Тож кожен, хто хоче увійти, повинен сказати секретну пароліну фразу; нікому не буде дозволено вхід, якщо він не скаже «сім коней» на запитання «Скільки?». Цей механізм автентифікації працює чудово, доки зловмисник, що стоїть поруч, не підслухає та не дізнається вашу пароліну фразу. Тепер він отримає доступ до вашої приватної зустрічі, ніби він один із вас. Було б корисно, якби у вас було щось складніше.

Ви можете спланувати десять запитань з десятьма різними секретними відповідями замість одного запитання та однієї відповіді; однак зловмисник, який перебуває досить близько, зрештою вивчить їх усі. Використання безпечного механізму автентифікації без застосування криптографії може бути практично неможливим. На щастя, у сценарії з охоронцем біля дверей легко помітити будь-яких підозрілих осіб, які бездіяльно гуляють; інакше вся ваша група буде скомпрометована.

Автентифікація в цифровому світі

Ситуацію в мережі ще складніше захистити. Якщо користувач надсилає своє ім'я користувача та пароль у відкритому тексті, будь-хто, хто перехоплює трафік у мережі, може дізнатися це ім'я користувача та пароль. Як ми можемо запобігти отриманню облікових даних для входу?

Сервер і користувач можуть домовитися про фіксований секретний ключ. Замість того, щоб надсилати пароль у відкритому вигляді, користувач шифрує його за допомогою вибраного секретного ключа. Щоразу, коли користувачі хочуть увійти, вони надсилають своє ім'я користувача та пароль у зашифрованому вигляді за допомогою призначеного їм секретного ключа. Тепер зловмисник ніколи не повинен мати змоги дізнатися пароль, чи не так? На жаль, хоча вони не зможуть дізнатися пароль, вони все одно зможуть пройти автентифікацію.

Хоча зловмисник не знає пароля, він все одно може автентифікуватися, відтворивши ту саму відповідь. Ця атака вважається **атакою повторного відтворення**. Чи можемо ми щось зробити, щоб виправити це?

Зробіть відповідь на виклик унікальною

Зашифрований пароль, який завжди має одне й те саме значення, легко обійти. Нам потрібен певний механізм, який гарантуватиме, що відповідь не буде використана повторно. Один із підходів – використовувати поточний час і дату як частину відповіді. Іншими словами, користувач надсилатиме зашифрований поточний час (і дату) разом із паролем.

Хоча це вимагає синхронізації годинників обох сторін, це гарантує, що відповідь буде дійсною лише протягом короткого часу, зазвичай у мілісекундах.

Це завдання має на меті пролити світло на деякі проблеми, пов'язані з автентифікацією та протоколами автентифікації. Багато інших вразливостей можуть потрапити в протоколи автентифікації; однак це виходить за рамки цієї кімнати.

Атака повторного відтворення відбувається, коли зломисник перехоплює дійсні дані автентифікації (наприклад, зашифрований пароль або токен сеансу) та повторно надсилає (або «відтворює») їх, щоб видати себе за оригінального користувача, навіть не знаючи пароля та не розшифровуючи повідомлення.

- Користувач шифрує свій пароль за допомогою спільного секретного ключа та надсилає його на сервер.

- Зломисник перехоплює це зашифроване повідомлення під час його передачі мережею.

- Пізніше зломисник відтворює точне повідомлення на сервері.

- Сервер приймає його як дійсний, оскільки він відповідає очікуванням, навіть якщо реального входу не відбулося.

Система не має можливості визначити, чи:

- Цей запит є свіжим (від легітимного користувача), або

- Це повторне повідомлення з попереднього сеансу.

Чому це трапляється:

- Статична відповідь: Зашифрований пароль виглядає однаково щоразу.

- Відсутність актуальності: Сервер не перевіряє, коли було створено повідомлення.

- Без одноразового номера/позначки часу: Немає унікального значення для кожного сеансу для розрізнення запитів.

Як запобігти атакам повторного відтворення

Щоб уникнути атак повторного відтворення, протоколи автентифікації повинні гарантувати, що кожна спроба автентифікації є унікальною.

- Мітки часу – Включити поточний час у зашифроване повідомлення. Сервер відхиляє старі позначки часу.

- Nonces Використовуйте одноразове випадкове число (nonce) для кожного сеансу або завдання.

- Токени сесії – генерувати унікальні токени сесії після автентифікації.

- Протоколи виклику-відповіді – сервер надсилає виклик; клієнт підписує його своїм секретним ключем. Запобігає повторному використанню.

Сучасні протоколи, що пом'якшують це:

- Kerberos: використовує позначки часу та симетричне шифрування для запобігання атакам повторного відтворення.

- OAuth 2.0: видає короточасні токени та використовує токени оновлення для тривалих сеансів.

- TLS/SSL: використовує унікальні ключі сеансу та рукописання з одноразовими числами для забезпечення актуальності повідомлень.

Моделі контролю доступу

Система контролює доступ до різних ресурсів на основі обраної моделі. Деякі з поширених моделей контролю доступу:

- Дискреційний контроль доступу (DAC).

- Контроль доступу на основі ролей (RBAC).

- Обов'язковий контроль доступу (MAC).

Дискреційний контроль доступу

Багато хто вже використовував дискреційний контроль доступу (DAC) під час обміну файлами або папками з друзями та колегами. Під час використання DAC власник ресурсу явно додасть користувачів із відповідними дозволами.

Розглянемо наступний приклад. Ви зберігаєте свої фотографії на одній з онлайн-платформ для зберігання. Щоб поділитися всіма зображеннями, пов'язаними з вашим випускним, з родиною, ви додаєте їхні облікові записи окремо та надаєте їм доступ до відповідного альбому. Зрештою, дозволи альбому відображатимуть кілька облікових записів із правами перегляду.

Весь процес простий і повністю контролюється власником даних. Він дуже добре працює для обміну даними з членами родини або кількома користувачами компанії. Однак це може стати складним, коли ви намагаєтеся масштабувати обмін з багатьма користувачами, особливо якщо роль користувача змінюється з часом. Ця ситуація підводить нас до обміну на основі ролей користувачів.

Контроль доступу на основі ролей

Контроль доступу на основі ролей (RBAC) використовує дуже інтуїтивно зрозумілий підхід. Кожен користувач має одну або кілька ролей або функціональних посад; крім того, вони мають право доступу до різних ресурсів на основі своїх ролей.

Бухгалтеру потрібен доступ до бухгалтерських книг компанії, але не потрібен доступ до дослідницьких та розробницьких лабораторій чи документів. Відповідно, користувачі розподіляються на різні групи залежно від їхніх ролей. Авторизація та доступ надаються залежно від групи, до якої належить користувач.

Класифікація користувачів на основі їхніх ролей має багато переваг. Наприклад, якщо користувачеві призначено нову роль, все, що потрібно, це додати його до відповідної нової групи. Більше того, якщо користувачі відмовилися від певної ролі, нам потрібно лише видалити їх зі старої групи. Такий підхід робить обслуговування більш керованим та ефективним.

Обов'язковий контроль доступу

Операційна система, що використовує обов'язковий контроль доступу (MAC), надасть пріоритет безпеці та значно обмежить можливості користувачів. Такі системи використовуються для певних цілей або для обробки високосекретних даних. Отже, користувачам не потрібно виконувати завдання, що перевищують суворо необхідні. Іншими словами, користувачі не зможуть встановлювати нове програмне забезпечення або змінювати дозволи на доступ до файлів.

AppArmor надає можливість використовувати MAC на дистрибутиві Linux. Він вже постачається з різними дистрибутивами Linux, такими як Debian та Ubuntu.

Проект **SELinux** забезпечує гнучку MAC-адресу для систем Linux. Вона є стандартною для кількох дистрибутивів Linux, таких як Red Hat та Fedora.

Єдиний вхід

Користувачам потрібен доступ до різних джерел для виконання своїх щоденних робочих завдань. Наприклад, їм потрібен доступ до електронної пошти, спільних файлів, принтерів тощо. Доступ до цих ресурсів вимагає від користувача облікових даних для успішної автентифікації. Кількість різних імен користувачів та паролів робить це досить складним, особливо якщо користувачі не мають підстав використовувати один і той самий пароль у кількох системах.

Єдиний вхід (SSO) вирішує цю проблему. Замість того, щоб користувачеві доводилося запам'ятовувати кілька імен користувачів та паролів, йому потрібно запам'ятати лише один набір облікових даних для входу. Він може автентифікувати себе в одній системі, що надає йому доступ до інших систем, необхідних для його роботи.

Традиційно користувач повинен створити кілька паролів, таких як пароль для входу на комп'ютер, ще один пароль для перевірки електронної пошти та третій пароль для доступу до спільного файлового ресурсу. Запам'ятовування такої кількості паролів може бути складним завданням, особливо тому, що, в ідеалі, пароль не слід використовувати повторно. Кращим підходом було б вимагати від користувача одноразового входу в систему та надавати йому доступ до всіх необхідних служб; саме це робить SSO.

SSO дозволяє організаціям автентифікувати користувачів один раз, перш ніж надати їм доступ до ресурсів, необхідних для їхньої роботи. Це може дати нам багато переваг. Ми розглянемо деякі з них.

- Один надійний пароль: очікувати, що користувач запам'ятає один надійний пароль, прийнятніше, ніж просити його запам'ятати десять різних надійних паролів.
- Простіша багатофакторна автентифікація (MFA): додавання MFA до кожної окремої служби є надзвичайно складним завданням для виконання та підтримки. За допомогою єдиного входу (SSO) MFA потрібно вмикати та налаштовувати один раз.
- Простіша підтримка: запити на підтримку, такі як скидання пароля, стали простішими, оскільки тепер вони обмежені одним обліковим записом.
- Ефективність: Користувачеві не потрібно входити в систему щоразу, коли йому потрібен доступ до нової послуги.

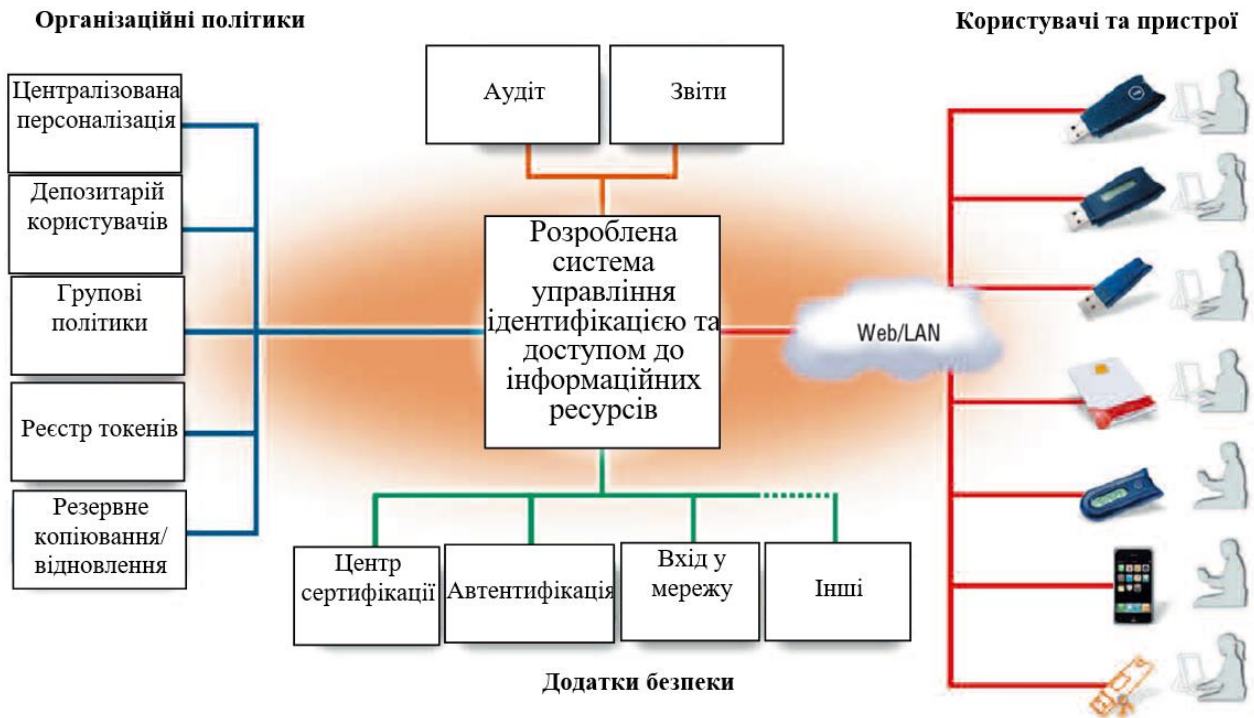


Рисунок 1 – Структурна схема системи

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів управління ідентифікацією та доступом до мережевих інформаційних ресурсів. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем управління ідентифікацією та доступом до мережевих інформаційних ресурсів.
- Досліджена система управління ідентифікацією та доступом до мережевих інформаційних ресурсів.
- На основі отриманих результатів досліджень створена програмна реалізація системи управління ідентифікацією та доступом до мережевих інформаційних ресурсів.

Розроблені алгоритми дозволяють успішно вирішувати завдання управління ідентифікацією та доступом до мережевих інформаційних ресурсів. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Усік, П.С., Смірнова, Т.В., Буравченко, К.О., Смірнов, О.А., Улічев, О.С., Смірнов, С.А. «Дослідження

- технологій забезпечення кібербезпеки банківських систем з використанням штучного інтелекту». Кібербезпека: освіта, наука, техніка. 2025. Том 1 № 29. С.704–716, 2025
2. Kuznetsov, O., Frontoni, E., Kuznetsova, K., Arnesano, M., Smirnov, O. «A secure biometric authentication architecture for blockchain-driven cyber-physical systems». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 193–224.
 3. Kuznetsov, O., Atzeni, G., Arnesano, M., Randieri, C., Smirnov, O. «Secure IoT-based smart wheelchair system: From implementation to security enhancement strategy». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 225–257.
 4. Kuznetsov, O., Smirnov, O., Kuznetsova, T., Shaikhanova, A., Svatowsky, I. «Privacy-utility trade-offs in IoT networks: A comparative analysis of differential privacy mechanisms for sensor data aggregation». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 589–622.
 5. Lakhno, V., Malyukov, V., Smirnov, O., Bebesko, B., Chubaievskiy, V., Zhumadilova, M., Malyukova, I., Smirnov, S. «Multifactorial Model for Targeted Attacks Counteracting Within the Framework of a Multi-Step Quality Game with Fuzzy Information». *8th International Symposium on Intelligent Informatics, ISI 2023*, 2025. vol 389. pp 377-389. Springer, Singapore.
 6. Kuznetsov O., Frontoni E., Kuznetsova Y., Smirnov O., Moskovchenko I. «Trust-Based Security Architecture for Edge Computing: A Simulation Study of Dynamic Trust Evolution and Attack Detection». *CEUR Workshop Proceedings*, 2024, 3909, pp. 227–241.
 7. Kuznetsov, O., Frontoni, E., Kryvinska, N., Chevardin, V., Smirnov, O. «Wireless Network Encryption Stream Ciphers, Computational Modeling, and Security Analysis». *Computational Modeling and Simulation of Advanced Wireless Communication Systems*, 2024, pp. 379–402.
 8. Kuznetsov, O., Frontoni, E., Kryvinska, N., Smirnov, O., Imoize, G.L. «Computational Modeling of Enhanced Spread Spectrum Codes for Asynchronous Wireless Communication». *Computational Modeling and Simulation of Advanced Wireless Communication Systems*, 2024, pp. 403–447.
 9. Ткаченко, О., Ільченко, А., Улічев, О., Мелешко, Є., Смірнов, О. «Правові засади поширення інформаційних впливів в соціальних мережах». Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2024. № 2(26), С. 170–188.
 10. Смірнова Т.В., Коноплицька-Слободенюк О.К., Буравченко К.О., Смірнов С.А., Кравчук О.В., Козірова Н.Л., Смірнов О.А. «Дослідження технологій забезпечення кібербезпеки хмарних сервісів IaaS, PaaS та SaaS». *Кібербезпека: освіта, наука, техніка*. 2024. №4(24), С. 6-27.
 11. Вінтенко, Б., Миронець, І., Смірнов, О., Кравчук, О., Козірова, Н., Савеленко, Г., Коваленко, А. «Дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». *Кібербезпека: освіта, наука, техніка*. 2024. №3(23), С. 111-131.
 12. Батрак О., Смірнова Т., Гнатюк В., Одарченко Р., Смірнов О. «Дослідження показників ефективності функціонування та перспектив розвитку систем IP-телефонії». *Підводні технології*, 2024, № 13, с. 28-35.
 13. Kuznetsov, O., Kryvinska, N., Ilchenko, O., Smirnova, T., Ulianovska, Y. «Comparative Analysis of Cryptocurrency Trading Platforms Using the Analytic Hierarchy Process». *CEUR Workshop Proceedings*, 2023, 3628, pp. 106-115.
 14. Akhalaia, G., Iavich, M., Iashvili, G., Prysiashnyy, D., Smirnova, T. «Secure Encrypted Connection on Georgian Website». *CEUR Workshop Proceedings*, 2023, 3550, pp. 313-320.
 15. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». *Advanced Information Systems*, 2023, 7(2), pp. 49-56
 16. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchov, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». *CEUR Workshop Proceedings*, Volume 3530, 2023, pp. 256-265.
 17. Kuznetsov, O., Kandiy, S., Frontoni, E., Smirnov, O. «Trade-offs in Post-Quantum Cryptography: A Comparative Assessment of BIKE, HQC, and Classic McEliece». *CEUR Workshop Proceedings*, Volume 3504, 2023, pp. 1-11.
 18. Smirnov, O., Lakhno, V., Akhmetov, B., Chubaievskiy, V., Khorolska, K., Bebesko, B. «Selection of a Rational Composition of Information Protection Means Using a Genetic Algorithm». In: Rajakumar, G., Du, K.L., Vuppapapati, C., Beligiannis, G.N. (eds) *Intelligent Communication Technologies and Virtual Mobile Networks. Lecture Notes on Data Engineering and Communications Technologies*, vol 131. 2023. Springer, Singapore. pp. 21-34.
 19. Смірнова Т.В., Гнатюк С.О., Бердибаєв Р.Ш., Сидоренко В.М., Жигаревич О.К., «Система корелювання подій та управління інцидентами кібербезпеки на об'єктах критичної інфраструктури». *Кібербезпека: освіта, наука, техніка*, №3(19), 2023, С. 176-196.
 20. Смірнов О.А. Козлов Я.О., Смірнова Т.В. «Дослідження застосування SIEM-систем для забезпечення кібербезпеки та захисту інформації». II Міжнародна науково-практична Інтернет-конференція «Інновації та перспективні шляхи розвитку інформаційних технологій (ІПШРІТ-2023)» м.Черкаси 6 грудня 2023 року – Черкаси: ЧДТУ.– 2023. – С.251-252.
 21. Козлов Я.О., Смірнова Т.В., Смірнов О.А. «Дослідження SIEM-систем для забезпечення кібербезпеки». VII міжнародна науково-практична конференція «Інформаційна безпека та комп'ютерні технології» до 30-ти річчя кафедри кібербезпеки та програмного забезпечення, м.Кропивницький. 1 листопада 2023 р. –

- Кропивницький: ЦНТУ. – 2023. – С. 26.
22. Козлов Я.О., Козірова Н.Л., Смірнов О.А. «Дослідження структури та принципу роботи SIEM-системи». VII міжнародна науково-практична конференція “Інформаційна безпека та комп’ютерні технології” до 30-ти річчя кафедри кібербезпеки та програмного забезпечення, м. Кропивницький. 1 листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 59.
23. Вінтенко Б.Ю., Смірнов О.А., Коваленко О.В., Смірнов С.А., Коваленко А.С. «Дослідження нормативних документів та галузевих стандартів розробки програмного забезпечення комп’ютерних систем управління АЕС, важливих для безпеки». Системи управління, навігації та зв’язку, 2023, вип. 2(72), С. 170-178.
24. Smirnov, O., Neskorodieva, T., Fedorov, E., Rudakov, K., Neskorodieva, A. «Method Detection Audit Data Anomalies on Basis Restricted Cauchy Machine» CEUR Workshop Proceedings, Volume 3187, 2022,
25. Smirnov O.A., Al-Oraiqat A.M., Ulichev O.S., Meleshko Ye.V., Al-Rawashdeh H.S., Polishchuk L.I. «Modeling strategies for information influence dissemination in social networks». Journal of Ambient Intelligence and Humanized Computing Volume 13, Issue 5. Springer, Cham. 2022, pp. 2463-2477.
26. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». Проблеми інформатизації та управління, № 2(70). 2022. С. 28-37.
27. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції ґешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв’язку, 2022, № 3(69). С. 93-98.
28. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції ґешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Вісник Хмельницького національного університету. Серія: «Технічні науки», № 2 (307). С. 46-52. 2022.
29. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції ґешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв’язку, 2022, № 1(67). С. 84-89.
30. Smirnov O., Kuznetsov A., Zhora V., Onikiychuk A., Pieshkova O. «Hiding Messages in Audio Files Using Direct Spread Spectrum». 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2021, Cracow, Poland, 22-25 September 2021. P. 414-418
31. Smirnov O., Kuznetsov A., Lokotkova I., Kuznetsova T., Florov S., Lebid O. «Using Orthogonal Signals to Hide Information in Images». 4 IEEE International Conference on Advanced Information and Communication Technologies (AICT) - 2021, Lviv, Ukraine, September 21-25, 2021. P. 255-260.
32. Smirnov O., Kuznetsov A., Girzheva O., Kiiian A., Nakisko O., Kuznetsova T. «Advanced Code-Based Electronic Digital Signature Scheme». 2020 IEEE International Conference on Problems of Infocommunications Science and Technology, PIC S and T 2020, Kharkiv, 6 October 2020-9 October 2020, P. 358-362.

УДК 004

Б.Подольян, магістр гр. КІ-24М,*Центральноукраїнський національний технічний університет*

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ПРОЕКТУВАННЯ ТА ПОБУДОВИ ТОПОЛОГІЇ МЕРЕЖ У ЦЕНТРАХ ОБРОБКИ ДАНИХ

У статті розроблено програмне забезпечення, яке призначено для системи проектування та побудови топології мереж у центрах обробки даних. Метою розробки є дослідження та принципи побудови системи проектування та побудови топології мереж у центрах обробки даних. Об'єктом дослідження є процес проектування та побудови топології мереж у центрах обробки даних. Предметом дослідження є методи проектування та побудови топології мереж у центрах обробки даних. Методи дослідження базуються на методах побудови комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи проектування та побудови топології мереж у центрах обробки даних. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

проектування та побудова топології мереж, центр обробки даних

Постановка проблеми. Надійна топологія мережі центру обробки даних є важливою для забезпечення ефективної, масштабованої та безпечної роботи мережі в сучасному цифровому середовищі.

Ви інвестували у високоякісні мережеві комутатори та маршрутизатори. Ви оптимізували свої програми для обробки запитів з мінімальною затримкою. І все ж продуктивність мережі вашого центру обробки даних все ще низька.

Виною може бути неоптимальна топологія мережі центру обробки даних. Оскільки топології мережі відіграють ключову роль у визначенні ефективності потоку мережевого трафіку в центрі обробки даних, погані топології можуть знижувати продуктивність, навіть якщо ваші програми та інфраструктура в іншому розраховані на швидкість.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи проектування та побудови топології мереж у центрах обробки даних.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи проектування та побудови топології мереж у центрах обробки даних.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем проектування та побудови топології мереж у центрах обробки даних.
- Дослідження системи проектування та побудови топології мереж у центрах обробки даних.
- Програмна реалізація системи проектування та побудови топології мереж у центрах обробки даних.

Об'єктом дослідження є процес проектування та побудови топології мереж у центрах обробки даних.

Предметом дослідження є методи проектування та побудови топології мереж у центрах обробки даних.

Методи дослідження базуються на методах побудови комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Існує кілька способів проектування топології мережі центру обробки даних. Ось найпоширеніші:

1. Трирівнева топологія

Традиційно більшість центрів обробки даних використовували так звану трирівневу мережеву топологію. Згідно з цією схемою, мережеві ресурси організовані на три рівні:

- Рівень доступу: забезпечує пряме підключення до пристроїв кінцевих користувачів, що дозволяє здійснювати зв'язок з мережею.

- Рівень розподілу: діє як посередник, агрегуючи трафік від комутаторів доступу та забезпечуючи дотримання політик для керування маршрутизацією та безпекою.

- Базовий рівень: забезпечує високошвидкісне та надійне з'єднання між рівнями розподілу та зовнішніми мережами, обробляючи трафік магістральної мережі.

Трирівнева топологія відносно проста в реалізації. Її головним недоліком є те, що вона не дуже гнучка та нелегка в масштабуванні, оскільки відносно невелика кількість комутаторів та маршрутизаторів повинна обробляти великий обсяг мережевого трафіку. Отже, ці пристрої зазвичай є дорогими моделями високого класу, а це означає, що якщо ви хочете збільшити їхню ємність, вам доведеться додати дорожче обладнання.

Додавання такого обладнання не є ні простим, ні швидким, і може бути неефективним з точки зору витрат, якщо обсяги трафіку коливаються, а розширені можливості комутації та маршрутизації потрібні лише зрідка. У такому разі ви отримаєте дороге обладнання, яке буде використовуватися недостатньо. З цих причин трирівнева топологія зазвичай не ідеальна для центрів обробки даних, обсяги мережевого трафіку яких коливаються, хоча вона може добре працювати, коли рівні трафіку є стабільними та передбачуваними.

2. Верхня частина полиці

У топології центру обробки даних «top-of-rack» ви встановлюєте мережеві комутатори в кожній серверній стійці. Таким чином, топологія «top-of-rack» спрощує швидке та економічно ефективно додавання потужності.

Оскільки обсяг трафіку, який має обробляти кожен комутатор, менший, ніж у трирівневій топології (де кілька стійок можуть бути підключені до одного комутатора), підхід «верхня частина стійки» може використовувати менш дорогі комутатори.

Таким чином, топологія «top-of-rack» спрощує дешеве та швидке додавання потужності. Конструкції «top-of-rack» також масштабуються природним чином залежно від потужності центру обробки даних, оскільки чим більше серверних стійок ви додаєте, тим більше комутаторів ви додаєте.

Недоліком є те, що вам доведеться встановлювати та обслуговувати більше комутаторів, що збільшує експлуатаційне навантаження на команди, відповідальні за розгортання та управління мережевим обладнанням. Конструкції, що встановлюються зверху стійки, також можуть знижувати ефективність у ситуаціях, коли серверна стійка не надсилає або не отримує достатньо трафіку для використання своїх комутаторів на повну потужність.

3. Перемикання мереж

Комутована структура мереж у деяких аспектах схожа на трирівневу топологію, але з більшою кількістю комутаторів її легше масштабувати. Вона також нагадує топологію «top-of-rack», з тією ключовою відмінністю, що сервери не призначені постійно до конкретного комутатора, що дозволяє ефективніше використовувати його потужність.

Комутована структура (fabric) у деяких аспектах схожа на трирівневу топологію, але в ній є більша кількість комутаторів, що полегшує масштабування. Вона також схожа на топологію "top-of-rack", з головною відмінністю в тому, що сервери не призначені до конкретного комутатора, тому легше використовувати потужність комутатора ефективніше.

Основним недоліком комутуваних тканин є їхня складність; їх важко проектувати та впроваджувати, оскільки необхідно балансувати трафік та постійно реструктуризувати з'єднання між серверами та комутаційною тканиною.

4. Гібридна топологія

Гібридна топологія – це не окремий тип, а радше комбінація кількох підходів. Наприклад, ви можете розробити топологію, де деякі серверні стійки мають виділені комутатори, а інші сервери підключаються до більш гнучкої серверної структури. Такий підхід призведе до топології «top-of-rack» для однієї частини вашої мережі та комутованої структури для інших.

Як вибрати мережеву топологію для вашого центру обробки даних

Вибираючи, яка топологія мережі підходить для вашого центру обробки даних, слід врахувати такі ключові фактори:

- Потреби масштабованості: Якщо ви очікуєте високий ступінь коливань мережевого трафіку, конструкція з верхнім розташуванням стійки або комутована структура, ймовірно, буде кращою, оскільки вона легше масштабується.

- Фінансові ресурси: Трирівневі топології можуть мати вищі початкові витрати, оскільки вам потрібно купувати дорогі комутатори та маршрутизатори корпоративного класу. З іншого боку, конструкції верхньої стійки та комутованих мережевих структур часто вимагають вищих поточних витрат, оскільки вам потрібно додавати обладнання в міру масштабування та замінювати окремі комутатори, якщо вони виходять з ладу.

- Операційні ресурси: Якщо у вас менше технічних спеціалістів центру обробки даних, доступних для керування обладнанням, розгляньте можливість використання простішої топології, наприклад, трирівневої.

- Фізичні обмеження: Хоча мережеве обладнання та кабелі, що до нього підключаються, зазвичай не займають забагато місця порівняно із серверами, фізичні обмеження простору можуть бути проблемою, особливо в невеликих центрах обробки даних або серверних кімнатах. Якщо так, то трирівнева топологія, як правило, працює краще, оскільки вона не вимагає стільки окремих мережевих пристроїв або кабелів.

Використання хмарних обчислювальних сервісів зростає щороку [1] і має багатообіцяюче майбутнє [2] [3]. З 3,0 зеттабайтами IP-трафіку на рік та очікуваним трафіком 8,6 зеттабайтів у 2029 році [1], хмарний трафік зросте майже втричі. Однак цей трафік поділяється на три типи: від центрів обробки даних до користувачів, від центрів обробки даних до центрів обробки даних та всередині центрів обробки даних. Найбільша частина цього трафіку залишається всередині центрів обробки даних і відповідає типу трафіку всередині центрів обробки даних.

Щоб керувати таким величезним трафіком, приблизно 3342 екзабайти (ЕБ) у 2025 році та 7566 ЕБ, що очікуються у 2029 році [1], хмарні мережі перебувають під пильною увагою з метою пошуку нових рішень, що забезпечують достатню продуктивність та масштабованість. Серед цих нових рішень ми зосереджуємося як на TRILL (прозоре взаємозв'язок багатьох каналів) [4], так і на OpenFlow [5].

Перший має децентралізовану площину керування, тоді як другий має централізовану площину керування та центральний контролер. У розділах III-B та III-A ми детально розглядаємо відповідно TRILL та OpenFlow.

Другим за важливістю типом трафіку за кількістю є трафік від центру обробки даних до користувача. Очікується, що цей трафік зросте на 25% протягом наступних чотирьох років. Це показує як збільшення кількості клієнтів хмар, так і збільшення завдань, делегованих інфраструктурі хмари.

Останній тип трафіку, між центрами обробки даних, є найменш важливим за кількістю. Однак, він матиме найсильніше зростання, зі збільшенням на 31% протягом наступних чотирьох років. У цій статті ми зосереджуємося на цьому типі трафіку, який становить приблизно 7% від загального хмарного трафіку. Крім того, цей трафік між центрами обробки даних має інші обмеження, ніж два інших. Той факт, що він є міжцентровим, має бути прихований від користувачів хмар. У більшості випадків, коли відбувається зв'язок між центрами обробки даних, центри обробки даних належать одному

хмарному постачальнику. Тому здебільшого вони використовують одну й ту саму технологію. У цих випадках для рішення TRILL ми пропонуємо в [6] рішення, яке дозволяє взаємодіяти з кількома кампусами TRILL без їх об'єднання.

Однак у деяких випадках обидва центри обробки даних використовують різні технології, оскільки вони належать різним постачальникам. У [7] наведено декілька прикладів.

Перший – це хмарна федерація. Вона об'єднує хмарних постачальників, які спільно використовують свої ресурси за допомогою спільного регулювання для задоволення потреб своїх клієнтів.

Другий приклад – міжхмарне середовище. У цьому середовищі мережі кількох постачальників хмарних послуг взаємопов'язані, а їхні центри обробки даних використовують різні технології. У цих випадках трафік між центрами обробки даних має бути модифікований, щоб його приймав кожен центр обробки даних. Ця модифікація має бути прозорою для користувачів.

Третім прикладом може бути випадок, коли користувачі бажають скористатися перевагами продуктів різних постачальників хмарних послуг залежно від їхніх пропозицій та обмежень. Користувач може обрати одного постачальника хмарних послуг для зберігання величезної кількості даних, використовуючи іншого постачальника для його обчислювальної продуктивності, і, нарешті, обрати третього постачальника з високою пропускну здатністю для розміщення своїх веб-сервісів.

Четвертим прикладом може бути компанія, яка має кілька філій. Кожна філія підключена до найближчого центру обробки даних, щоб зменшити час доступу. Ми бачимо, що якщо немає міжхмарного доступу, то користувачі не зможуть досягти такого використання хмарних сервісів.

Спосіб взаємоз'єднання центрів обробки даних можна розділити на два підходи, кожен з яких має два рішення [7]. Якщо саме постачальник послуг хоче встановити взаємозв'язок центрів обробки даних, то це підхід, орієнтований на постачальника. В іншому випадку, коли клієнт хоче використовувати хмару кількох постачальників, це підхід, орієнтований на клієнта.

Серед підходів, орієнтованих на постачальника, є два рішення: федеративна хмара та гібридна хмара. У федеративному хмарному рішенні кілька постачальників хмарних послуг домовляються про правила та політики, що дозволяють взаємодію між своїми ресурсами.

Таким чином, вони можуть обмінюватися своїми невикористаними ресурсами один з одним. Клієнт хмари може навіть не знати про цей обмін ресурсами та використовувати інфраструктуру іншого постачальника.

Друге рішення – це гібридна хмара. У цьому рішенні організація з приватною хмарою, яка потребує більшої кількості ресурсів, використовуватиме хмару третьої сторони замість того, щоб розширювати власну інфраструктуру. Це рішення має економічну привабливість для клієнтів, оскільки таким чином їм не потрібно модифікувати свою приватну хмарну інфраструктуру.

Клієнтоорієнтований підхід містить два інших рішення: Мультихмарне рішення та Агрегований сервіс від брокера.

Мультихмарне рішення перекладає все управління кількома хмарними постачальниками та кількома технологіями на клієнта. У цьому випадку клієнту, можливо, доведеться розробити адаптер для API кожного постачальника. Таким чином, постачальники не знають про своє хмарне з'єднання, оскільки саме клієнт керує ним.

Останнє рішення, Агрегований сервіс від брокера, схоже на попереднє, за винятком того, що клієнт не повинен керувати абстракцією API. Натомість клієнти використовують послуги третьої сторони, яка називається брокером. Він надає єдиний API для кількох хмарних постачальників, абстрагуючи кожен з API постачальників.

У даній роботі ми зосереджуємося на підході, орієнтованому на постачальника, а точніше на федеративному хмарному рішенні. Ми розробили рішення для з'єднання кількох

центрів обробки даних за допомогою двох різних технологій. Це рішення є шлюзом, який з'єднує центри обробки даних за допомогою TRILL або OpenFlow.

Передумови OpenFlow

OpenFlow має централізовану площину керування, один центральний контролер та стандартні комутатори OpenFlow. Контролер OpenFlow має глобальне уявлення про топологію мережі та віртуальні мережі клієнтів. Контролер приймає кожне рішення щодо маршрутизації та кожне рішення щодо комутації всередині цієї мережі. Протокол OpenFlow здатний взаємодіяти з обладнанням, сумісним з OpenFlow, для заповнення їхньої таблиці комутації.

Ці таблиці комутації дозволяють застосовувати певний набір правил до кожного потоку. У разі відсутності таких правил для потоку, цей потік надсилається комутатором до контролера. Контролер є єдиним пристроєм, здатним вирішувати, які правила застосовувати до цього потоку.

Сумісні комутатори OpenFlow можуть бути як апаратними, так і програмними. Наприклад, Open vSwitch – це віртуальний комутатор, призначений для програмних гіпервізорів. Він пропонує мережеве підключення для віртуальних машин. Open vSwitch працює через таблицю потоків, яка визначає правила та дії для кожного потоку. Для ізоляції потоків кожного орендаря, комутатори OpenFlow можуть використовувати протоколи тунелювання, такі як VLAN або GRE. Однак, OpenvSwitch також може керувати протоколом бездержавного транспортного тунелювання (STT), успадкованим від розробки Nicira.

Архітектура OpenFlow містить принаймні один контролер, підключений до одного або кількох комутаторів OpenFlow. Контролер транслює всі свої правила на підключені комутатори через певний захищений канал. Ці комутатори зберігають усі ці правила у своїх таблицях комутації. Ці таблиці потім використовуються щоразу, коли комутатор отримує пакет, щоб визначити, як обробити пакет. Такий підхід має перевагу в централізації процесу прийняття рішень лише на одному логічному пристрої.

Логічна централізація процесу прийняття рішень дозволяє краще керувати кожним потоком від початку до кінця. Це також запобігає неузгодженості в обробці потоку та дозволяє швидко транслювати оновлення процесу потоку.

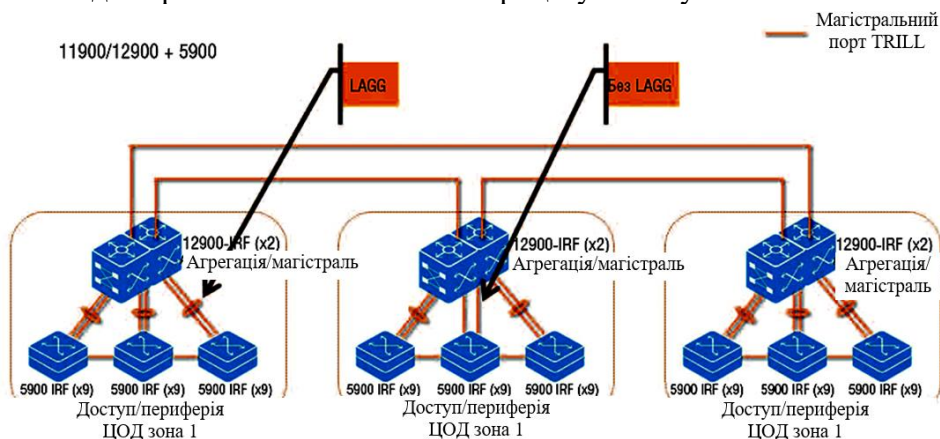


Рисунок 1 – Структурна схема системи

Передумови прозорого з'єднання багатьох каналів (TRILL)

На відміну від централізованої площини керування OpenFlow, TRILL [4] має децентралізовану площину керування. Це призводить до більшої стійкості TRILL, ніж OpenFlow. TRILL не має єдиної точки відмови, на відміну від Openflow та його контролера. TRILL – це протокол другого рівня з повною неблокуючою структурою, яка дозволяє будь-яке з'єднання в мережі. Новий компонент (RBridge) визначається специфікаціями TRILL для заміни традиційних комутаторів. Навіть якщо не всі комутатори потрібно замінити для роботи TRILL, вибір комутаторів для заміни є важливим. Фактично, RBridge діє як проксі, додаючи свою адресу до кадру.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів проектування та побудови топології мереж у центрах обробки даних. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем проектування та побудови топології мереж у центрах обробки даних.
- Досліджена система проектування та побудови топології мереж у центрах обробки даних.
- На основі отриманих результатів досліджень створена програмна реалізація системи проектування та побудови топології мереж у центрах обробки даних.
- Розроблені алгоритми дозволяють успішно вирішувати завдання проектування та побудови топології мереж у центрах обробки даних. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Smirnov, O., Odarchenko, R., Smirnova, T., Bondar, S., Volosheniuk, D. «Optimal Structure Construction of Private 5G Network for the Needs of Enterprises». Lecture Notes on Data Engineering and Communications Technologies, 2023, 178, pp. 208–223.
2. Аль-Мудхафар Акіл Абдулхуссейн М., Смірнова Т.В., Буравченко К.О., Смірнов О.А. «Метод оцінки та підвищення користувальницького досвіду абонентів в програмно-конфігурованих мережах на основі використання машинного навчання». Сучасні інформаційні системи, 2023, том 7, № 2, С. 49-56.
3. Smirnova, T., Gnatyuk, S., Yudin, O., Sydorenko, V., Polozhentsev, A., «The Model for Calculating the Quantitative Criteria for Assessing the Security Level of Information and Telecommunication Systems». CEUR Workshop Proceedings Volume 3156, 2022, Pages 390-399.
4. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». Проблеми інформатизації та управління, № 2(70). 2022. С. 28-37.
5. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 3(69). С. 93-98.
6. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Вісник Хмельницького національного університету. Серія: «Технічні науки», № 2 (307). С. 46-52. 2022.
7. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 1(67). С. 84-89.
8. Smirnova T., Gnatyuk S., Berdibayev R., Avkurova Zh., Iavich M. «Cloud-Based Cyber Incidents Response System and Software Tools». Communications in Computer and Information Science, 2021, vol 1486. Springer, Cham. pp 169-184.
9. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
10. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». Journal of theoretical and applied information technology Vol.98. No 21, 2020, P. 3334-3346.
11. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177.
12. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587.
13. Smirnov, O., Markovets, O. Vovk, N., Turchyn, Y., «Model of informational support for social network administrators' content creation». CEUR Workshop Proceedings Volume 2616, 2020, Pages 125-136.
14. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic

- generation by a model of generator on the graph». CEUR Workshop Proceedings Volume 2616, 2020, Pages 366-379.
15. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645.
 16. Smirnov O., Kuznetsov A., Zaichenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019; Odessa; Ukraine; 9-13 September 2019. P.22-28.
 17. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.
 18. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019 . P.517-522.
 19. Smirnov, O., Odarchenko, R., Abakumova, A., Usik, P., Kundyzy, M., «QoE optimization technique for media delivery in 5G networks». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019. P.597-601.
 20. Smirnov, O., Krasnobayev, V., Yanko, A., Kuznetsova, T. «Methods of nulling numbers in the system of residual classes». CEUR Workshop Proceedings, Vol 2588, P. 90-106, 2019.
 21. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Averchev, A., Pastukhov, M., Kuznetsova, K., «Formation of Pseudorandom Sequences with Special Correlation Properties», 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT -2019/ Lviv, Ukraine, 2-6 July, 2019, P. 395-399.
 22. Smirnov, O., Kuznetsov, A., Kiian, A., Zamula, A., Rudenko, S., Hryhorenko, V., «Variance Analysis of Networks Traffic for Intrusion Detection in Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 353-358.
 23. Smirnov, O., Kuznetsov, A., Kavun, S., Babenko, B., Nakisko, O., Kuznetsova, K., «Malware Correlation Monitoring in Computer Networks of Promising Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 347-352.
 24. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Pastukhov, M., Kuznetsova, K., Prokopovych-Tkachenko, D., «Discrete Signals with Special Correlation Properties», CEUR Workshop Proceedings Volume 2353, CEUR Workshop Proceedings 2019, Pages 618-629.
 25. Smirnov A.A., Kuznetsov A.A., Danilenko D.A., Berezovsky A., «The statistical analysis of a network traffic for the intrusion detection and prevention systems», Telecommunications and Radio Engineering. – Volume 74, Issue 1. – Begel House Inc. – 2015. – P. 61-78.
 26. Смірнов О.А., Смірнова Т.В., Буравченко К.О., Кравченко С.С., Горбов В.О., «Хмарна система підтримки прийняття рішень технологічного процесу відновлення поверхонь конструкцій і деталей машин». Сучасні інформаційні системи. 2021. Т. 5, № 4. С. 79-95
 27. Смірнов О.А., Усік П.С., Миронець І.В., Буравченко К.О., Якименко Н.М. «Метод підвищення ефективності розподіленої обробки даних у комп'ютерних системах операторів стільникового зв'язку» Вісник Черкаського державного технологічного університету. Технічні науки. №4. С. 103-110. 2020.
 28. О.А.Смірнов, Т.В.Смірнова, Л.І. Поліщук, К.О. Буравченко, А.О.Макевнін, «Дослідження хмарних технологій як сервісів», Кібербезпека: освіта, наука, техніка. № 3(7). С. 43-62. 2020.
 29. Смірнов О.А., Коноплицька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Поліщук Л.І. Інформаційна безпека в комп'ютерних мережах. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2020. – 294 с.
 30. О.А. Смірнов, П.С. Усік, «дослідження перспектив використання технологічних рішень в мережах 5g» у Кібербезпека та інформаційні технології: монографія. – Х. : ТОВ «ДІСА ПЛЮС», 2020.С. 122-135.
 31. Смірнов О.А., Дреєва Г.М., Дреєв О.М., Смірнова Т.В. «Фрактальний аналіз генератора самоподібного трафіку на основі ланцюга Маркова». Центральнотрапівський науковий вісник. Технічні науки. № 2(33). с. 161-172, 2019.
 32. Смірнов О.А., Коноплицька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В. Поліщук Л.І. Проектування комп'ютерних систем та мереж. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2019. – 264 с.

УДК 004

С.Приймак, магістр гр. КН-24М,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ОНЛАЙН-СЕРВІСУ ДЛЯ РЕДАГУВАННЯ ЗОБРАЖЕНЬ ЗА ДОПОМОГОЮ ШТУЧНОГО ІНТЕЛЕКТУ

У статті розроблено програмне забезпечення, яке призначено для системи онлайн-сервісу для редагування зображень за допомогою штучного інтелекту. Метою розробки є дослідження та принципи побудови системи онлайн-сервісу для редагування зображень за допомогою штучного інтелекту. Об'єктом дослідження є процес онлайн-сервісу для редагування зображень за допомогою штучного інтелекту. Предметом дослідження є методи онлайн-сервісу для редагування зображень за допомогою штучного інтелекту. Методи дослідження базуються на методах обробки графічної інформації, методах штучного інтелекту, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи онлайн-сервісу для редагування зображень за допомогою штучного інтелекту. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

онлайн-сервіс, редагування зображень, штучний інтелект

Постановка проблеми. Якщо ви створюєте контент онлайн, ви знаєте, що привабливе візуальне оформлення має значення. Воно впливає на те, скільки часу люди проводять над вашим контентом і як вони з ним взаємодіють.

Ви маєте справу з аудиторією з дефіцитом уваги, конкуруючи з усіма видами контенту, доступними в Інтернеті, не лише з письмовими публікаціями чи відео.

Вам потрібен цей X-фактор, щоб зупинити вашу аудиторію посеред прокручування. Високоякісне зображення може бути цією зупинкою прокручування.

Важливо оптимізувати ваші онлайн-зображення та зробити їх відповідними для платформи. Ви не можете просто використовувати селфі, зроблене у вітальні, як портрет у LinkedIn, або розміщувати низькоякісне зображення у своїй SEO-статті.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи онлайн-сервісу для редагування зображень за допомогою штучного інтелекту.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи онлайн-сервісу для редагування зображень за допомогою штучного інтелекту.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем онлайн-сервісу для редагування зображень за допомогою штучного інтелекту.
- Дослідження системи онлайн-сервісу для редагування зображень за допомогою штучного інтелекту.
- Програмна реалізація системи онлайн-сервісу для редагування зображень за допомогою штучного інтелекту.

Об'єктом дослідження є процес онлайн-сервісу для редагування зображень за допомогою штучного інтелекту.

Предметом дослідження є методи онлайн-сервісу для редагування зображень за допомогою штучного інтелекту.

Методи дослідження базуються на методах обробки графічно інформації, методах штучного інтелекту, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Завдяки набору функцій на платформі розробленого в даній роботі програмного забезпечення перетворювати ідеї в чудові дизайни дуже просто. Досить підібрати найбільш підходящу графіку, зображенні й шрифти, а потім скористатися конструктором розробленого в даній роботі програмного забезпечення, щоб створити дизайн.

Незалежно від того, що буде являти собою ваш наступний дизайн: творчий колаж, графіку для соціальних мереж або навіть макет веб-сторінки, – за допомогою функцій розробленого в даній роботі програмного забезпечення кожний може створювати чудові роботи.

Засіб обробки зображень: нехай зображенні виглядають красиво

Правда, некрасиво, якщо фото перекошено, немов сумно висячий на цвяху портрет? Якщо надто нахилили фотоапарат, коли робили знімок, або злегка навскіс помістили фото в сканер, використовуйте функцію повороту, щоб вирівняти кожну зображення.

На платформі розробленого в даній роботі програмного забезпечення не витрачається час на промальовування: ефекти повороту відображаються в реальному часі на всіх ділянках дизайну, щоб зображення було рівним і гарним.

Обрізка зображень: обрізайте зображенні, щоб помістити їх у рамку й скласти митецьку композицію

Часи ножиців, кадрування й кашування давно пройшли. На платформі розробленого в даній роботі програмного забезпечення можна створювати творчі роботи, використовуючи цифрову обрізку. Кожну зображення у вашій дизайні можна обрізати, масштабувати й переміщати всього декількома клацаннями миші.

Обрізайте власні зображенні, щоб виправити композицію, або зображення з нашої великої бібліотеки, щоб додати їм новий вид. І не переживайте, що можете не вписати в сітку або рамку.

Друкуйте текст на зображеннях, щоб у кожного знімка була своя історія

За допомогою графічного редактора зображень на платформі розробленого в даній роботі програмного забезпечення дуже просто надрукувати текст на зображенні, щоб поділитися важливою інформацією або, наприклад, перетворити врівноваженого домашнього улюбленця в прикольного кота з інтернет-мемів. Розмістивши зображення, виберіть засіб додавання тексту, щоб відкрити велику добірку текстових шаблонів і макетів з ідеально підібраними шрифтами й стильним оформленням.

Можна навіть форматувати повідомлення, підібравши свій власний шрифт, стиль і колір. Можливості безмежні.

Засіб створення хмарини з текстом: оживете думки й слова на фото за допомогою хмарини з текстом

Представте на загальний огляд свої пригоди разом із друзями у вигляді коміксу. Додавайте хмарини з текстом у будь-який дизайн і заповнюйте їхніми влучними репліками. Шукайте в нашій бібліотеці хмарини з текстом різноманітних квітів і стилів, перетаскуйте їх прямо у свій макет, клацайте й починайте вводити напису. Незалежно від того, чи хочете скласти комікс із власних зображень або показати багатий внутрішній мир герані на підвіконні, додавати хмарини з текстом на платформі розробленого в даній роботі програмного забезпечення можна за дві секунди.

Додайте зображенням елегантною приглушеності за допомогою налаштувань прозорості

Привнесіть у дизайн глибину, міняючи прозорість. Налаштовуйте прозорість кожного елемента дизайну, натискаючи на стрілку долілиць і пересуваючи відповідного повзунка. Збільшуючи прозорість по своєму смаку, можна додати зображенню делікатний приглушений вид. Помістите за прозорим зображенням кольорові фігури й фони для

яскравого ефекту й художньої краси або сполучіть прозорість із фотофільтрами, щоб поекспериментувати із видом зображень.

Засіб редагування зображень: редагуйте зображення, щоб виправити невдалі знімки

Імпортуйте зображення на платформу розробленого в даній роботі програмного забезпечення, щоб вони засяяли яскравіше, ніж на плівці, за допомогою цілого набору засобів фоторедагування. Зображення виглядає тускло й розмито? Спробуйте збільшити насиченість. Знімок темнуватий і мрачнуватий? Налаштуйте яскравість і контраст, поки об'єкт не стане чітко видно.

Всі зміни відображаються на екрані макета відразу ж, а ми не випустимо з уваги оригінальні файли, щоб могли редагувати їх і застосовувати фільтри знову й знову.

Розмиття фото: додайте зображенням художності за допомогою повзунка розмиття

Мир стає набагато краще, якщо згладжувати гострі кути. Додайте своїм дизайнам наліт ефемерності, небагато розмив зображення. Можливості для творчості практично безмежні! Зробіть зображенню злегка розмитої, щоб зробити її схожою на знімок з фотокабінки, або істотно додайте розмитості, щоб використовувати фото як тло для інших елементів дизайну. Перемістите повзунка розмитості в іншу сторону, щоб додати різкості – відмінний засіб, якщо треба акцентувати деталі на знімку або виправити розмиту зображення.

Ефект віньєтування: додайте знімкам відтінок вінтажності

Крім запечатління казкової моди тих часів старі зображення на плівці передають тепле почуття ностальгії, що дуже важко відтворити. Відтворіть ефект затемнення по краях знімка, характерний для стародавніх фотоапаратів, використовуючи ефект віньєтування на своїх зображеннях. За допомогою легкого ефекту віньєтування так багато чого можна досягти: додати зображенням наліт меланхолії відтінками сірого кольору або поліпшити композицію, акцентувавши увагу на центрі знімка. Використовуйте ефект віньєтування разом з фотофільтрами, щоб додати зображенням шикарний ретро-вид.

Розмітка: якщо в пошуку ідей для макета, спробуйте розмітку

Почніть працювати над дизайном не голіруч! У нас на вибір є маса варіантів розмітки, щоб розділити сторінку навпіл, на чотири частини або застосувати більше складну розбивку. Після вибору розмітки дуже просто перетаскувати в дизайн власні зображення, використовувати зображення з нашої бібліотеки або заливати поля кольором. Ми навіть подбаємо про обрізок! Розмітка ідеально підходить для фотоколлажів, публікацій у соціальних мережах, графіки для блогів і т.д.

Безкоштовні значки: доповнюйте свої дизайни яскравими значками

Є чи щось більше пізнаване, чим великий жовтий смайл? Крім великої бібліотеки зображень одержуєте доступ до безлічі векторних і графічних зображень, які можна використовувати в дизайнах. Сполучіть у своїх дизайнах значки, що притягають погляд, і символи, щоб додати роботам закінчений сучасний вид. Використовуйте значки разом з яскравими шрифтами, щоб створювати вивіски, фірмові бланки, логотипи, візитні картки й багато чого ще!

Фоторамки: додавайте фоторамки, щоб прикрасити пам'ятні знімки

Самі дорогоцінні моменти в житті заслуговують самого дбайливого поводження! Помістіть знімки з пам'ятними подіями в чудову фоторамку. Від милих до кричущих – у нас на вибір представлена безліч фоторамок, які допоможуть пожвавити зображенню. Відкрийте нашу бібліотеку й вибирайте круглі, дурненькі, прості рамки – вибір за вами. Потім перетягнете в дизайн власні зображення або інші зображення з нашої бібліотеки, а ми обріжемо й масштабуємо їх точно під розмір рамки.

Макет веб-сторінки: почніть із азів і створіть макет веб-сторінки

Почніть дизайн веб-сайту з макета веб-сторінки – грубого начерку користувальницького інтерфейсу й функціональності сайту. Можна не тільки перетаскувати

в дизайн і розміщати прості фігури, але й вибирати повністю готові до використання віджети, бічні панелі й елементи інтерфейсу з нашої безкоштовної бібліотеки зображень. Функції й ефекти, які пропонує платформа розробленого в даній роботі програмного забезпечення, дозволяють не тільки налаштовувати дизайн до одержання потрібного результату, але ще й без зайвих зусиль перетворити готовий макет веб-сторінки в повномасштабну дизайнерську модель.

Наклейки: прикрасьте свої зображення несподіваними наклейками

Поверніться у веселі шкільні роки за допомогою цифрових наклейок! Уведіть «наклейки» у поле пошуку нашої бібліотеки зображень і вибирайте з безлічі ексцентричних слоганів і безневинних штампів, які можна перетягнути у свої колажі й зображення у соцмережах. Прикрасьте зображення коханої людини наклейкою й покажіть, що ні про кого іншому не можете думати, або оживете колаж із зображень поїздки за допомогою смішних крилатих фраз і висловлень.

Таблички з ім'ям: створюйте ефектні таблички з ім'ям за допомогою розробленого в даній роботі програмного забезпечення

Готуєтеся до конференції або перспективних переговорів? Зробіть незабутнє перше враження елегантною табличкою з ім'ям! Виберіть один з наших численних текстових шаблонів, щоб доповнити дизайн гарними шрифтами, які міняють розмір у міру введення тексту. Можна навіть налаштовувати кольору й додавати логотип компанії або іншу інформацію, по якій вас довідаються. За допомогою розробленого в даній роботі програмного забезпечення неодмінно створите табличку з ім'ям, що буде виділятися з юрби.

Додайте текстуру: додайте в дизайн текстуру з нашої бібліотеки зображень, настільки правдоподібну, що до нього захочеться доторкнутися

Коли одного тільки кольору недостатньо, додайте в дизайн текстуру за допомогою розробленого в даній роботі програмного забезпечення! Вибирайте з розмаїтості текстурованих фонів: від справжнього паперу й тканин до фантастичних дизайнів і візерунків. Знаходьте текстури в нашій бібліотеці зображень, доповнюйте їхніми фотофільтрами й регулюйте прозорість для будь-якого елемента дизайну.

Зі швидким розвитком штучного інтелекту він змінює те, як ми створюємо зображення та взаємодіємо з ними. Від автоматизованого редагування та ретушування фотографій у фотографії до генеративного дизайну в графічному мистецтві, ШІ не лише оптимізує робочі процеси, але й відкриває нові творчі можливості. У цій публікації ми дослідимо, як ШІ трансформує візуальний ландшафт, обговоримо його застосування в різних творчих дисциплінах та розглянемо виклики та етичні міркування, пов'язані з цими змінами.

Штучний інтелект у фотографії: переосмислення мистецтва знімка

Автоматизоване редагування та інтелектуальні покращення

Один з найперших наслідків використання штучного інтелекту у фотографії – це постпродакшн. Передові алгоритми тепер виконують завдання, які раніше вимагали годин ручної роботи. Інструменти, які автоматично покращують освітлення, колір та різкість, стають стандартом, гарантуючи, що кожне зображення досягає професійної якості з мінімальними втручаннями. Наприклад, рішення на базі штучного інтелекту, такі як функції автоматичного покращення, оптимізують процес редагування, дозволяючи фотографам зосередитися на творчості, а не на виснажливому налаштуванні. Ці досягнення майже миттєво перетворюють навіть аматорські знімки на фотографії, готові до публікації.

Зараз митці вчаться використовувати абсолютно нові інструменти для візуальної творчості.

У швидкозмінному ландшафті штучного інтелекту інструменти штучного інтелекту революціонізують наш підхід до створення візуального контенту. Використовуючи передові алгоритми штучного інтелекту, цей інструмент дозволяє користувачам без зусиль збільшувати масштаб зображень, видаляти шуми та коригувати кольори, забезпечуючи високоякісні результати, придатні як для цифрових, так і для друкованих носіїв. Незалежно від того, чи ви фотограф, який прагне врятувати недоекспоновані знімки, чи графічний

дизайнер, який шукає ефективні рішення для редагування, інтеграція таких інструментів на базі штучного інтелекту у ваш робочий процес може значно підвищити продуктивність та креативність.

Корекція обличчя, ретуш та не тільки

З'явилися інноваційні функції, такі як заміна обличчя та корекція погляду, які дозволяють фотографам легко виправляти ледь помітні недоліки. Уявіть собі портрет, де вираз обличчя об'єкта зйомки не зовсім правильний; за допомогою еталонного фото та інструментів ретушування обличчя за допомогою штучного інтелекту ви тепер можете замінити його ідеальною посмішкою або відкритими очима. Таке інтелектуальне ретушування не лише зберігає автентичність зображення, але й підвищує його загальну привабливість.

Ці досягнення швидко стають важливими в таких галузях, як весільна фотографія, портретна фотографія та висвітлення подій, де важливий кожен вираз обличчя.

Пошук облич та інтелектуальне зіставлення

Передова технологія пошуку облич змінює те, як фотографи та редактори організовують та покращують свою роботу. Завдяки пошуку за допомогою розпізнавання облич на основі штучного інтелекту тепер можна швидко знаходити певних людей серед тисяч зображень, що робить процес вибору ідеального знімка швидшим та інтуїтивнішим. Незалежно від того, чи складаєте ви весільний альбом, чи куруєте яскраві моменти події, пошук облич гарантує, що жодного важливого моменту чи людини не буде пропущено. Цей розумний інструмент сортування стає незамінним у робочих процесах, де точність, швидкість та персоналізація є ключовими.

Штучний інтелект у графічному дизайні: розширення можливостей креативності через автоматизацію

Генеративний дизайн та моделі перетворення тексту в зображення

Графічний дизайн зазнає трансформації з появою генеративного штучного інтелекту. Дизайнери тепер мають доступ до потужних інструментів, які можуть створювати кілька ітерацій дизайну за лічені секунди. Моделі перетворення тексту на зображення, такі як DALL-E, Midjourney, FLUX та Stable Diffusion, дозволяють творцям перетворювати прості підказки на яскраві візуальні елементи. Така демократизація дизайну означає, що навіть ті, хто має обмежені технічні навички, можуть створювати роботи професійного рівня, відкриваючи творчий процес для ширшої аудиторії.

Налаштування та ефективність у творчому робочому процесі

Штучний інтелект також революціонізує традиційні робочі процеси графічного дизайну, автоматизуючи повторювані завдання. Від зміни розміру зображень до налаштування макетів на основі евристики дизайну, ці інструменти звільняють дорогоцінний час для творчих ідей. Такі платформи, як Freepik AI Suite, Adobe Express та Pixlr, мають інтегровані функції на базі штучного інтелекту, які допомагають дизайнерам створювати дошки настрою, оптимізувати макети та навіть видаляти відволікаючі елементи із зображень – і все це за лічені кліки.

Для багатьох креативних фахівців це означає ефективніший робочий процес, який дозволяє їм зосередитися на інноваціях, а не на ручному налаштуванні. Як результат, компанії можуть масштабувати свою творчу продукцію без шкоди для якості, знижуючи витрати, зберігаючи при цьому високий стандарт візуального контенту.

Мистецтво, згенероване штучним інтелектом, та новий ландшафт візуальних медіа

Дія штучного інтелекту виходить далеко за межі традиційної фотографії та графічного дизайну. У сфері образотворчого мистецтва візуальні ефекти, створені штучним інтелектом, викликали дебати про авторство, креативність та оригінальність. Такі митці-піонери, як Девід Салле, навіть почали інтегрувати штучний інтелект у свій творчий процес, використовуючи його як інструмент для концептуалізації варіацій або мозкового штурму нових ідей. Ця співпраця між людською винахідливістю та машинним навчанням призвела

до появи творів мистецтва, які кидають виклик нашому розумінню креативності та автентичності.

Машинні галюцинації та ера «промптографії»

Виставки та фестивалі зараз присвячують цілі шоу зображенням, створеним штучним інтелектом. Такі проекти, як Photo Brussels 2025, демонструють роботи, де штучний інтелект «винаходить» альтернативні реальності, розмиваючи межу між фактом і вигадкою. Ці проекти не лише підкреслюють технічну майстерність сучасного штучного інтелекту, але й запрошують глядачів поставити під сумнів природу пам'яті, історії та самого мистецтва. Вони слугують нагадуванням про те, що хоча штучний інтелект може імітувати реальність, він також відкриває абсолютно нові світи для художнього вираження.

Демократизація візуальної творчості

Мабуть, найбільш трансформаційним аспектом штучного інтелекту у візуальній роботі є його здатність демократизувати творчість. Люди з будь-яким досвідом більше не обмежуються дорогим обладнанням чи передовими технічними навичками, тому тепер можуть створювати переконливий візуальний контент. Цей зсув вже очевидний у сплеску користувацького контенту в соціальних мережах, де програми для редагування та інструменти дизайну на базі штучного інтелекту роблять зображення професійної якості доступними для всіх.

Наслідки для бізнесу та промисловості: нова ера візуальної роботи

Економічна ефективність та масштабованість

Для бізнесу інтеграція штучного інтелекту у візуальне виробництво є революційним рішенням. Тепер компанії можуть створювати високоякісний візуальний контент за значно меншу вартість та час, ніж раніше. Ця ефективність особливо цінна в таких галузях, як електронна комерція, реклама та цифровий маркетинг, де візуальний контент є ключовим. Інструменти штучного інтелекту допомагають оптимізувати робочі процеси, зменшити обсяг ручної праці та забезпечити швидке створення прототипів, забезпечуючи гнучкість бізнесу в умовах швидкоплинного цифрового середовища.

Розширення ринкових можливостей

Оскільки інструменти штучного інтелекту стають все більш складними, вони готові розширити креативний ринок неочікуваним чином. Традиційні ролі у фотографії та дизайні розвиваються, з'являються нові можливості працевлаштування для інженерів-прогнозистів, кураторів контенту зі штучним інтелектом та гібридних креативних директорів. Ці ролі скорочують розрив між технологіями та мистецтвом, гарантуючи, що людська креативність залишається на передньому краї, одночасно використовуючи ефективність штучного інтелекту.

Співпраця між людьми та машинами

Замість того, щоб замінити людський талент, ШІ стає партнером для співпраці. Майбутнє візуальної роботи полягає у використанні унікальних сильних сторін як людської творчості, так і машинної точності. Як наголошує генеральний директор Adobe Шантану Нараєн, ШІ покликаний бути інструментом, який посилює наші творчі можливості, а не замінює їх. Ця модель співпраці вже очевидна в передових проектах і продовжуватиме формувати майбутнє креативних індустрій.

Етичні міркування та виклики

Автентичність та цінність людського дотику

Хоча ШІ пропонує неймовірні переваги, він також порушує важливі питання щодо автентичності. Оскільки зображення, створені ШІ, стають більш реалістичними, розрізняти мистецтво, створене людиною, та мистецтво, створене машиною, ставатиме дедалі складніше. Це розмивання меж може знецінити «людський дотик», який, на думку багатьох, є невід'ємною частиною справжньої творчості. Критики стверджують, що надмірна залежність від ШІ може призвести до гомогенізації візуального контенту, де оригінальність приноситься в жертву заради ефективності.

Боротьба з упередженнями та забезпечення справедливості

Ще одна проблема полягає у вирішенні проблеми упереджень, вбудованих в алгоритми ШІ. Оскільки ці системи навчаються на існуючих наборах даних, вони можуть ненавмисно відтворювати культурні чи соціальні стереотипи. Для розробників вкрай важливо створювати етичні рамки та різноманітні навчальні набори даних, які забезпечують справедливе представництво та мінімізують ненавмисні упередження у візуальних елементах, створених ШІ.

Баланс інновацій та відповідальності

Зрештою, майбутнє штучного інтелекту у візуальній творчості залежатиме від знаходження правильного балансу між прийняттям інновацій та підтримкою етичної відповідальності. Оскільки штучний інтелект продовжує розвиватися, постійний діалог між митцями, технологіями та етиками буде важливим для того, щоб ці інструменти служили силою добра, збагачуючи наш творчий ландшафт без шкоди для художньої цілісності.

Погляд у майбутнє: Бачення спільного творчого майбутнього

Злиття штучного інтелекту та візуальної творчості все ще перебуває на ранній стадії, проте потенціал величезний. Від революційних змін у фотографії за допомогою автоматизованого редагування та інтелектуальних покращень до трансформації графічного дизайну за допомогою генеративних моделей, штучний інтелект готує ґрунт для нової ери творчості. Хоча проблеми, пов'язані з автентичністю, упередженістю та витісненням робочих місць, залишаються, потенціал співпраці між людьми-митцями та інструментами штучного інтелекту пропонує обнадійливе та динамічне майбутнє.

Дивлячись у майбутнє, стає зрозуміло, що креативні індустрії продовжуватимуть розвиватися, інтегруючи штучний інтелект не як заміну людської винахідливості, а як потужний інструмент, що покращує наше творче самовираження та розширює наші мистецькі горизонти. Сприймаючи цю технологію з етичним передбаченням та духом співпраці, ми можемо відкрити безпрецедентні можливості у візуальній творчості та сформувати майбутнє, де мистецтво та інновації йдуть пліч-о-пліч.

На завершення, майбутнє штучного інтелекту у зображеннях та візуальній роботі – це не кінець творчості, а трансформація, яка дозволить нам досягати більшого, швидше та ефективніше, не втрачаючи душі мистецтва. Незалежно від того, чи ви фотограф, графічний дизайнер чи цифровий художник, революція штучного інтелекту вже тут, щоб розширити ваш творчий шлях.

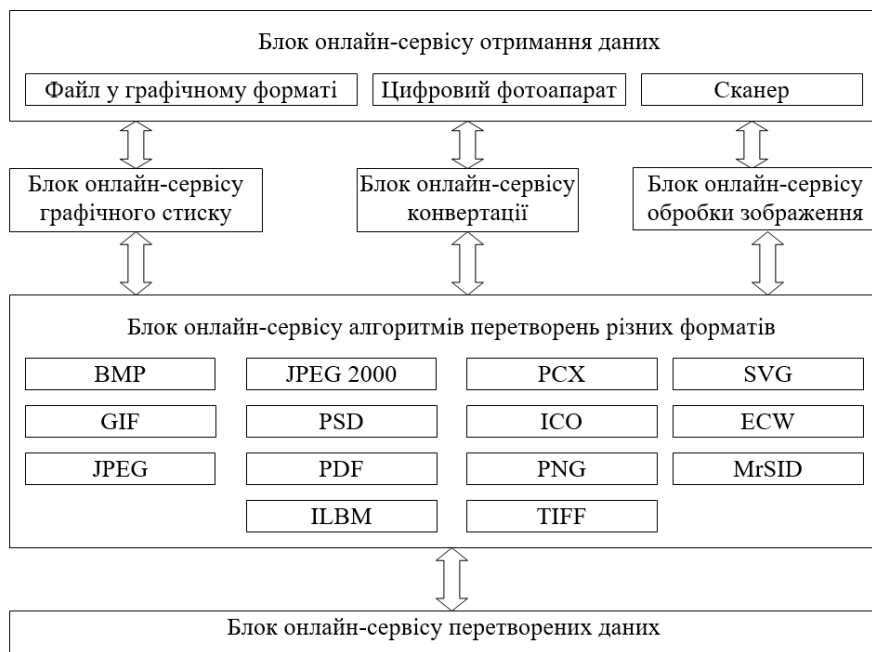


Рисунок 1 – Структурна схема системи

Структурна схема системи складається з наступних блоків онлайн-сервісів: 1. Блок онлайн-сервісу алгоритмів перетворень різних форматів. 2. Блок онлайн-сервісу отримання даних: – Отримання даних з файлу у графічному форматі. – Отримання даних зі сканера або цифрового фотоапарату. 3. Блок онлайн-сервісу обробки зображення – призначений для обробки зображення, тобто являє собою невеликий графічний редактор. 4. Блок онлайн-сервісу конвертації форматів – призначений для конвертації графічних файлів з одного формату у інший. 5. Блок онлайн-сервісу графічного стиску даних – призначений для стиснення даних, отриманих зі сканера, у графічний файл. 6. Блок онлайн-сервісу перетворених даних – призначений для реалізації іншого алгоритму стиску даних, ніж той, що був, до конвертації.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів онлайн-сервісу для редагування зображень за допомогою штучного інтелекту. Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем онлайн-сервісу для редагування зображень за допомогою штучного інтелекту.

– Досліджена система онлайн-сервісу для редагування зображень за допомогою штучного інтелекту.

– На основі отриманих результатів досліджень створена програмна реалізація системи онлайн-сервісу для редагування зображень за допомогою штучного інтелекту.

Розроблені алгоритми дозволяють успішно вирішувати завдання онлайн-сервісу для редагування зображень за допомогою штучного інтелекту. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Kuznetsov, O., Smirnov, O., Akhmetov, B., Alimseitova, Z., Imoize, A.L. «Deep Learning Frontiers in Copy-Move Forgery Detection: Advances, Challenges, and Future Directions». *Advancements in Cybersecurity Next Generation Systems and Applications*, 2025. 202-229.
2. Вінтенко Б., Смірнов О., Миронець І., Смірнова Т., Смірнов С. «Імітаційна модель шляхів вхідних даних комп'ютерної інтелектуальної системи підтримки оператора енергоблоку АЕС». Комбінаторні конфігурації та їхні застосування: Матеріали XXVII Міжнародного науково-практичного семінару, присвяченого 125-річчю Національного університету «Запорізька політехніка» (Запоріжжя-Кропивницький-Київ, 4-6 червня 2025 р.). Запоріжжя: НУ «Запорізька політехніка», 2025. С.82-91.
3. Al-Azzeh, J., Ayyoub, B., Mesleh, A., Smirnova, T., Gnatyuk, S., Drieiev, O., Smirnov, O., Dorenskyi, O. «Cloud-Based Information System for Evaluating Caverns in the Process of Blasting Metal Surfaces of Details». *International Review on Modelling and Simulations* 18 (1), 2025. pp. 32-42.
4. Вінтенко Б.Ю., Смірнов О.А., Миронець І.В., Смірнова Т.В., Коваленко О.В., Мацуй А.М. «Модель шляхів отримання вхідних даних комп'ютерної інтелектуальної системи підтримки оперативного персоналу АЕС». *Центральноукраїнський науковий вісник. Технічні науки*. 2025. Вип. 11(42), ч. II. С.52-62.
5. Вінтенко Б.Ю., Смірнов О.А., Миронець І.В., Смірнова Т.В. «Методи забезпечення відмовостійкості інтелектуальних систем підтримки оператора». VIII міжнародна науково-практична конференція «Інформаційна безпека та комп'ютерні технології», м. Кропивницький. 24-25 квітня 2025 р. – Кропивницький: ЦНТУ. – 2025. – С. 44-46.
6. Смірнов, О.А., Константинова, Л.В., Коноплицька-Слободенюк, О.К., Козірова, Н.В., Якименко, Н.М., Доренський, О.П., Буравченко, К.О. «Дослідження інструментів штучного інтелекту для роботи з базами даних та аналізу даних». *Кібербезпека: освіта, наука, техніка*. 2025. №3(27), С. 429–448.
7. Lakhno, V., Malyukov, V., Smirnov, O., Bebesko, B., Chubaievskiy, V., Zhumadilova, M., Malyukova, I., Smirnov, S. «Multifactorial Model for Targeted Attacks Counteracting Within the Framework of a Multi-Step Quality Game with Fuzzy Information». *8th International Symposium on Intelligent Informatics, ISI 2023*, 2025. vol 389. pp 377-389. Springer, Singapore.
8. Smirnov O., Fedorov E., Neskrodieva A., Neskrodieva T. «Intellectual Classification method of Gymnastic Elements Based on Combinations of Descriptive and Generative Approache». *CEUR Workshop Proceedings Volume 3664*, 2024, Pages 11-23.
9. Kuznetsov, O., Kryvinska, N., Ilchenko, O., Smirnova, T., Ulianovska, Y. «Comparative Analysis of Cryptocurrency Trading Platforms Using the Analytic Hierarchy Process». *CEUR Workshop Proceedings*, 2023,

- 3628, pp. 106-115.
10. Malyukov V., Bebesko B., Lakhno V., Smirnov O., Malyukova I., Mohylnyi H. «Managing the Purchase-Sale Process of Digital Currencies Under Fuzzy Conditions». *Lecture Notes in Networks and Systems*, 2023, 729 LNNS, pp. 104–112.
 11. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». *Advanced Information Systems*, 2023, 7(2), pp. 49-56.
 12. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchov, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». *CEUR Workshop Proceedings*, Volume 3530, 2023, pp. 256-265.
 13. Аль-Мудхафар Акіл Абдулхуссейн М., Смірнова Т.В., Буравченко К.О., Смірнов О.А. «Метод оцінки та підвищення користуальницького досвіду абонентів в програмно-конфігурованих мережах на основі використання машинного навчання». *Сучасні інформаційні системи*, 2023, том 7, № 2, С. 49-56.
 14. Smirnov, O., Karapetyan, A., Fedorov, E., «Creating Neural Network and Single Solution Human-Based Metaheuristic Methods of Solving the Traveling Salesman Problem». *CEUR Workshop Proceedings*, Volume 3312, 2022, pp. 47-58.
 15. Smirnov, O., Neskoriadiya, T., Fedorov, E., Rudakov, K., Neskoriadiya, A. «Method Detection Audit Data Anomalies on Basis Restricted Cauchy Machine» *CEUR Workshop Proceedings*, Volume 3187, 2022, pp. 1-12.
 16. Smirnov O., Smirnova T., Anas M. Al-Oraiqat, Drieiev O., Polishchuk L., Sheroz Khan, Yassin M. Y. Hasan, Aladdein M. Amro, Hazim S. AlRawashdeh «Method for Determining Treated Metal Surface Quality Using Computer Vision Technology». *Sensors (Basel, Switzerland)* Volume 22, Issue 16, 6223, 2022.
 17. Smirnov, O., Lakhno, V., Akhmetov, B., Chubaievskiy, V., Khorolska, K., Bebesko, B. «Selection of a Rational Composition of Information Protection Means Using a Genetic Algorithm». In: Rajakumar, G., Du, KL., Vuppapapati, C., Beligiannis, G.N. (eds) *Intelligent Communication Technologies and Virtual Mobile Networks. Lecture Notes on Data Engineering and Communications Technologies*, vol 131. 2023. Springer, Singapore. pp. 21-34.
 18. Kuznetsov, A., Oleshko, I., Chernov, K., Bagmut, M., Smirnova, T. «Biometric authentication using convolutional neural networks». *Lecture Notes in Networks and Systems*. Volume 152, 2021, Pages 85-98.
 19. Smirnov O., Kuznetsov A., Kryvinska N., Kiian A., Kuznetsova K. «Full Non-Binary Constant-Weight Codes». *SN Computer Science*, Vol 2, 337, 2021. <https://doi.org/10.1007/s42979-021-00739-w>.
 20. Smirnov O., Neskoriadiya T., Fedorov E., Rymar P. «Neural Network Modeling Method of Transformations Data of Audit Production with Returnable Waste». *CEUR Workshop Proceedings* Volume 3101, 2021, Pages 192-207.
 21. Smirnov, O., Kuznetsov, A., Potii, O., Poluyanenko, N., Stelnyk, I., Mialkovsky, D. «Combining and filtering functions in the framework of nonlinear-feedback shift register». *International Journal of Computing*; 2020, Volume 19, Issue 2 – Research Institute for Intelligent Computer Systems – 2020. – P. 247-256.
 22. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». *CEUR Workshop Proceedings*. Volume 2740, 2020, Pages 102-114.
 23. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177.
 24. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) *Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies*, vol 48. Springer, Cham. 2021. pp 557-587.
 25. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». *CEUR Workshop Proceedings* Volume 2616, 2020, Pages 366-379.
 26. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», *CEUR Workshop Proceedings* Volume 2608, 2020, Pages 633-645.
 27. Smirnov O. Kuznetsov A., Zaichenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». *International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019; Odessa; Ukraine; 9-13 September 2019*. P.22-28.
 28. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». *International Journal of Computing*; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.
 29. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019 . P.517-522.
 30. Smirnov, O., Ulichev, O., Meleshko, Y., Khokh, V., Goncharenko, I. «Method of Choosing Objects for Informational Influence in Social Networks during Information Campaign Based on the Analytic Hierarchy Process». *CEUR Workshop Proceedings*, Vol 2588, P. 215-227, 2019.

УДК 004

Є.Прокопенко, магістр гр. КІ-24М,

Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ АПАРАТНО-ПРОГРАМНИХ КОМПЛЕКСІВ ДЛЯ ВИЯВЛЕННЯ АТАК НА РІВНІ ІОТ-ПРИСТРОЇВ З ВИКОРИСТАННЯМ КВАНТОВАНИХ НЕЙРОМЕРЕЖ

У статті розроблено програмне забезпечення, яке призначено для автономного виявлення та протидії кібератакам у мережах Інтернету речей (IoT) за допомогою технологій Edge AI. Метою розробки є підвищення рівня захищеності мереж IoT шляхом розробки та реалізації апаратно-програмного комплексу виявлення вторгнень на основі адаптованих легковагих нейромереж. Об'єктом дослідження є процеси функціонування та обміну даними в мережах інтернету речей в умовах кібернетичного впливу та ресурсних обмежень апаратної платформи. Предметом дослідження є методи та апаратно-програмні засоби нейромережевого виявлення аномалій, оптимізовані для виконання на мікроконтролерах. Методи дослідження базуються на методах системного аналізу для визначення вимог до системи, теорії штучних нейронних мереж для побудови моделі класифікації трафіку, математичній статистиці та методах розробки вбудованого програмного забезпечення. Результат роботи – апаратно-програмна реалізація системи виявлення атак на базі мікроконтролера ESP32-S3 з використанням квантованих нейронних мереж. В процесі роботи над програмною моделлю виконано аналіз існуючих систем захисту IoT-інфраструктури, обґрунтовано вибір апаратної платформи з підтримкою векторних інструкцій та методів компресії моделей TinyML. В повній мірі описані всі компоненти розробленого програмного забезпечення.

виявлення та протидія кібератакам, Інтернет речей (IoT), Edge AI

Постановка проблеми. Швидке зростання кількості підключених пристроїв у глобальній мережі Інтернет речей (IoT) призводить до стрімкого збільшення векторів кібератак. Різноманітність пристроїв та використання спрощених протоколів обміну даними роблять цей сегмент вразливим до несанкціонованого втручання, що підтверджується зростанням кількості інцидентів, пов'язаних із ботнетами та DDoS-атаками [1, 2].

Для запобігання таких інцидентів необхідно захищати кінцеві вузли, які функціонують в умовах жорстких апаратних обмежень (енергоспоживання, обчислювальна потужність, обсяг пам'яті). Традиційні засоби захисту, такі як класичні системи виявлення вторгнень (IDS) або антивірусне програмне забезпечення, не можуть бути ефективно розгорнуті на мікроконтролерах через високі вимоги до ресурсів системи.

Враховуючи що перенесення функцій аналізу безпеки у хмарне середовище створює деякі затримки в реакції на інциденти та залежність від стабільності каналу зв'язку. Перспективним напрямом вирішення цієї проблеми є концепція Edge AI (граничний штучний інтелект), що передбачає виконання алгоритмів машинного навчання безпосередньо на кінцевому пристрої. Застосування оптимізованих легковагих нейронних мереж дозволяє забезпечити автономне виявлення аномалій у мережевому трафіку в реальному часі.

Таким чином, дослідження та реалізація апаратно-програмного комплексу для виявлення атак на рівні IoT-пристроїв з використанням легковагих нейромереж є актуальною науково-прикладною задачею, яка потребує вирішення у даній випускній кваліфікаційній роботі.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні дослідження та реалізація апаратно-програмних комплексів для виявлення атак на рівні IoT-пристроїв з використанням квантованих нейромереж.

Мета й завдання дослідження. Метою роботи є підвищення рівня захищеності мереж IoT шляхом розробки та реалізації апаратно-програмного комплексу виявлення вторгнень на основі адаптованих ейзеносних нейромереж.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

1. Провести огляд існуючих систем виявлення вторгнень в IoT та методів розгортання нейромереж на мікроконтролерах.
2. Обґрунтувати вибір апаратної платформи та програмних засобів для реалізації граничних обчислень.
3. Розробити структурну та функціональну схеми комплексу виявлення атак на базі вибраного мікроконтролера.
4. Здійснити програмну реалізацію модуля інференсу нейронної мережі з використанням векторних інструкцій для аналізу трафіку в реальному часі.
5. Провести експериментальне дослідження ефективності розробленого комплексу при виявленні типових мережевих атак.

Виклад основного матеріалу. Ініціалізація комплексу та конфігурація пам'яті

Прийнятому запуску система ініціює виконання завантажувача другого рівня. Для цього важливим етапом ініціалізації є розгортання карти пам'яті відповідно до попередньо визначеної таблиці розділів. Це потрібно задля стабільності роботи нейромережі та можливості оновлення прошивки «по повітрю». Нами була використана схема розмітки Flash-пам'яті на 4 мегабайти яка наведена в таблиці 1.

Таблиця 1 – Розподіл простору Flash-пам'яті

Тип	Підтип	Зсув	Розмір	Призначення
data	nvs	0x9000	20 КБ	Енергонезалежне сховище налаштувань
data	phy_init	0xe000	4 КБ	Калібрувальні дані радіомодуля
app	factory	0x10000	1.5 МБ	Основний образ прошивки
app	ota_0	0x180000	1.5 МБ	Слот для оновлення прошивки
data	coredump	0x300000	64 КБ	Збереження дампу пам'яті при критичних збоях

Після монтування файлової системи виконується налаштування таймерів для забезпечення відмовостійкості. Враховуючи високе навантаження на процесор під час роботи нейромережі нами було запроваджено таку систему контролю:

1. Interrupt Watchdog – це апаратний таймер, що гарантує перемикання контексту переривань. Тайм-аут встановлено на рівні 300 мс для запобігання блокуванню системи драйвером Wi-Fi.

2. Task Watchdog – являє собою програмний механізм FreeRTOS, що відстежує стан задач. Задача нейромережевого аналізу повинна періодично скидати таймер, підтверджуючи нормальне функціонування алгоритму [29].

Далі відбувається переміщення статичного буфера Tensor Arena у зовнішній модуль PSRAM. Таким чином використання зовнішньої пам'яті через високошвидкісний інтерфейс

Octal SPI дозволяє виділити неперервний блок розміром до 2 МБ для зберігання вхідних, вихідних та проміжних тензорів, що унеможливорює помилки викликані розподілом ресурсів під час роботи системи.

Після ініціалізації стека TCP/IP та встановлення захищеного з'єднання з MQTT-брокером, радіомодуль переводиться у режим прослуховування.

Цикл збору даних та структура кадрів

Механізм щодобору даних реалізований нами на механіки зворотних викликів, що спрацьовують при виявленні підходящого фрейму стандарту IEEE 802.11. Функція обробки `promiscuous_rx_cb` отримує доступ до сирого пакету, структура якого відповідає стандарту 802.11 MAC Header загальною довжиною 24 байти (без врахування поля QoS Control).

Ключові поля заголовка, що підлягають аналізу:

— Frame Control (2 байти): містить ідентифікатори версії протоколу, типу (Management, Control, Data) та підтипу (Beacon, Probe Request, Deauthentication) кадру. Також включає прапори ToDS та FromDS, що визначають напрямок руху пакету відносно точки доступу.

— Duration/ID (2 байти): визначає час, на який середовище передачі буде зайнято. Аномально великі значення в цьому полі можуть свідчити про спробу атаки «Virtual Jamming» (Nav Attack).

— Address Fields (6 байт x 3): MAC-адреси приймача (DA), передавача (SA) та точки доступу (BSSID).

Для буферизації потоку даних було створено структуру кільцевого буфера фіксованої ємності N . Керування доступом здійснюється за допомогою двох індексів з яких Head (голова) для запису нових даних та Tail (хвіст) для читання нейромережовим модулем. Розрахунок індексу для запису наступного елемента розраховується за формулою:

$$Index_{next} = (Index_{current} + 1) \bmod N \quad (1)$$

Для запобігання пошкодженню даних, що знаходяться в процесі аналізу, застосовано стратегію «Drop on Full». У випадку, коли буфер заповнений (умова $(Head + 1) \bmod N == Tail$), нові пакети ігноруються до моменту звільнення місця задачею аналізу. Це гарантує цілісність часового вікна, яке вже сформовано та передано на вхід нейромережі.

Нейромережовий аналіз

Основною логікою виявлення аномалій являється обробка вектора ознак, сформованих з сирих даних буфера. Цей процес називається розрахунком інженерії ознак яка передбачає перетворення статистичних характеристик трафіку в числовий вектор V .

Для детектування складних атак обчислюються наступні метрики: ентропія Шеннона, середньоквадратичне відхилення інтервалів прибуття, співвідношення керуючих кадрів

$$\left(\begin{matrix} R_{mgmt} \\ \end{matrix} \right).$$

Використання ентропії Шеннона щодо розмірів пакетів потрібна для виявлення тунелювання даних або аномального розподілу навантаження.

$$H(X) = - \sum_{i=1}^n P(x_i) \log_2 P(x_i) \quad (2)$$

де $P(x_i)$ - ймовірність появи пакету розміром x_i у поточному вікні. Низька ентропія характерна для DDoS-атак, висока - для нормального трафіку.

Середньоквадратичне відхилення інтервалів прибуття дозволяє виявити автоматизовані інструменти сканування, які генерують пакети з фіксованою періодичністю, на відміну від стохастичної природи людської активності.

Співвідношення керуючих кадрів це частка кадрів управління до загальної їх

кількості. Різке зростання R_{mgmt} свідчить про атаки типу Deauthentication Flood.

Перед подачею на вхідний шар нейромережі вектор ознак підлягає квантуванню. Оскільки модель TensorFlow Lite оптимізована для цілочисельних обчислень (int8), дійсні значення ознак x_{float} (формат float32) перетворюються у цілі числа x_{quant} за формулою афінного квантування:

$$x_{quant} = clamp \left(\left\lfloor \frac{x_{float}}{S} \right\rfloor + Z, -128, 127 \right), \quad (3)$$

де S (Scale) - масштабний коефіцієнт, Z (Zero-point) - зміщення нуля, визначені на етапі навчання моделі. Операція clamp обмежує значення діапазоном 8-бітного знакового цілого. Такий підхід зменшує вимоги до пам'яті для зберігання ваг моделі з 4 байт до 1 байта на параметр, що є необхідним для обмеженої кількості ресурсів до будь якого мікроконтролера [30].

Механізм реагування на інциденти

Логіка прийняття рішень та керування режимами роботи системи реалізована у вигляді скінченного автомата. Визначено наступні стани системи:

- STATE_IDLE: початкова ініціалізація, очікування підключення до Wi-Fi/MQTT.
- STATE_MONITOR: пасивне накопичення даних у кільцевий буфер.
- STATE_ANALYSIS: активна фаза інференсу нейромережі.
- STATE_ALERT: формування та відправка сповіщення про загрозу.
- STATE_ISOLATION: виконання активних контрзаходів (блокування).

Перехід у стан STATE_ALERT відбувається за умови, що ймовірність атаки $P(\text{Attack})$, розрахована нейромережею, перевищує порогове значення Threshold. Для запобігання перевантаженню каналу зв'язку та перенасичення одноманітними повідомленнями впроваджено алгоритм.

Алгоритм обмежує частоту відправки повідомлень про один і той самий тип атаки. Нове повідомлення генерується лише за умови виконання нерівності:

$$t_{current} - t_{lastalert} > \Delta T_{cooldown}, \quad (4)$$

де $\Delta T_{cooldown}$ — період «охолодження» (наприклад, 5000 мс). Якщо атака триває, система лише інкрементує лічильник інцидентів у локальному лозі, але не ініціює нову транзакцію MQTT, доки не спливе час затримки.

У стані STATE_ISOLATION система може відправляти спеціально сформовані пакети (наприклад, Channel Switch Announcement) для міграції пристроїв на інший частотний канал, ізолюючи їх від джерела перешкод.

Архітектура системи декомпозована на функціональні рівні, що забезпечують збір, первинну обробку, аналіз та передачу інформації.

Обґрунтування топології мережі

Мережева архітектура реалізована за топологією типу «Зірка». Роль центрального концентратора та арбітра безпеки виконує інтелектуальний шлюз. Зовнішні вузли (сенсори, актуатори) функціонують як клієнти, трафік яких підлягає моніторингу та аналізу.

Застосування топології згаданої вище обумовлено необхідністю мінімізації часових затримок при передачі тривожних сповіщень. На відміну від децентралізованих мереж, де маршрутизація пакетів здійснюється через ланцюжок проміжних вузлів, централізована схема виключає затримки при ретрансляції. Такий підхід є необхідним для системи виявлення вторгнень, де час реакції на атаку має складати мілісекунди.

Фізичним середовищем для передачі даних є радіоканал стандарту IEEE 802.11n (Wi-Fi) у діапазоні 2.4 ГГц.

Апаратна реалізація центрального вузла

Основою обчислювального ядра є високоефективна система ESP32-S3-WROOM-1-N16R8. Архітектура мікроконтролера включає два 32-розрядних процесори Xtensa LX7, що

працюють на тактовій частоті 240 МГц. Вибір даної платформи обумовлений наявністю розширеного набору векторних інструкцій, що забезпечують апаратне прискорення операцій матричного множення та згортки, які складають основу обчислювального навантаження згорткових нейронних мереж.

Підсистема пам'яті та інтерфейс Octal SPI

Критичною особливістю обраної модифікації модуля (N16R8) є розширена підсистема пам'яті, що включає:

1. Flash-пам'ять складає 16 МБ і підключена через інтерфейс Quad SPI. Вона використовується для зберігання прошивки, файлової системи LittleFS та статичних вагових коефіцієнтів нейромережі.

2. Оперативна пам'ять (зокрема PSRAM) складає 8 МБ і підключена через високошвидкісний інтерфейс Octal SPI (надалі OPI).

Використання OPI PSRAM є визначальним проектним рішенням. На відміну від стандартної внутрішньої SRAM (512 КБ), якої недостатньо для розміщення складних моделей глибокого навчання, зовнішня пам'ять дозволяє виділити значний обсяг адресного простору під Tensor Arena - безперервну ділянку пам'яті для зберігання вхідних/вихідних тензорів та проміжних результатів активації нейронів. Інтерфейс OPI забезпечує передачу даних по 8 лініях за один такт, що гарантує високу пропускну здатність шини, необхідну для динамічного завантаження шарів моделі без суттєвих затримок інференсу.

Додатково, наявність 8 МБ оперативної пам'яті дозволяє реалізувати глибокий кільцевий буфер (Ring Buffer) для захоплення мережевих пакетів. Це забезпечує режим моніторингу Zero-drop sniffing, нівелюючи ризик втрати пакетів під час пікових навантажень на центральний процесор при обробці результатів нейромережі.

Зовнішні інтерфейси та підсистема реєстрації

Для забезпечення автономності функціонування та реалізації режиму «Чорної скриньки», структурна схема передбачає підключення зовнішнього накопичувача – карти пам'яті MicroSD. Обмін даними реалізовано через апаратний інтерфейс SPI (режим VSPI). Накопичувач використовується для ведення журналів подій безпеки та збереження дамів аномального трафіку для подальшого криміналістичного аналізу.

Комунікація із зовнішнім світом здійснюється через вбудований радіомодуль Wi-Fi, який підтримує роботу в режимі прослуховування. Цей режим потрібен для захоплення кадрів каналного рівня без підключення до конкретної точки доступу. Передача телеметрії на сервер здійснюється через захищений канал MQTTS.

Структурна схема комплексу

Графічне представлення архітектури системи, що ілюструє логічні зв'язки та високошвидкісні інтерфейси обміну даними між основними функціональними блоками, наведено на рисунку 1.

Запропонована схема, завдяки використанню розширеної пам'яті OPI PSRAM, забезпечує необхідний апаратний ресурс для розгортання повноцінних моделей глибокого навчання на периферійному пристрої, зберігаючи при цьому стабільність роботи в режимі реального часу.

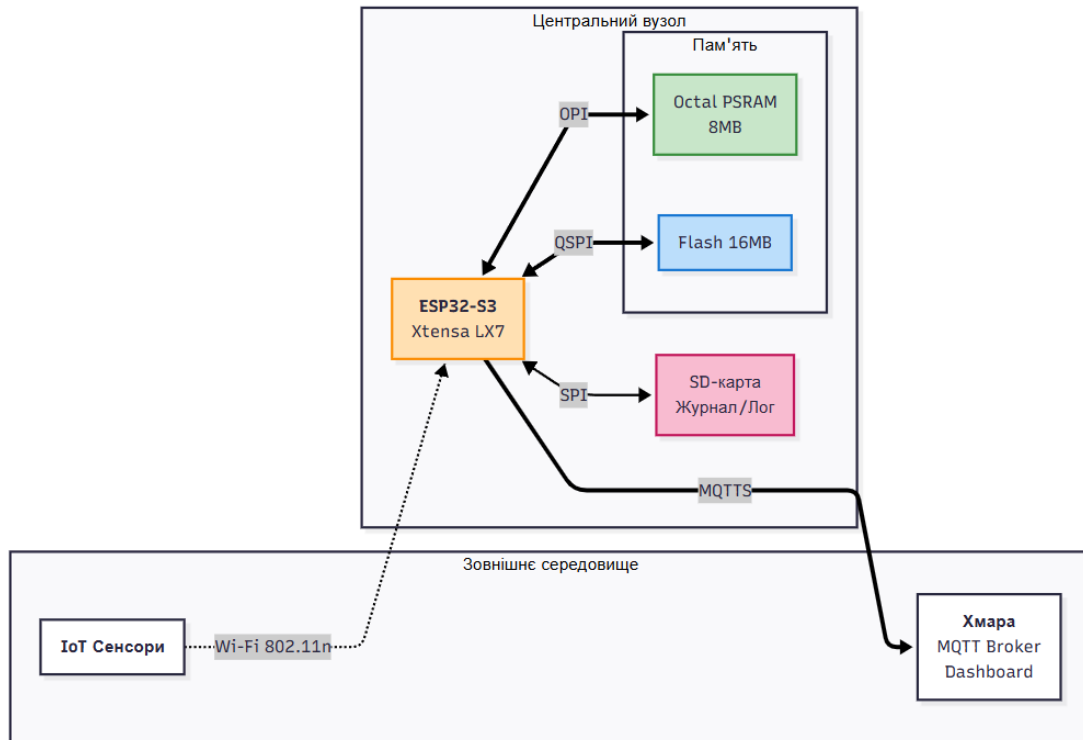


Рисунок 1 – Структурна схема апаратно-програмного комплексу

Висновки. У статті наведено теоретичне узагальнення та розв’язання науково-технічного завдання щодо впровадження легковажних нейронних мереж у вбудовані системи. Досягнення поставленої мети базувалося на послідовному виконанні таких етапів:

— Проведено аналітичний огляд існуючих систем виявлення вторгнень та архітектурних рішень для інтернету речей.

— Досліджено методи оптимізації нейромережових моделей TinyML для роботи в умовах обмежених апаратних ресурсів мікроконтролерів.

— На основі отриманих результатів створено програмну реалізацію комплексу детекції аномалій трафіку безпосередньо на периферійному вузлі.

Розроблені алгоритми інференсу, адаптовані під векторні інструкції архітектури Xtensa LX7, дозволяють успішно вирішувати завдання ідентифікації кіберзагроз у реальному часі з мінімальною латентністю. У ході аналізу предметної галузі було ідентифіковано ключові об’єкти взаємодії, визначено їхні функціональні характеристики та побудовано математичну модель детектора атак.

Список літератури

1. Kuznetsov O., Frontoni E., Kuznetsova Y., Chevardin V., Smirnov O. «Architectural foundations for adaptive security in edge computing systems». Cybersecurity Defensive Walls in Edge Computing, 2025. pp. 21-61.
2. Вінтенко, Б.Ю., Миронець, І.В., Смірнов, О.А., Коваленко, О.В., Усік, П.С., Буравченко, К.О., Лисенко, І.А. «Логіко-структурна модель комп’ютерно-орієнтованої процедури системи підтримки оперативного персоналу АЕС». Кібербезпека: освіта, наука, техніка. 2025. Том 2 № 30. С. 413-427, 2025.
3. Смірнова, Т.В. «Дослідження методів, моделей та сучасних ІТ-рішень для підтримки технологічних процесів у критичній інфраструктурі держави». Кібербезпека: освіта, наука, техніка. 2025. Том 2 № 30. С.195-208, 2025.
4. Kuznetsov, O., Frontoni, E., Kuznetsova, K., Arnesano, M., Smirnov, O. «A secure biometric authentication architecture for blockchain-driven cyber-physical systems». Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications, 2025, pp. 193–224.
5. Kuznetsov, O., Atzeni, G., Arnesano, M., Randieri, C., Smirnov, O. «Secure IoT-based smart wheelchair system: From implementation to security enhancement strategy». Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications, 2025, pp. 225–257.

6. Kuznetsov, O., Smirnov, O., Kuznetsova, T., Shaikhanova, A., Svatowsky, I. «Privacy-utility trade-offs in IoT networks: A comparative analysis of differential privacy mechanisms for sensor data aggregation». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 589–622.
7. Вінтенко Б., Смірнов О., Миронець І., Смірнова Т., Смірнов С. «Імітаційна модель шляхів вхідних даних комп'ютерної інтелектуальної системи підтримки оператора енергоблоку АЕС». Комбінаторні конфігурації та їхні застосування: Матеріали XXVII Міжнародного науково-практичного семінару, присвяченого 125-річчю Національного університету «Запорізька політехніка» (Запоріжжя-Кропивницький-Київ, 4-6 червня 2025 р.). Запоріжжя: НУ «Запорізька політехніка», 2025. С.82-91.
8. Al-Azzeh, J., Ayyoub, B., Mesleh, A., Smirnova, T., Gnatyuk, S., Drieiev, O., Smirnov, O., Dorenskyi, O. «Cloud-Based Information System for Evaluating Caverns in the Process of Blasting Metal Surfaces of Details». *International Review on Modelling and Simulations* 18 (1), 2025. pp. 32-42.
9. Вінтенко Б.Ю., Смірнов О.А., Миронець І.В., Смірнова Т.В., Коваленко О.В., Мацуй А.М. «Модель шляхів отримання вхідних даних комп'ютерної інтелектуальної системи підтримки оперативного персоналу АЕС». *Центральноукраїнський науковий вісник. Технічні науки*. 2025. Вип. 11(42), ч. II. С.52-62.
10. Вінтенко Б.Ю., Смірнов О.А., Миронець І.В., Смірнова Т.В. «Методи забезпечення відмовостійкості інтелектуальних систем підтримки оператора». VIII міжнародна науково-практична конференція «Інформаційна безпека та комп'ютерні технології», м. Кропивницький. 24-25 квітня 2025 р. – Кропивницький: ЦНТУ. – 2025. – С. 44-46.
11. Вінтенко, Б., Миронець, І., Смірнов, О., Коваленко, А., Коноплицька-Слободенюк, О., Смірнова, Т., Константинова, Л. «Дослідження застосування систем підтримки оперативного персоналу об'єкту критичної інфраструктури при керуванні енергоблоком АЕС з реактором типу ВВЕР-1000». *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2024. № 2(26), С. 6-26.
12. Смірнова Т.В., Коноплицька-Слободенюк О.К., Буравченко К.О., Смірнов С.А., Кравчук О.В., Козірова Н.Л., Смірнов О.А. «Дослідження технологій забезпечення кібербезпеки хмарних сервісів IaaS, PaaS та SaaS». *Кібербезпека: освіта, наука, техніка*. 2024. №4(24), С. 6-27.
13. Вінтенко, Б., Миронець, І., Смірнов, О., Кравчук, О., Козірова, Н., Савеленко, Г., Коваленко, А. «Дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». *Кібербезпека: освіта, наука, техніка*. 2024. №3(23), С. 111-131.
14. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». *Advanced Information Systems*, 2023, 7(2), pp. 49-56.
15. Kuznetsov, O., Kuznetsova, Y., Smirnov, O., Kostenko, O., Zvieriev, V. «Evaluating Hashing Algorithms in the Age of ASIC Resistance». *CEUR Workshop Proceedings*, 2023, 3628, pp. 93-105.
16. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchey, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». *CEUR Workshop Proceedings*, Volume 3530, 2023, pp. 256-265.
17. Smirnov, O., Odarchenko, R., Smirnova, T., Bondar, S., Volosheniuk, D. «Optimal Structure Construction of Private 5G Network for the Needs of Enterprises». *Lecture Notes on Data Engineering and Communications Technologies*, 2023, 178, pp. 208–223.
18. Вінтенко Б.Ю., Смірнов О.А., Коваленко А.С., Смірнов С.А., Буравченко К.О. «Дослідження вимог міжнародних стандартів IEC60880 та IEC62138 з розробки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». *Системи управління, навігації та зв'язку*, 2023, вип. 3(73), С. 155-166.
19. Аль-Мудхафар Акіл Абдулхуссейн М., Смірнова Т.В., Буравченко К.О., Смірнов О.А. «Метод оцінки та підвищення користувальницького досвіду абонентів в програмно-конфігурованих мережах на основі використання машинного навчання». *Сучасні інформаційні системи*, 2023, том 7, № 2, С. 49-56.
20. Smirnova, T., Gnatyuk, S., Yudin, O., Sydorenko, V., Polozhentsev, A., «The Model for Calculating the Quantitative Criteria for Assessing the Security Level of Information and Telecommunication Systems». *CEUR Workshop Proceedings Volume 3156*, 2022, Pages 390-399.
21. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». *Проблеми інформатизації та управління*, № 2(70). 2022. С. 28-37.
22. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції ґешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» *Системи управління, навігації та зв'язку*, 2022, № 3(69). С. 93-98.
23. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції ґешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» *Вісник Хмельницького національного університету. Серія: «Технічні науки»*, № 2 (307). С. 46-52. 2022.
24. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції ґешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» *Системи управління, навігації та зв'язку*, 2022, № 1(67).

C. 84-89.

25. Smirnova T., Gnatyuk S., Berdibayev R., Avkurova Zh., Iavich M. «Cloud-Based Cyber Incidents Response System and Software Tools». Communications in Computer and Information Science, 2021, vol 1486. Springer, Cham. pp 169-184.
26. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
27. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». Journal of theoretical and applied information technology Vol.98. No 21, 2020, P. 3334-3346.
28. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177.
29. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587.
30. Smirnov, O., Markovets, O. Vovk, N., Turchyn, Y., «Model of informational support for social network administrators' content creation». CEUR Workshop Proceedings Volume 2616, 2020, Pages 125-136.

УДК 004

Д.Радін, магістр гр. КІ-24М,

Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ АПАРАТНО-ПРОГРАМНИХ ЗАСОБІВ ОТРИМАННЯ ФОТОЗОБРАЖЕННЯ, ЙОГО СТИЛІЗАЦІЇ ТА ВІДТВОРЕННЯ ЗА ДОПОМОГОЮ РЕАЛІЗАЦІЇ ПРИСТРОЮ ІОТ ПЛОТТЕРУ

У статті розроблено програмне забезпечення, яке призначено системи отримання фотозображення, його стилізації та відтворення за допомогою пристрою ІоТ плоттеру. Метою роботи є отримання та відтворення попередньо стилізованого фотографічного зображення з використанням можливостей ІоТ на плотері. Об'єкт дослідження є процес стилізації растрового зображення, перетворення його у векторну графіку й відтворення пристроєм. Предмет дослідження є методи, програмні засоби й алгоритми отримання, стилізації та векторизації зображення. Методи дослідження базуються на методах системного аналізу, методи цифрової обробки зображень та алгоритми машинного навчання. Результат роботи – програмна реалізація отримання та відтворення попередньо стилізованого фотографічного зображення з використанням можливостей ІоТ на плотері. У процесі проектування програмної моделі проведено аналіз сучасних апаратних рішень та програмних засобів для керування плоттером.

ІоТ плоттер

Постановка проблеми. Стрімкий розвиток інформаційних технологій, зокрема штучного інтелекту, суттєво вплинув на різні галузі. Паралельно продовжує активно розвиватися Інтернет речей, який охоплює мільярди фізичних пристроїв та розширює сфери свого застосування. Поєднання двох цих напрямів стало відоме як Інтелект речей (AIoT).

Поява генеративних моделей, зробила можливою трансформацію зображень в різноманітні стилі. Однак більшість існуючих рішень реалізують або програмну обробку зображень або їх відтворення.

Проблема полягає у відсутності повноцінних систем, які поєднували отримання зображення, його подальшу обробку та відтворення пристроєм.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні дослідження та реалізація апаратно-програмних засобів отримання фотозображення, його стилізації та відтворення за допомогою реалізації пристрою ІОТ плоттеру.

Мета й завдання дослідження. Метою роботи є отримання та відтворення попередньо стилізованого фотографічного зображення з використанням можливостей ІоТ на плотері.

Для досягнення мети було поставлено такі завдання:

- провести огляд існуючих методів векторизації растрових зображень;
- порівняти існуючі моделі стилізації зображень на базі архітектури Stable Diffusion;
- програмно реалізувати захоплення та передачу зображення, стилізацію, подальше перетворення у дані придатні для відображення плоттером.

Об'єкт дослідження. Процес стилізації растрового зображення, перетворення його у векторну графіку й відтворення пристроєм.

Предмет дослідження. Методи, програмні засоби й алгоритми отримання, стилізації та векторизації зображення.

Методи дослідження. Застосовуються наступні методи, а саме: методи системного аналізу, методи цифрової обробки зображень та алгоритми машинного навчання.

Виклад основного матеріалу. Функціонування запропонованої системи представляє собою циклічний конвеєр обробки даних, який об'єднує методи отримання первинної візуальної інформації, її візуальну трансформацію та механічне відтворення. Загальний алгоритм роботи системи розділено на чотири етапи:

- Захоплення зображення.
- Стилзація зображення.
- Векторизація.
- Відображення.

На першому етапі ми здійснюємо ініціалізацію модуля камери. Вона, функціонуючи як окремий вузол, виконує захоплення растрового зображення. Ми можемо звертатися до вбудованої камери обчислювальної станції або зовнішньої USB-периферії через системні драйвери та інтерфейси API засобами бібліотеки OpenCV.

Другий етап полягає в обробці отриманого кадру неймережами. Програмне забезпечення сервера, реалізоване мовою Python, відправляє отримані дані до API Automatic1111. На цьому етапі ми використовуємо модель Stable Diffusion 1.5 у поєднанні з додатковими модулями керованої генерації:

- ControlNet.
- LoRA-моделі.

LoRA-моделі фокусують генерацію на отриманні специфічного стилю “Line Art”, що важливо для роботи плотера, тому що вихідне зображення виходить з чіткими лініями та мінімальною кількістю шумів, які легше відобразити.

На третьому етапі виконуємо постобробку згенерованого стилізованого зображення. За допомогою бібліотеки OpenCV здійснюється бінаризація та фільтрація дефектів. Отриманий растр піддається алгоритму векторизації, що перетворює масив пікселів у набір ліній та кривих. В результаті формується файл з розширенням .gcode, який містить послідовність команд для переміщення пера плоттера у тривимірному просторі.

На фінальному етапі ми передаємо згенеровані команди на контролер плоттера. Контролер інтерпретує G-код, керує кроковими двигунами для точного фізичного відтворення стилізованого малюнка на носії.

Структурної схема вказує взаємозв'язки між компонентами, розподіл обчислювального навантаження та протоколи інформаційного обміну. Відповідно до поставленого завдання, архітектура системи побудована за модульним принципом, для стабільності передачі даних між різнорідними середовищами. Структурна схема системи зображена на малюнку 1. Розглянемо детальніше її елементи.

Блок отримання візуальних даних

Здійснює роль сенсорного входу системи. Схема передбачає універсальність інтерфейсу підключення. Це дозволить нам використовувати як автономні IoT-модулі, наприклад, ESP32-CAM, так і стаціонарні пристрої відеозахоплення, як інтегровані камери. Єдине завдання цього блоку – це формувати стабільний кадровий потік або знімків та їх передача у центральний вузол обробки. Відео транслюється одразу в оперативну пам'ять керуючого комп'ютера, мінаючи проміжні буфери. Через це ми зможемо мати можливість інтерактивно змінювати композицію кадру, параметри експозиції та позицію об'єкта ще до моменту фіксації зображення, нівелює вірогідність отримання некоректних вхідних даних. Вихідними даними блоку буде растрове зображення у форматі високої чіткості для подальшої стилізації.

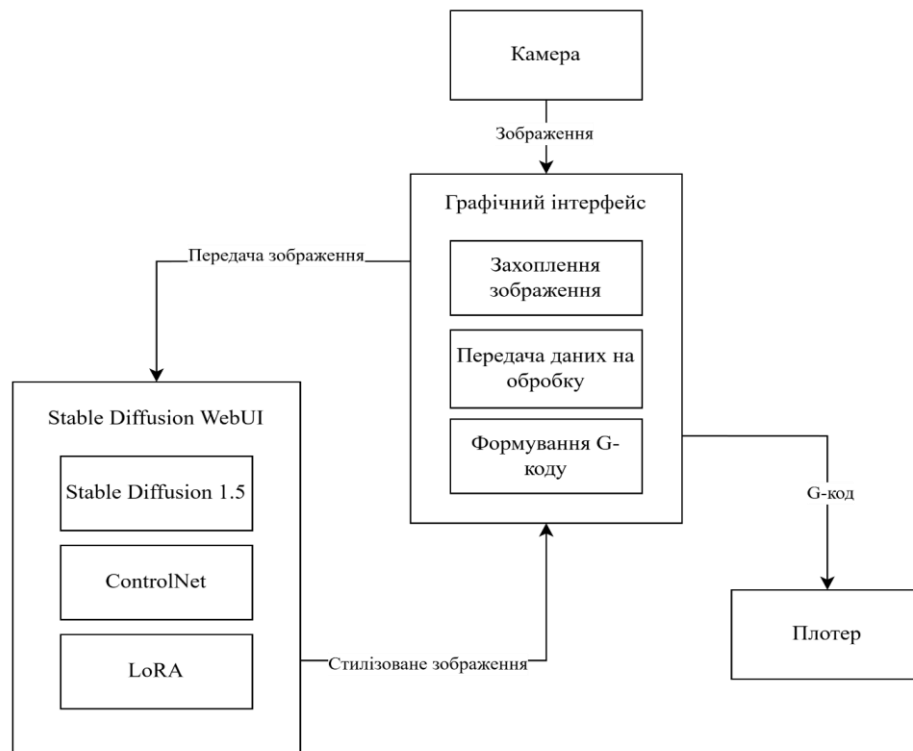


Рисунок 1 – Структурна схема системи

Графічний інтерфейс

Посідає центральне місце у структурній ієрархії. Це вузол графічного інтерфейсу та керування, який виступає архітектурним ядром системи. Якщо традиційні клієнтські додатки виконують лише роль терміналу введення-виведення, то даний вузол – це повноцінний оркестратор асинхронних процесів. Внутрішня логіка керуючого вузла включає підсистему попередньої обробки відеосигналу, модуль векторизації та драйвер комунікації з периферійними пристроями. Тобто цей блок керує:

- Захопленням зображення.
- Передача даних на обробку.
- Формування G-коду.

Таким рішенням ми можемо інкапсулювати складність керування різномірним обладнанням всередині однієї програми, надаючи користувачу інтуїтивно зрозумілий інтерфейс високого рівня абстракції. Через реалізацію багатопотокової моделі обчислень, керуючий вузол гарантує швидкодію інтерфейсу навіть під час тривалих операцій.

Модуль інтелектуальної трансформації

Цей блок винесено в окремий блок через високу обчислювальну складність операцій. Крім того така архітектура дозволяє нам розвантажити основний потік виконання та забезпечити масштабованість системи. Він представляє собою серверне середовище, де відбувається дифузійна обробка зображення.

Внутрішня архітектура блока складається з трьох інтегрованих рівнів. Найголовніший рівень – це базова генеративна модель Stable Diffusion 1.5, яка відповідає за формування загальної текстури та композиції на основі ймовірнісної дифузії. Для адаптації цієї моделі до задач інженерної графіки застосовано адаптер ControlNet. Додатково застосовується стилізаційний модуль LoRA, що застосовує специфічний художній стиль для моделі без повної модифікації ваг нейромережі.

Плотер

Останній блок структурної схеми, для фізичного втілення початкового растрового зображення. Вхідні дані для цього блоку – це послідовність команд G-коду. Плотер має у собі мікроконтролер керування двигунами, драйвери силової частини та безпосередньо

механіку. Має архітектурною особливість. Це наявність буфера команд із функцією попереднього перегляду. Це дозволяє нам згладити надходження даних та забезпечити неперервність руху інструменту. Результатом функціонування цього блоку є точне відтворення графічних ліній на фізичному носії.

Висновки. У статті наведено теоретичне узагальнення та розв'язання науково-технічного завдання щодо інтеграції нейромережових алгоритмів обробки зображень у системи числового програмного керування (ЧПК). Досягнення поставленої мети базувалося на послідовному виконанні таких етапів:

- Проведено аналітичний огляд існуючих методів векторизації растрових зображень та архітектурних рішень для CNC-систем;
- Досліджено методи оптимізації генеративних моделей Stable Diffusion за допомогою адаптерів ControlNet для збереження геометричної точності контурів;
- На основі отриманих результатів створено програмну реалізацію комплексу стилізації та векторизації зображень безпосередньо на керуючому вузлі (Host-системі);
- Розроблені алгоритми спірального пошуку та спрощення ламаних, адаптовані під специфіку плотерів, дозволяють успішно вирішувати завдання перетворення піксельних масивів у векторні траєкторії з мінімальною кількістю холостих ходів.

У ході аналізу предметної галузі було ідентифіковано ключові об'єкти взаємодії, визначено їхні функціональні характеристики та побудовано математичну модель перетворення графічної інформації.

Список літератури

1. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». Advanced Information Systems, 2023, 7(2), pp. 49-56.
2. Kuznetsov, O., Kuznetsova, Y., Smirnov, O., Kostenko, O., Zvieriev, V. «Evaluating Hashing Algorithms in the Age of ASIC Resistance». CEUR Workshop Proceedings, 2023, 3628, pp. 93-105.
3. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchey, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». CEUR Workshop Proceedings, Volume 3530, 2023, pp. 256-265.
4. Smirnov, O., Odarchenko, R., Smirnova, T., Bondar, S., Volosheniuk, D. «Optimal Structure Construction of Private 5G Network for the Needs of Enterprises». Lecture Notes on Data Engineering and Communications Technologies, 2023, 178, pp. 208–223.
5. Вінтенко Б.Ю., Смірнов О.А., Коваленко А.С., Смірнов С.А., Буравченко К.О. «Дослідження вимог міжнародних стандартів IEC60880 та IEC62138 з розробки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». Системи управління, навігації та зв'язку, 2023, вип. 3(73), С. 155-166.
6. Аль-Мудхафар Акіл Абдулхуссейн М., Смірнова Т.В., Буравченко К.О., Смірнов О.А. «Метод оцінки та підвищення користувальницького досвіду абонентів в програмно-конфігурованих мережах на основі використання машинного навчання». Сучасні інформаційні системи, 2023, том 7, № 2, С. 49-56.
7. Smirnova, T., Gnatyuk, S., Yudin, O., Sydorenko, V., Polozhentsev, A., «The Model for Calculating the Quantitative Criteria for Assessing the Security Level of Information and Telecommunication Systems». CEUR Workshop Proceedings Volume 3156, 2022, Pages 390-399.
8. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». Проблеми інформатизації та управління, № 2(70). 2022. С. 28-37.
9. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 3(69). С. 93-98.
10. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Вісник Хмельницького національного університету. Серія: «Технічні науки», № 2 (307). С. 46-52. 2022.
11. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 1(67). С. 84-89.

12. Smirnova T., Gnatyuk S., Berdibayev R., Avkurova Zh., Iavich M. «Cloud-Based Cyber Incidents Response System and Software Tools». *Communications in Computer and Information Science*, 2021, vol 1486. Springer, Cham. pp 169-184.
13. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». *CEUR Workshop Proceedings*. Volume 2740, 2020, Pages 102-114.
14. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». *Journal of theoretical and applied information technology* Vol.98. No 21, 2020, P. 3334-3346.
15. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177.
16. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) *Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies*, vol 48. Springer, Cham. 2021. pp 557-587.
17. Smirnov, O., Markovets, O. Vovk, N., Turchyn, Y., «Model of informational support for social network administrators' content creation». *CEUR Workshop Proceedings Volume 2616*, 2020, Pages 125-136.
18. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». *CEUR Workshop Proceedings Volume 2616*, 2020, Pages 366-379.
19. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», *CEUR Workshop Proceedings Volume 2608*, 2020, Pages 633-645.
20. Smirnov O. Kuznetsov A., Zaichenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». *International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019; Odessa; Ukraine; 9-13 September 2019*. P.22-28.
21. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». *International Journal of Computing*; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.
22. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019 . P.517-522.
23. Smirnov, O., Odarchenko, R., Abakumova, A., Usik, P., Kundyz, M., «QoE optimization technique for media delivery in 5G networks». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019. P.597-601.
24. Smirnov, O., Krasnobayev, V., Yanko, A., Kuznetsova, T. «Methods of nulling numbers in the system of residual classes». *CEUR Workshop Proceedings*, Vol 2588, P. 90-106, 2019.
25. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Averchev, A., Pastukhov, M., Kuznetsova, K., «Formation of Pseudorandom Sequences with Special Correlation Properties», 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT -2019/ Lviv, Ukraine, 2-6 July, 2019, P. 395-399.
26. Smirnov, O., Kuznetsov, A., Kiian, A., Zamula, A., Rudenko, S., Hryhorenko, V., «Variance Analysis of Networks Traffic for Intrusion Detection in Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 353-358.
27. Smirnov, O., Kuznetsov, A., Kavun, S., Babenko, B., Nakisko, O., Kuznetsova, K., «Malware Correlation Monitoring in Computer Networks of Promising Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 347-352.
28. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Pastukhov, M., Kuznetsova, K., Prokopovych-Tkachenko, D., «Discrete Signals with Special Correlation Properties», *CEUR Workshop Proceedings Volume 2353*, *CEUR Workshop Proceedings 2019*, Pages 618-629.
29. Smirnov A.A., Kuznetsov A.A., Danilenko D.A., Berezovsky A., «The statistical analysis of a network traffic for the intrusion detection and prevention systems», *Telecommunications and Radio Engineering*. – Volume 74, Issue 1. – Beggel House Inc. – 2015. – P. 61-78.
30. Смірнов О.А., Смірнова Т.В., Буравченко К.О., Кравченко С.С., Горбов В.О., «Хмарна система підтримки прийняття рішень технологічного процесу відновлення поверхонь конструкцій і деталей машин». *Сучасні інформаційні системи*. 2021. Т. 5, № 4. С. 79-95

УДК 004

М.Рисований, магістр гр. КІ-24М,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ПОБУДОВИ ПРОГРАМУЄМОЇ МЕРЕЖІ SDN НА БАЗІ SD-WAN

У статті розроблено програмне забезпечення, яке призначено для системи побудови програмуємої мережі SDN на базі SD-WAN. Метою розробки є дослідження та принципи побудови системи побудови програмуємої мережі SDN на базі SD-WAN. Об'єктом дослідження є процес побудови програмуємої мережі SDN на базі SD-WAN. Предметом дослідження є методи побудови програмуємої мережі SDN на базі SD-WAN. Методи дослідження базуються на методах теорії побудови комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи побудови програмуємої мережі SDN на базі SD-WAN. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

SDN, SD-WAN

Постановка проблеми. Перехід до програмувальних мереж SDN останні п'ять років перебуває у фокусі уваги основних постачальників і замовників продуктів для мережних інфраструктур, поки ця технологія більш-менш активно використовується тільки в одному сегменті – у мережах центрів обробки даних.

Програмно-конфігуруєма мережа (SDN від англ. Software-defined Networking, також програмно-визначаєма мережа) – мережа передачі даних, у якій рівень керування мережею відділений від пристроїв передачі даних і реалізується програмно, одна з форм віртуалізації обчислювальних ресурсів.

Давайте розшифруємо це визначення. Якщо розглянути сучасний мережний пристрій (роутер або комутатор, не принципово), то він логічно складається із трьох компонентів.

1. Рівень керування – це CLI, убудований веб-сервер або API і протоколи керування. Завдання цього рівня забезпечити керуваність пристроєм.

2. Рівень керування трафіком – це різні алгоритми й функціонал завданням якого є автоматична реакція на зміни трафіку тобто інтелект пристрою.

3. Передача трафіку – функціонал який забезпечує фізичну передачу даних, рівень мікросхем і мережних пакетів.

Що якщо:

– централізувати керування трафіком, відокремивши керування від пристроїв?

– централізувати керування пристроями?

У результаті «новий» роутер або комутатор обслуговує тільки потік даних (рівень передачі трафіку DATAPLANE), ставати більше простим відповідно до більше дешевих. Звичайно ж позбавити повністю інтелекту мережний пристрій не вийде, але його досить замінити простою таблицею переадресації (forwarding table).

SD-WAN – це архітектура, в основі якої лежить принцип пріоритетної реалізації хмарних рішень, що розділяє площини даних і керування, керовані через консоль. Можливо швидко створити оверлейну фабрику SD-WAN для підключення центра обробки даних, філій, комплексів будинків і центрів спільного розміщення ресурсів для підвищення швидкості, безпеки й ефективності мережі.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи побудови програмуємої мережі sdn на базі SD-WAN.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи побудови програмуємої мережі SDN на базі SD-WAN.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем побудови програмуємої мережі SDN на базі SD-WAN.
- Дослідження системи побудови програмуємої мережі SDN на базі SD-WAN.
- Програмна реалізація системи побудови програмуємої мережі SDN на базі SD-WAN.

Об'єктом дослідження є процес побудови програмуємої мережі SDN на базі SD-WAN.

Предметом дослідження є методи побудови програмуємої мережі SDN на базі SD-WAN.

Методи дослідження базуються на методах теорії побудови комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. SDN – програмно-визначаєма мережа. Перевага даної технології в тому, що SDN допомагає управляти мережею саме на програмному рівні. А це значить, що ІТ-фахівцям більше немає необхідності вручну налагоджувати роботу або змінювати налаштування мережного устаткування й, таким чином, витрачати масу часу. Усе робиться в автоматичному режимі із застосуванням інтелектуальних алгоритмів керування. Яку вигоду при цьому одержує бізнес? Це – досягнення максимальної ефективності при керуванні мережею: скорочення витрат на її експлуатацію, підвищення надійності роботи й швидкості відгуку бізнес-додатків, забезпечення мережної безпеки, підвищення швидкості запуску на ринок нових сервісів і послуг. І все це доступно відразу завдяки переходу на програмно-визначаєме рішення.

Зараз SDN активно застосовується в центрах обробки даних, тому що без цієї технології вже не можна реалізувати ні одного завдання по віртуалізації Ікт-інфраструктури дати-центра. Крім цього, SDN використовується з метою модернізації транспортної телеком-інфраструктури компаній зі складними розподіленими мережами передачі даних. Є також і спеціалізована технологія SD-WAN, що у першу чергу цікава компаніям з більшою кількістю філій – фінансовим установам, ритейлу, промисловим і добувним підприємствам і т.д. У цьому випадку SD-WAN дозволяє відмовитися від дорогих VPN-каналів зв'язку від телеком-операторів, для роботи досить звичайного інтернет-з'єднання й LTE, наприклад, як резервного. Технологія дозволяє автоматично розподіляти трафік у мережі передачі даних і відправляти його по найбільш дешевому й незавантаженому в даний момент каналу без втрати швидкості і якості роботи додатків. SD-WAN уже завойовує американський і європейський ринок, в Україні дана технологія ще тільки починає розвиватися. Отже, SDN можна умовно розділити на три групи:

- SDN для ЦОДів;
- транспортний SDN;
- окрема технологія SD-WAN для побудови територіально-розподілених мереж.

У кожного свої особливості й переваги для бізнесу.

Як я вже говорив, різні типи SDN вирішують різні завдання. Доцільність впровадження SDN у дата-центрах уже давно доведена на практиці. Що стосується SDN у транспортній інфраструктурі, те це рішення цікаво переважно провайдерам зв'язку. З його допомогою можна істотно скорочувати витрати на ІТ і при цьому прискорювати процес Time-to-Market, тобто виводу ІТ-сервісів для клієнтів на ринок. Оптимізація витрат досягається за рахунок зниження CAPEX і OPEX, оскільки SDN відразу легко «подружити» практично з будь-яким мережним устаткуванням на відміну від класичних дорогих моновендорних рішень.

От вам конкретний приклад. Модель операторського бізнесу міняється, гравці ринку змушені швидше запускати нові сервіси для користувачів, щоб, з одного боку, забезпечити необхідний рівень виторгу, з іншої, підвищити рівень лояльності абонентів. Не секрет, що вартість класичних послуг, будь то голос, смс, інтернет, стрімко падає, а для того, щоб їх робити, необхідно підтримувати дорогу інфраструктуру. Більше того, нові сервіси вимагають технологічно грамотного налаштування, забезпечення необхідного рівня безпеки й іншого.

Виникає питання – як це можна зробити оперативнo в більших територіально-розподілених мережах операторів? Це непросто навіть із управлінської точки зору. Тільки представте, послуга впроваджується в дата-центрі, потім «попадає» у транспортну мережу й по ній уже доставляється до кінцевого устаткування. За кожний з етапів відповідає певна група технічних фахівців, що працює строго в рамках своєї компетенції. А це значить, що при підключенні нового сервісу абонентів починається передача заявок між відділами – іншими словами, бюрократія. При цьому клієнти стають усе більше розпеченими, нетерплячими. Вони хочуть скористатися послугою миттєво, буквально нажавши пару кнопок на телефоні. От це завдання – максимально швидко запустити новий сервіс для абонента – і допомагає вирішувати SDN.

У корпоративному сегменті, як я вже говорив раніше, усе в більшій кількості ЦОДів впроваджується SDN-технологія. Важливо, що вона застосовна як при будівництві нових ЦОД, так і при модернізації існуючих. Що стосується транспортних мереж, те тут програмно-визначаємі мережі розвиваються повільніше, ніж у телекомі, тому що для Enterprise мережі не є ключовим бізнесом. Плюс корпоративні сервіси для кінцевих клієнтів розвиваються не так швидко, як хотілося б. Транспортної мережі приділяють менше увагу, на її модернізацію витрачають менше грошей.

При цьому, якщо говорити про SD-WAN, то ситуація є трохи інакшою, тому що на перше місце тут виходить не економія на обслуговуванні устаткування, а економія на каналах зв'язку й швидкість підключення нових філій.

Рішення SD-WAN допомагає компаніям замінити або доповнювати оренду мереж VPN в операторів зв'язку. Звичайна побудова класичної телекомунікаційної інфраструктури розподіленої компанії виглядає в такий спосіб. Є головний офіс і трохи регіональних, які потрібно об'єднати в єдиний інформаційний простір, дотримати якості надання сервісу й вимоги безпеки. Компанія повідомляє тендер, у якому беруть участь оператори зв'язку. При цьому, по-перше, вартість каналу зв'язку від оператора значно перевищує вартість звичайного інтернет-з'єднання, по-друге, компанії, для яких критично важлива доступність сервісів для клієнтів, замовляють резервний канал у другого оператора зв'язку. Поверх цього замовник повинен вибудувати свою телекомунікаційну мережу, що складається з маршрутизаторів, мережних пристроїв і міжмережевих екранів. І тільки потім Ікт-інфраструктуру можна експлуатувати. Іноді виникають ситуації, коли оператор зв'язку не обслуговує район, у якому розміщений філія. Тоді завдання по підключенню вирішується нетиповими методами – добре, якщо це прокладка оптоволокну або оренда останньої милі, і гірше, якщо радіорелейне устаткування або той же модем LTE. Все це істотно позначається на строках запуску нових офісів і вартості каналів зв'язку.

Для того, щоб скоротити витрати, і застосовується технологія SD-WAN. Розповім небагато про технічну частину. Роботу програмно-визначаємої розподіленої мережі WAN забезпечує «розумний» контролер у ЦОДі головного офісу, на якому встановлене спеціалізоване ПЗ. До комутатора можна прямо підключати основний і резервний канали доступу в інтернет. При цьому ПЗ саме робить балансування каналів зв'язку, домагаючись порівнянної якості передачі даних. Контролер також виконує функції кінцевого роутера, на якому створюється приватна мережа. Плюс на контролер встановлюються додатки, що контролюють безпеку й прозорість роботи мережі. Повний комплекс в одній «залізці» у головному офісі й підключаються до цього контролера набагато менш «розумні», а, отже, недорогі, комутатори у філіях.

Будь-яка компанія може відмовитися або, як мінімум, оптимізувати дорогі контракти з операторами зв'язку, мінімізувати кількість устаткування у своїх офісах, здійснювати керування офісами через єдиний інтерфейс. SD-WAN – це ефективний інструмент для перекладу витрат з CAPEX в OPEX.

Більше того, SD-WAN не вимагає особливих знань для його інсталяції. Особливо це важливо для віддалених філій, де може просто не бути власного штату ІТ-фахівців. На ринку є «коробкові» пропозиції, у рамках яких SD-WAN устаткування доставляють клієнтові поштою або кур'єром. Будь-який співробітник, не обов'язково ІТ-фахівець, здатний зрозуміти й виконати інструкцію виду «взьміть комутатор і два кабелі, один підключите до порту 1, іншої – до порту 2». Більше нічого не потрібно – пристрій саме зв'язується із центральним сервером, одержує всі конфігурації, настроюється, і цей офіс стає частиною захищеної мережі компанії. Як результат – зовсім інші бюджет і строки. У світі вже є дуже багато кейсів впровадження SD-WAN, наприклад, це мережі магазинів Gap і Tata Group. Потреба даної технології підтверджується великими аналітичними компаніями, зокрема, Gartner пророкує SD-WAN підливний ріст у найближчі два роки.

Україна традиційно переймає західні технології із затримкою в кілька років, поки ми небагато менш просунуті в цьому питанні. Чому так відбувається? Спробу пояснити.

Більшість рішень по віртуалізації за кордоном будується на вільному ПЗ. Співтовариство розроблювачів має потребу в інвестиціях. У частині SDN такими лідерами-інвесторами виступають великі світові оператори зв'язку, а також ІТ-компанії, які не бажають переплачувати вендорам за пропріетарні рішення й бути прив'язаними до продуктових лінійок розроблювачів, тому що це позбавляє їхній бізнес гнучкості. Всі вони готові вкладатися в створення нових продуктів і тримати штат R&D-розроблювачів. Результатом стають повноцінні комплексні рішення, які ідеально підходять під бізнес стільникових операторів і компаній з Enterprise сегмента – вони дійсно на всіх рівнях керування зацікавлені у віртуалізації інфраструктури.

В Україні ж у першу чергу виникає питання, хто буде відповідати за впровадження цього комплексного рішення в рамках компанії, частиною якого є SDN. Адже віртуалізація мереж передачі даних вимагає зміни не тільки технологічного, але й організаційного підходу.

Розвиток власних апаратних елементів, на жаль, іде дуже повільно в Україні, у зв'язку із чим програмні рішення оптимізовані для роботи на чипах іноземного виробництва: Intel, Broadcom, Qualcomm. Із софтом ситуація краще. Українські рішення досить конкурентоспроможні. Є кілька українських компаній, які показують непогані результати в частині SDN розробок.

Важливо відзначити, що рішення SD-WAN може бути впроваджене як у замовника, так і надаватися як керований сервіс. У цьому випадку за розвиток, керування й технічну підтримку Ікт-інфраструктури повністю відповідають фахівці системного інтегратора. У рамках сервісу замовник одержує гарантію безперервності роботи мережі передачі даних філій і при цьому заощаджує на змісті телеком-інфраструктури – переводить капітальні витрати в операційні.

Якщо говорити про конкретні цифри економії, то однакових показників ми не знайдемо навіть у межах однієї галузі, тому що в Україні поки проектів мало, а на Заході зовсім інші умови – наприклад, в операторів зв'язку значно відрізняється ARPU – прибутковість від кожного абонента. Орієнтовно можна сказати, що в наших проектах для телеком-операторів економія досягає 20-30%. З огляду на масштаби бізнесу великих провайдерів, потрібно визнати, що це досить серйозний аргумент на користь руху у бік SDN.

Навіщо потрібний новий підхід до побудови територіально розподілених мереж? Відповідаючи на це питання, вказується на підвищення складності таких мереж, що утрудняє їхнє обслуговування й розвиток, пошук несправностей, забезпечення безпеки й вимагає залучення висококваліфікованих (читай, дорогих) фахівців служби експлуатації та ін. Підхід SD-WAN покликаний спростити рішення цих завдань.

Пояснюючи суть технології SD-WAN, можна сказати наступне: якщо раніше для підключення нової філії до корпоративної мережі могли знадобитися тижні й місяці, те зараз досить відправити пристрій у філію й просто підключити його до мережі: автоматично будуть зроблені весь необхідні налаштування й підключені всі необхідні мережні сервіси. Сучасні рішення SD-WAN дозволяють автоматично визначити, через який тип підключення потрібно маршрутизувати трафік даного додатка – приватний канал зв'язку, Інтернет або мережа стільникового зв'язку. Це дозволить знизити навантаження на дорогі канали зв'язку й використовувати мережу Інтернет для передачі некритичного трафіку.

Рішення SD-WAN автоматично виявляють несправність на каналі зв'язку (або погіршення його характеристик) і автоматично ж переводять трафік на інші канали. При цьому ніякого розриву сеансу зв'язку не відбувається й користувач додатка нічого не зауважує. Для підвищення якості роботи певних додатків, наприклад сеансу голосовий або відеозв'язку, їх трафік може дублюватися по декількох каналах, тоді на пристрої-приймачі будуть вибиратися пакети, які в цей момент часу доставлені з мінімальною втратою й затримкою. Інший можливий варіант – балансування однієї сесії між декількома каналами, що дозволяє задіяти більшу транспортну «трубу», скажемо, при зкачуванні більших файлів.

Тонке регулювання

Рішення SD-WAN – це повноцінні маршрутизатори з функціями забезпечення безпеки, глибокого аналізу трафіку (DPI), балансування трафіку та ін. Рішення здатне ідентифікувати трафік більше 4000 додатків, що дає широкі можливості для регулювання їхнього використання. Наприклад, можна блокувати можливість перегляду Facebook, дозволивши при цьому користуватися месенджером, щоб віддалені колеги могли взаємодіяти між собою. Або, навпаки, блокувати месенджер, залишивши можливість переглядати новини Facebook.

Рішення SD-WAN здатні «розбирати» закритий трафік цих систем і оптимальним образом використовувати всі наявні канали для їхньої доставки.

Як контролер керування мережі SD-WAN виступає SD-WAN Center. Ця віртуальна машина, що поставляється в комплекті з іншими продуктами SD-WAN, забезпечує централізоване адміністрування й керування, а також збір інформації з конфігурації, нагромадження різних звітів (наприклад, по виконанню SLA) та ін. Як і покладено системі SD-WAN, рішення Citrix реалізує принцип автоматичного розгортання (zero touch deployment): досить підключити доставлене у філію пристрій, і конфігураційні параметри будуть автоматично завантажені й активовані.

Коли важлива безпека

Важливе, а для багатьох замовників ключова перевага SD-WAN – підвищення мережної безпеки. Не дивно, що реалізовано підтримку SD-WAN на базі наявних продуктів, що формують так звану фабрику безпеки для комплексного рішення завдань ІБ. До складу рішення SD-WAN входять міжмережеві екрани, засоби організації бездротових локальних мереж, а також системи централізованого керування й аналітики.

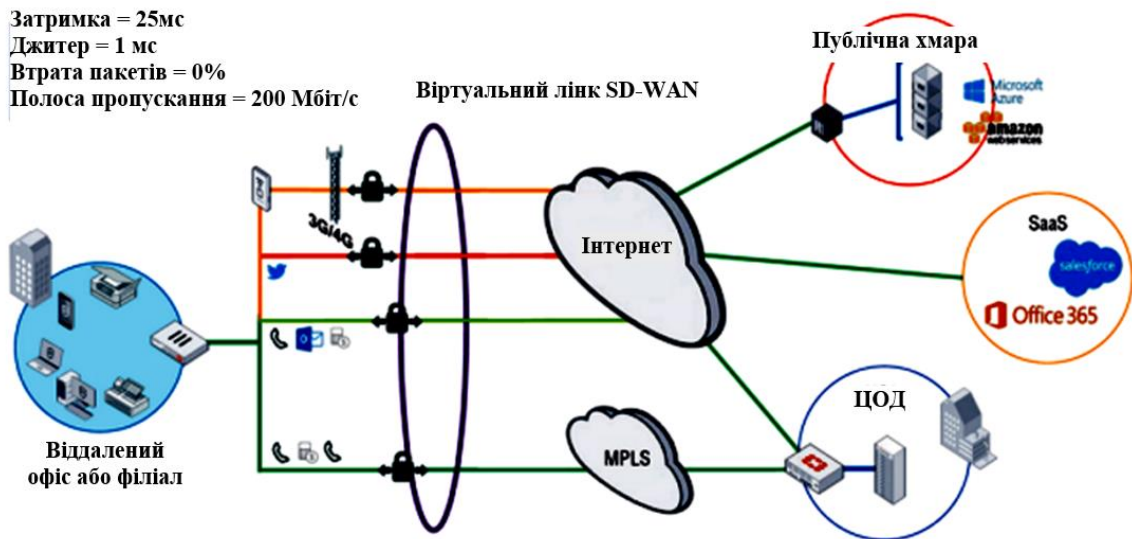


Рисунок 1 – Структурна схема системи

Для реалізації розширених функцій SD-WAN використовуються власні процесори безпеки, застосування яких прискорює виконання завдань, зв'язаних безпосередньо з безпекою й забезпеченням мережними підключеннями. Оптимізована архітектура підтримує реалізацію функцій глибокого аналізу й інспекції трафіку.

Відповідно до останнього звіту про дослідження погроз, частка зашифрованого трафіку становить більше 50% від загального обсягу корпоративного трафіку. Це утрудняє моніторинг і аналіз трафіку, а також знижує ефективність маршрутизації мереж SD-WAN. Як розширені функції SD-WAN підтримують застосування дозволених шифрів SSL і забезпечують найвищу у своєму класі пропускну здатність при інспекції SSL, що гарантує безпечну й ефективну доставку шифрованого трафіку.

Сьогодні забезпечення інформаційної безпеки вимагає нового підходу, якому можна реалізувати, використовуючи комплексні рішення безпеки, інтегровані в мережну інфраструктуру. Серед причин, що ускладнюють рішення завдань мережної безпеки, – ріст числа підключених пристроїв, у тому числі завдяки розвитку Інтернету речей, розмивання границь мереж, уже згадане підвищення частки зашифрованого трафіку й ін. Відповіддю на нові виклики й стала «фабрика безпеки», до складу якої входить комплекс різних продуктів.

Кожний вендор розуміє SD-WAN так, як це йому вигідно, щоб рішення SD-WAN краще корелювало з його лінійкою продуктів. Фахівці виділяють два підходи до реалізації концепції SD-WAN.

При першому підході встановлюване у філії пристрій SD-WAN наділяється максимальним числом функцій, включаючи DPI, просунуті функції безпеки, шифрування та ін. Головний недолік цього підходу – висока вартість таких пристроїв, що може віджахнути багатьох замовників. Крім того, у цьому випадку обмежена можливість керування мережними функціями (сервісами), оскільки вони «прошиті» у кінцевих пристроях.

Другий підхід – коли всі сервіси виносяться в хмару (ЦОД), а в клієнта встановлюється дуже просте (недороге) пристрій. Його завдання зводяться до маркування трафіку і його пробросу (наприклад, по каналі IPsec) до ЦОДу. Крім істотного зниження вартості пристроїв, даний підхід вирішує завдання гнучкого керування сервісами. Але виникає інша проблема, пов'язана з каналами зв'язку. Ряд сервісів висувають досить високі вимоги до пропускну здатності таких каналів, величині затримки та ін.

Єдиного універсального рішення SD-WAN, здатного оптимально вирішити всі завдання, просто не існує. Тому треба шукати компроміс, а можливо, іти по шляху гібридного підходу, що сполучить перший з розглянутих варіантів із другим.

Керування із хмари

Існує хмарна система керування мережною інфраструктурою, що служить для роботи з мережами, побудованими на основі провідних і бездротових пристроїв.

Система підтримує бездротові крапки доступу, маршрутизатори, апаратні міжмережеві екрани й інші пристрої. Система в реальному часі збирає й видає на один екран різні дані: статистику по трафіку, інформацію про стан пристроїв, розташуванні сегмента мережі, його завантаженості та ін. Вся ця інформація доступна через Web-інтерфейс на комп'ютері, планшеті й смартфоні оператора. Система дозволяє не тільки одночасно управляти декількома віддаленими сегментами мережі, але й зберігати й швидко завантажувати налаштування при запуску нового сегмента. За допомогою мобільного додатка монтажникові досить відсканувати QR-код на кришці підключеного до мережі пристрою, і воно буде автоматично зареєстроване й настроєне для роботи.

Більшість компаній, які продають устаткування, одержують більшу частину свого доходу, надаючи послуги інсталяції й післяпродажної підтримки. Підхід Cloud Networking може допомогти перейти від продажів продуктів до продажів рішень і сервісів з постійним доходом.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів побудови програмуємої мережі SDN на базі SD-WAN. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем побудови програмуємої мережі SDN на базі SD-WAN.
- Досліджена система побудови програмуємої мережі SDN на базі SD-WAN.
- На основі отриманих результатів досліджень створена програмна реалізація системи побудови програмуємої мережі SDN на базі SD-WAN.

Розроблені алгоритми дозволяють успішно вирішувати завдання побудови програмуємої мережі SDN на базі SD-WAN. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Kuznetsov, O., Kryvinska, N., Ilchenko, O., Smirnova, T., Ulianovska, Y. «Comparative Analysis of Cryptocurrency Trading Platforms Using the Analytic Hierarchy Process». CEUR Workshop Proceedings, 2023, 3628, pp. 106-115.
2. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». Advanced Information Systems, 2023, 7(2), pp. 49-56.
3. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchov, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». CEUR Workshop Proceedings, Volume 3530, 2023, pp. 256-265.
4. Smirnov, O., Odarchenko, R., Smirnova, T., Bondar, S., Volosheniuk, D. «Optimal Structure Construction of Private 5G Network for the Needs of Enterprises». Lecture Notes on Data Engineering and Communications Technologies, 2023, 178, pp. 208–223.
5. Аль-Мудхафар Акіл Абдулхуссейн М., Смірнова Т.В., Буравченко К.О., Смірнов О.А. «Метод оцінки та підвищення користувацького досвіду абонентів в програмно-конфігурованих мережах на основі використання машинного навчання». Сучасні інформаційні системи, 2023, том 7, № 2, С. 49-56.
6. Smirnova, T., Gnatyuk, S., Yudin, O., Sydorenko, V., Polozhentsev, A., «The Model for Calculating the Quantitative Criteria for Assessing the Security Level of Information and Telecommunication Systems». CEUR Workshop Proceedings Volume 3156, 2022, Pages 390-399.
7. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». Проблеми інформатизації та управління, № 2(70). 2022. С. 28-37.
8. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 3(69). С. 93-98.

9. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції ґешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Вісник Хмельницького національного університету. Серія: «Технічні науки», № 2 (307). С. 46-52. 2022.
10. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції ґешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 1(67). С. 84-89.
11. Smirnova T., Gnatyuk S., Berdibayev R., Avkurova Zh., Iavich M. «Cloud-Based Cyber Incidents Response System and Software Tools». Communications in Computer and Information Science, 2021, vol 1486. Springer, Cham. pp 169-184.
12. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
13. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». Journal of theoretical and applied information technology Vol.98. No 21, 2020, P. 3334-3346.
14. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177.
15. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587.
16. Smirnov, O., Markovets, O. Vovk, N., Turchyn, Y., «Model of informational support for social network administrators' content creation». CEUR Workshop Proceedings Volume 2616, 2020, Pages 125-136.
17. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». CEUR Workshop Proceedings Volume 2616, 2020, Pages 366-379.
18. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645.
19. Smirnov O. Kuznetsov A., Zaichenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019; Odessa; Ukraine; 9-13 September 2019. P.22-28.
20. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.
21. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019 . P.517-522.
22. Smirnov, O., Odarchenko, R., Abakumova, A., Usik, P., Kundyzy, M., «QoE optimization technique for media delivery in 5G networks». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019. P.597-601.
23. Smirnov, O., Krasnobayev, V., Yanko, A., Kuznetsova, T. «Methods of nulling numbers in the system of residual classes». CEUR Workshop Proceedings, Vol 2588, P. 90-106, 2019.
24. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Averchev, A., Pastukhov, M., Kuznetsova, K., «Formation of Pseudorandom Sequences with Special Correlation Properties», 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT -2019/ Lviv, Ukraine, 2-6 July, 2019, P. 395-399.
25. Smirnov, O., Kuznetsov, A., Kiian, A., Zamula, A., Rudenko, S., Hryhorenko, V., «Variance Analysis of Networks Traffic for Intrusion Detection in Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 353-358.
26. Smirnov, O., Kuznetsov, A., Kavun, S., Babenko, B., Nakisko, O., Kuznetsova, K., «Malware Correlation Monitoring in Computer Networks of Promising Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 347-352.
27. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Pastukhov, M., Kuznetsova, K., Prokopovych-Tkachenko, D., «Discrete Signals with Special Correlation Properties», CEUR Workshop Proceedings Volume 2353, CEUR Workshop Proceedings 2019, Pages 618-629.
28. Smirnov A.A., Kuznetsov A.A., Danilenko D.A., Berezovsky A., «The statistical analysis of a network traffic for the intrusion detection and prevention systems», Telecommunications and Radio Engineering. – Volume 74, Issue 1. – Begel House Inc. – 2015. – P. 61-78.
29. Смірнов О.А., Смірнова Т.В., Буравченко К.О., Кравченко С.С., Горбов В.О., «Хмарна система підтримки

прийняття рішень технологічного процесу відновлення поверхонь конструкцій і деталей машин». Сучасні інформаційні системи. 2021. Т. 5, № 4. С. 79-95

30. Смірнов О.А., Усік П.С., Миронець І.В., Буравченко К.О., Якименко Н.М. «Метод підвищення ефективності розподіленої обробки даних у комп'ютерних системах операторів стільникового зв'язку» Вісник Черкаського державного технологічного університету. Технічні науки. №4. С. 103-110. 2020.
31. О.А.Смірнов, Т.В.Смірнова, Л.І. Поліщук, К.О. Буравченко, А.О.Макевнін, «Дослідження хмарних технологій як сервісів», Кібербезпека: освіта, наука, техніка. № 3(7). С. 43-62. 2020.

УДК 004

А.Розиев, магістр гр. КІ-24М,

Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ БЕЗПЕЧНОЇ РОЗРОБКИ ПРИ ВИКОРИСТАННІ ТЕХНОЛОГІЇ AGILE

У статті розроблено програмне забезпечення, яке призначено для системи безпечної розробки при використанні технології Agile. Метою розробки є дослідження та принципи побудови системи безпечної розробки при використанні технології Agile. Об'єктом дослідження є процес безпечної розробки при використанні технології Agile. Предметом дослідження є методи безпечної розробки при використанні технології Agile. Методи дослідження базуються на методах теорії розробки програмного забезпечення, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи безпечної розробки при використанні технології Agile. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

методи безпечної розробки, Agile

Постановка проблеми. Популярність Web-застосунків як основного інструмента онлайн-бізнесу росте рік у рік, одночасно із цим усе більше залучаючи зловмисників. Тим часом, відповідно до досліджень Contrast Security, порядку 80% Web-застосунків у середньому містять до 45 уразливостей, з яких принаймні одна має високий рівень критичності. Така ситуація свідчить про недостатню увагу до питань безпеки в процесі розробки. Із впровадженням методологій прискореної розробки Agile положення ще більше збільшується.

Швидкість розробки збільшується рік у рік. Раніше новий реліз з'являвся один раз у квартал або один раз у рік, зараз же, в умовах зростаючої конкуренції, всі замовники прагнуть якнайшвидше реалізовувати новий функціонал. У зв'язку із цим доводиться скорочувати цикли розробки: релізи випускаються кілька разів у тиждень або навіть у день, так що стандартний підхід, коли про безпеку замислювалися лише в самому кінці, при такій моделі працює дуже погано.

Насамперед якщо не власники бізнесу, то власники застосунків повинні приділяти пріоритетну увагу безпеки й усвідомлювати, як наслідку зломів, компрометацій і витоку даних позначається на прибутку компанії. Крім того, необхідно переглянути роль фахівця з ІБ: з охоронця/наглядача, що заважає всім процесам і вставляє цівка в колеса, як його часто сприймають, він повинен перетворитися в партнера й ІБ-наставника.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи безпечної розробки при використанні технології Agile.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи безпечної розробки при використанні технології Agile.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем безпечної розробки при використанні технології Agile.
- Дослідження системи безпечної розробки при використанні технології Agile.
- Програмна реалізація системи безпечної розробки при використанні технології

Agile.

Об'єктом дослідження є процес безпечної розробки при використанні технології Agile.

Предметом дослідження є методи безпечної розробки при використанні технології Agile.

Методи дослідження базуються на методах теорії розробки програмного забезпечення, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Agile – це гнучка методологія розробки, яка являє собою концепцію, у рамках якої виконується розробка програмного забезпечення. У рамках даної концепції існує кілька методик, метою яких є мінімізація ризиків, досягається ця мета розробкою (проектуванням) короткими ітераціями.

Основні цінності Agile утримуються в “Маніфесті Agile”:

- Люди і їхня взаємодія важливіше, ніж процеси й засоби.
- Працююча система важливіше, ніж вичерпна документація.
- Співробітництво із замовником важливіше, ніж обговорення умов контракту.
- Реагування на зміни важливіше, ніж проходження плану.

Scrum – це конкретна технологія (методи ведення проекту й ролі учасників процесу), що реалізує принципи Agile.

Дана технологія дозволяє в жорстко фіксованій й невеликій за часом ітерації, називаній **спринтами (sprints)**, надавати замовникові працююче ПЗ з новими можливостями, для яких визначений найбільший пріоритет.

Вимоги до результатів спринту визначаються на початку спринту (планування спринту) і не можуть змінюватися в процесі спринту. Невелика тривалість спринту надає процесу передбачуваність і гнучкість.

Ролі Scrum

1. **Scrum Master.** Бізнес-аналітик, керівник проекту. Проводить наради, стежить за дотриманням технології Scrum, знімає протиріччя й направляє команду. Основний обов'язок – забезпечення виконання технології Scrum.

2. **Product Owner.** Власник проекту, функціональний замовник. Представляє інтереси замовника (кінцевих користувачів).

3. **Development Team.** Команда фахівців (розроблювачів). Складається з фахівців різного профілю – аналітиків, архітекторів, програмістів, тестувальників. Команда відповідає за результат як єдине ціле.

Елементи Scrum

Sprints (Спринт)

Спринт – ітерація в процесі, у ході якої створюється новий результат. Спринт жорстко фіксований у часі – від 1 до 4 тижнів. Ніж коротше спринт, тим гнучкішим є процес розробки, оскільки після кожного спринту вимоги до системи можуть коректуватися на підставі зворотного зв'язка від замовника. Відповідно, знижуються ризики роботи в неправильному напрямку. З іншої сторони при більш тривалому спринті знижуються витрати на наради, і більше залишається часу на рішення завдань проекту.

Project backlog (журнал завдань проекту)

Project backlog – журнал побажань проекту. Це список вимог до системи, упорядкований за пріоритетом – важливості реалізації. Журнал побажань можуть доповнювати всі учасники процесу.

Sprint backlog (журнал завдань спринту)

Sprint backlog – журнал побажань спринту. Містить функціональність, відібрану власником проекту (**Product Owner**) для реалізації на поточному спринті.

Burndown chart (Діаграма згоряння завдань)

Burndown chart – діаграма згоряння завдань. Демонструє обсяг зробленої й роботи, що залишилася, щодо строку проекту. Діаграма актуалізується щодня. Передбачено два види діаграм:

– Діаграма згоряння для спринту – показує, скільки вже завдань зроблене й скільки ще залишається зробити в поточному спринті.

– Діаграма згоряння для проекту – показує, скільки вже завдань зроблене й скільки ще залишається зробити до завершення проекту.

Abnormal Termination (Зупинка спринту)

Abnormal Termination – зупинка спринту. Спринт може бути зупинений раніше його планового строку закінчення у виняткових ситуаціях. Наприклад, якщо завдання спринту не можуть бути досягнуті або якщо вони стали неактуальними. Рішення про зупинку приймається командою або Власником проекту. Після зупинки починається новий спринт.

Daily Scrum meeting (Щоденна нарада)

Daily Scrum meeting – щоденна нарада команди. Правила проведення наради:

- проводиться в те саме час, у тому самому місці;
- не більше 15 хвилин;
- кожному учасникові треба відповісти на 3 питання:
- Що я зробив учора
- Що я планую зробити сьогодні
- Що мені заважає

Scrum of Scrums (Скрам над скрамом)

Scrum of Scrums – Скрам над скрамом – нарада декількох Scrum-команд. Проводиться після щоденної скрам наради. Дозволяє декільком скрам командам обговорювати роботу, фокусуючись на загальних областях і взаємній інтеграції. Повістка та ж, що й на щоденному скрам нараді плюс наступні питання:

- Що кожна команда зробила з моменту попередньої щоденної наради?
- Що кожна команда зробить до наступної щоденної наради?
- Є чи проблеми, що заважають або сповільнюють роботу кожної команди?
- Потрібно чи іншій команді зробити щось із завдань вашої команди?

Sprint review meeting (огляд підсумків спринту)

Sprint review meeting – огляд підсумків спринту. Проводиться наприкінці спринту:

– Команда демонструє результати спринту всім зацікавленим особам. Залучається максимальна кількість глядачів.

– Всі члени команди беруть участь у демонстрації (одна людина на демонстрацію або кожного показує, що зробив за спринт).

– Не можна демонструвати незавершену функціональність.

– Обмежена чотирма годинами залежно від тривалості ітерації й обсягу результату.

У цей час про гнучкі технології виконання проектів Agile/Scrum говорять всі частіше. У цій статті я напишу про своє бачення плюсів і мінусів застосування Scrum при виконанні проектів з позиції замовника.

Agile, Scrum, Kanban – ці слова вже встигли примелькатися всім, хто має яке-небудь відношення до розробки продуктів, бізнес-процесам, організації праці. Багато хто вважають, що за ціми технологіями майбутнє. Але, що цікаво, деякі можуть пояснити розходження між ціми поняттями, наприклад, відповістити на запитання про Scrum і Agile: різниця існує й у чому вона полягає?».

Отже, спершу визначимося з методологічним апаратом:

Agile – клас гнучких методологій розробки; набір цінностей і базових принципів в області розробки ПЗ, основна суть яких зводиться до взаємодії функціональних крос-команд що самоорганізуються. У суть Agile закладені адаптивне планування, еволюційна розробка, максимально швидкий випуск нових версій продукту, постійна доробка й швидка відповідь на виникаючі складності. На сьогоднішній день Agile уже давно вийшов за рамки розробки програмного забезпечення, а його різні дочірні методології використовуються в різних сферах керування.

Scrum – одна з методологій у рамках **Agile**. В основі даної методології лежать «спринти» – короткі жорстко фіксовані за часом ітерації, у рамках яких як виконавець так і замовник виконуються певний набір завдань.

Kanban – система, що передбачає організацію розробки/ праці/ виробництва/ постачання відповідно до принципу Just In Time (або точно в строк). В основі Kanban лежить виробнича й постачальницька система Toyota, що у другій половині XX століття ледве було не знищила весь американський автопром.

Основними цінностями в концепції **Scrum** оголошені комунікація й готовність до змін, а не тверде проходження первісному плану. Коли ж **Scrum** може принести тільки користь, а коли – шкода?

Тверда підрядна технологія

Суть підряду дуже проста. Замовник замовляє й чітко визначає в специфікації до договору, що саме він хоче одержати. У договорі чітко фіксується вартість і строк. Замовник передає виконавцеві матеріали, придатні для обробки. Виконавець перевіряє матеріали, і якщо вони непридатні, то негайно сповіщає про це Замовників і зупиняє роботи. Замовник зобов'язаний робити Виконавцеві сприяння в процесі робіт. Якщо Виконавець не уклався в строк, або надав настільки неякісний результат, що можна припустити недосягнення результату як такого – Замовник має право розірвати договір і зажадати повернення авансу в повному розмірі. Якщо ж результат досягнуть, то Замовник приймає роботи, підписує акт виконаних робіт, оплачує роботу.

При виконанні проектів по впровадженню ERP-систем звичайно полягають саме такі договори. У договорі визначаються фіксований бюджет і строк на кожний етап робіт, саме завдання (безпосередньо в договорі або окремо в ТЗ), обов'язку Замовника на кожному етапі, однозначні критерії результату. Зміни у вимогах у процесі робіт або не допускаються зовсім, або додатковий обсяг робіт оплачується додатково за окремою згодою.

Підкреслимо ключове положення цієї моделі взаємодії: у результаті оцінки Виконавцем поставленої споконвічно завдання в договорі встановлюється твердий строк і вартість етапу. Тому зміна завдання в процесі виконання робіт не допускається. Це правило діє, наприклад, і при ремонті квартири, і при впровадженні ERP-систем.

Якщо використовується ітераційний підхід, то після закінчення етапу робіт стають ясними завдання наступного етапу, а виходить, що впливають обсяги робіт. Відповідно, у додатковій угоді фіксується строк і вартість на наступний етап. Буває ще цікавіше – при впровадженні ERP-систем Виконавець (найчастіше щоб виграти тендер) фіксує бюджет на весь проект цілком, іноді на 1-2 роки вперед.

Замовники приймають бюджет, думаючи, що й строки, і бюджети будуть дотримуватися. При цьому, відповідно до договору, етапи робіт у кожному разі закриваються актами й оплачуються окремо, чи ледве не щомісячно. Не виключено, що через кілька місяців з'ясується, що бюджет необхідно збільшити в 2-3 рази (мов, вимоги до системи змінилися, а «ми про це не домовлялися, у ТЗ цього немає!»). Не хоче – до побачення.

Основний недолік твердої технології – істотні обмеження гнучкості у вимогах і рішеннях, в умовах виконання робіт, обмеження гнучкості участі Замовника в процесі виконання етапу. Така гнучкість у ході виконання робіт у край важлива, тому що на початку кожного етапу детальні, вичерпні, точні вимоги й організаційні умови сформулювати важко – високий ступінь невизначеності системи. Інтегратори-виконавці часто говорять: «Клієнт сам не знає, чого хоче»... Зовсім тупикові ситуації виникають, коли клієнт – який не знає, чого хоче – вимагає зробити систему «під ключ».

Оскільки строки й бюджети визначаються на початку кожного етапу, будь-які коректування вимог до системи з боку Замовника, а також будь-які зміни умов у процесі виконання робіт на етапі (наприклад, обсяг участі й сприяння з боку Замовника) можуть створити додаткову трудомісткість для Виконавця, що зажадає перегляду бюджету й строків. Але перегляд бюджетів і строків – потенційно конфліктна ситуація!

Отже, Замовник зацікавлений у можливості зміни вимог у процесі виконання робіт, але підрядна технологія не дає йому цього робити, викликаючи конфлікт із Виконавцем.

Для підвищення гнучкості – у бюджет і строки заставляються ризики. Крім того, досвідчені Виконавці передбачають і прописують процедуру «Керування змінами», відповідно до якої в остаточному підсумку всі зміни первісних вимог проходять через процедури ініціювання й оцінки.

Вартість ризиків Виконавця, відбитих у бюджеті проекту, у подібних роботах може досягати більше 50% від вартості етапу. Інакше кажучи, Виконавець продає замовникові не тільки результат робіт, але й свої ризики. Якщо ризики не реалізуються, вартість робіт для Замовника виявляється завищеною щодо реальної трудомісткості цих робіт, а Виконавець дістає додатковий прибуток. Буває й навпаки – реалізуються незаплановані ризики понад бюджет, у результаті чого Виконавець виявляється в збитку.

Таким чином, підрядна технологія обмежує гнучкість Замовника в зміні вимог, умов роботи й ступеня своєї участі, коли роботи вже початі, і «корабель відійшов від берега». Необхідна процедура керування змінами... але немає гарантії, що ця процедура зможе передбачити всі ситуації.

Більші витрати сторони несуть на формулюванні всіх умов робіт і вимог до результату при початку етапу, а також на формалізації правил керування змінами. І це при тім, що умови й вимоги можуть швидко втрачати актуальність у процесі виконання етапу! У результаті частина розробленого й оплаченого функціонала може виявитися незатребуваною в процесі експлуатації системи – нерідка ситуація при підрядному способі.

Чому ж Замовники, як правило, вимагають, щоб впровадження складних систем виконувалося по договорах підряду? Відповідь проста:

- Інші способи поділу відповідальності для Замовника менш комфортні. У договорі Замовник замовляє, а Виконавець – виконує, ця логіка породжує поділ відповідальності сторін за проект, зручне для Замовника.

- Інші (не підрядні) технології вимагають більшої відповідальності з боку замовника.

Чому Виконавці охоче погоджуються на підряд?

- Щоб забезпечити гнучкість у вимогах, Виконавці закладають у фіксовану вартість проекту ризики. Якщо ризики не реалізуються, Замовник переплачує.

- Вимоги до результату погодяться «на березі», а виходить, Замовник знову втрачає гнучкості, а Виконавець одержує можливість не робити потрібний Замовникові функціонал, посилячись на те, що «у ТЗ цього немає». Так працювати спокійніше: зафіксував вимоги й «уперед».

Гнучкість вимог у процесі виконання робіт

Через високу невизначеність системи на початку проекту й неможливості передбачити всі, замовники прагнуть міняти вимоги в процесі виконання робіт. З'являються нові ідеї, відбуваються зміни на підприємстві, з'ясовується, що замість інтеграції зі старою системою краще доробити нову систему й т.д.

Гнучкість вимог життєво необхідна для досягнення результату, дійсно потрібного підприємству.

Гнучка технологія (Scrum)

Зміст концепції Scrum у тому, що кожний етап робіт розбивають на короткі ітерації фіксованої тривалості (від 1-й тижня до місяця). На початку кожної ітерації визначають завдання сторін – Замовника й Виконавця – тільки на дану ітерацію. У процесі ітерації (у термінології Scrum – «Спринт») зміни в завданнях Сторін, вимогах і умовах виконання робіт не допускаються. По завершенні ітерації Сторони аналізують результати й ставлять завдання на наступну ітерацію; і при цьому **вужі допускається змінювати умови виконання робіт**.

Дуже важливо щільна й безперервна взаємодія Виконавця й Замовника. Якнайбільше спілкуватися, бути однією командою – от ключовий момент даного підходу!

Перевага гнучкої технології:

– За рахунок того, що ітерації набагато коротше, ніж весь етап робіт, досягається набагато більша гнучкість у прийнятті рішень і керуванні змінами в ході робіт. Між ітераціями Замовник не обмежений у прийнятті організаційних рішень, зміні рамок проекту й так далі. Очевидно, що сторони рухаються до результату більше коротким шляхом, чим при підряді, оскільки можуть безупинно вносити зміни в проект.

– Виключаються конфліктні ситуації через зміни, тому що в центр такої технології поставлена можливість зміни. Якщо при підряді зміна – це неприємне відхилення, що вимагає розбирань і з'ясування, хто кому повинен, то в Scrum зміни – це суть і складова процесу.

– Тарифікація ітерацій теж може бути гнучкою – або оплата виробляється по фактичній трудомісткості (відповідно до погодинної ставки роботи співробітника); або вартість ітерації фіксується на початку ітерації, виходячи із прогнозу її трудомісткості. У результаті, Замовник оплачує тільки фактичну трудомісткість і не переплачує за ризики.

Прогноз вартості кожної ітерації виконується досить просто по погодинному тарифі (якщо відомо кількість співробітників Виконавця, планованих на ітерацію з повним завантаженням).

Таким чином, при використанні гнучких технологій бюджет проекту на певний період будується на підставі прогнозу трудомісткості й кількості приваблюваних співробітників Виконавця.

Як правило, при використанні гнучких технологій вартість проекту не перевищує його вартості при використанні твердих технологій, оскільки кінцева вартість прямо залежить від сумарної трудомісткості. Трудомісткість гнучкої технології може виявитися навіть менше за рахунок того, що не розробляється незатребуваний функціонал, а виходить, менше буде й вартість проекту в цілому.

Однак технології Scrum властиві свої недоліки. Один з них – ризик несистемного підходу. Визначення всіх вимог до системи до початку робіт дозволяє продумати систему в цілому ще до її реалізації. У ході реалізації частини системи враховуються властивості всієї системи, всі вимоги до неї, а не тільки до одному з її сегментів. У цьому й полягає системний підхід.

При несистемному підході висока ймовірність, що замість системи вийде набір незв'язаних елементів – зовсім як у древній східній казці, у якій мудреці за хвостом, хоботом і ногами не побачили слона:

Тому якщо їсти можливість ретельно продумати функціонал і вимоги до початку реалізації, їй треба скористатися. Зрозуміло, якщо є вся необхідна інформація. Це ідеальний випадок, і таке буває рідко, тому найкращим варіантом у таких ситуаціях є Scrum, що дозволяє формувати вимоги до системи в процесі її реалізації й експлуатації. Якщо ж зміни не передбачаються, то Scrum – не кращий вибір.

Наприклад, при розробці типових рішень (не під конкретного замовника з його неочевидними «хотелками») систему краще продумувати відразу в повному обсязі, цілісно. Оскільки зовнішнього непередбаченого замовника немає – у цьому випадку замовником, по суті, є сама команда розроблювачів – вимоги до системи відомі споконвічно. Звичайно, якщо розроблювачі знають, за що беруться.

Отже, керування змінами при гнучкій технології Scrum відбувається найбільше ефективно. Варто врахувати, що в проектах з високим ступенем невизначеності системи на початку робіт керування змінами є ключовим чинником, що впливає як на кінцевий результат, так і на оптимізацію бюджету. У тому числі значно знижуються ризики розробки непотрібного функціонала, або функціонала, що не відповідає потребам бізнесу.

Договір підрядний, а працюємо по Scrum

Переваги Scrum всі частіше можна спостерігати, коли реалізується один із класичних проектних ризиків – “звалювання” проекту в Scrum по факту, хоча за договором робота виконується по підряді – із твердими строками й вартістю. Таке “звалювання” дуже вигідно активному Замовникові, тому що дозволяє досягти бажаного результату, відштовхуючись

щораз від фактичного результату проміжного етапу робіт. Замовникові набагато простіше зрозуміти, що він хоче одержати насправді, якщо він відштовхується від того, що вже зроблено.

Така ситуація характерна не тільки для IT-проектів. При ремонті квартири, будівництві будинку, і будь-якому проекті, коли складно чітко формалізувати остаточний результат, Замовник може почати контролювати безупинно кожний дрібний етап і вносити коректування в споконвічну постановку завдання. Це приводить Виконавця в замішання, тому що строки й трудомісткість роботи неконтрольована ростуть, а бюджет проекту не міняється. Виконавець починає думати, що «Замовник не знає, що хоче», це потенційно конфліктна ситуація. Насправді, Замовник і не може знати, що хоче – це цілком нормально. Що він хоче, він починає розуміти тільки після того як побачить, що виходить по факті – тільки після чергової ітерації робіт. Це Scrum.

На IT проекті “звалювання” проявляється в такий спосіб.

Як правило це відбувається на етапі реалізації (кодування). Як тільки Замовник просить показувати проміжні результати, і починає їх приймати, не чекаючи пред'явлення всього обсягу робіт на випробування, чекайте перехід по факті в Scrum. Приймання Замовником уже першої ітерації робіт швидше за все спричинить частковий перегляд Замовником усього технічного завдання, а це вже Scrum. Зрозуміло, для кінцевого результату й задоволення Замовника це благо. А перегляд ТЗ – це зміна трудомісткості, звичайно в більшу сторону. І якщо не укласти додаткову угоду на збільшення вартості, то ущемляються інтереси Виконавця. А це конфліктна ситуація.

Виникає питання – чи не простіше споконвічно домовитися працювати по Scrum? Адже справедлива оплата робіт повинна відповідати фактичній трудомісткості, що при “звалюванні” в Scrum не піддається точному розрахунку!

Що ж виходить? Замовник може заперечувати Scrum при укладанні договору, але потім фактично змусити Виконавця працювати по Scrum. У рамках фіксованого строку й бюджету. І не забуваємо, що прострочення строку здачі робіт (через постійне внесення Замовником дрібних коректувань у завдання) загрожує Виконавцеві серйозною відповідальністю, тому що Виконавець відповідає за строк здачі робіт. Невиконання строку надає право Замовникові висувати обґрунтовані претензії. Більше того, Замовник може дорікати Виконавцю в недостатньому професіоналізмі, тому що Замовник схильний часто свої коректування в постановку Завдання розцінювати як свої вимоги виправити недоліки.

На рисунку 1 зображена структурна схема програмного забезпечення, яке реалізує процес безпечної розробки при використанні технології Agile з застосуванням обфускації коду. Розглянемо цю схему більш детально.

Процес безпечної розробки при використанні технології Agile з застосуванням обфускації може бути здійснений над кожним з вище перерахованих видів подання програмного коду, тому прийнято виділяти наступні рівні процесу безпечної розробки при використанні технології Agile з застосуванням обфускації:

- нижчий рівень, коли процес безпечної розробки при використанні технології Agile з застосуванням обфускації здійснюється над асемблерним кодом програми, або навіть безпосередньо над двійковим файлом програми, що зберігає машинний код;
- вищий рівень, коли процес безпечної розробки при використанні технології Agile з застосуванням обфускації здійснюється над вихідним кодом програми написаному мовою високого рівня.

Здійснення безпечної розробки при використанні технології Agile з застосуванням обфускації на нижчому рівні вважається менш комплексним процесом, але при цьому більш важко реалізованим з ряду причин. Одна із цих причин полягає в тому, що повинні бути враховані особливості роботи більшості процесорів, так як спосіб безпечної розробки при використанні технології Agile з застосуванням обфускації, прийнятний на одній архітектурі, може виявитися неприйнятним на іншій.

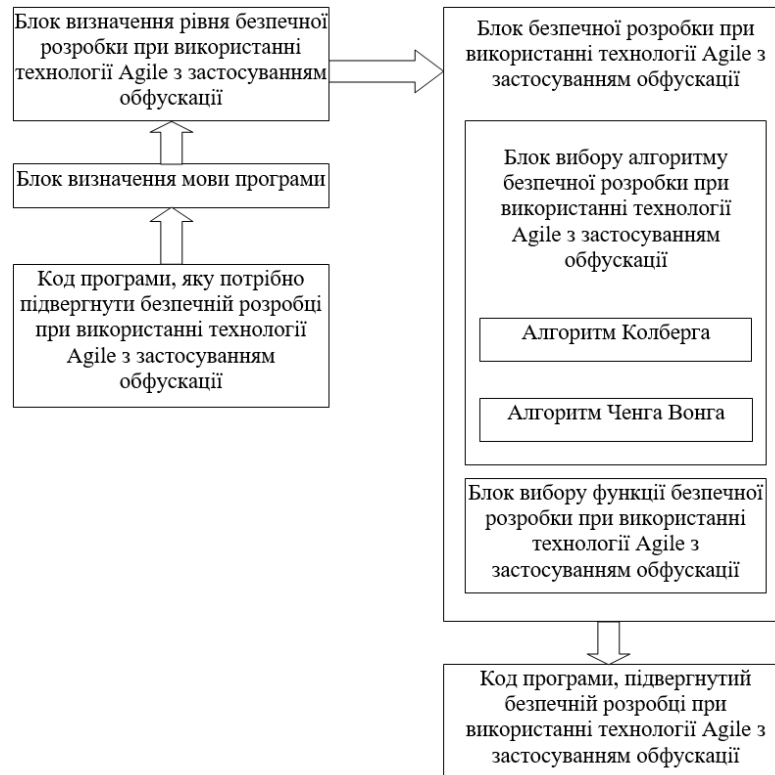


Рисунок 1 – Структурна схема системи

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів безпечної розробки при використанні технології Agile. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем безпечної розробки при використанні технології Agile.
- Досліджена система безпечної розробки при використанні технології Agile.
- На основі отриманих результатів досліджень створена програмна реалізація системи безпечної розробки при використанні технології Agile.

Розроблені алгоритми дозволяють успішно вирішувати завдання безпечної розробки при використанні технології Agile. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Смірнова, Т.В. «Дослідження методів, моделей та сучасних ІТ-рішень для підтримки технологічних процесів у критичній інфраструктурі держави». Кібербезпека: освіта, наука, техніка. 2025. Том 2 № 30. С.195-208, 2025.
2. Вінтенко Б., Смірнов О., Миронець І., Смірнова Т., Смірнов С. «Імітаційна модель шляхів вхідних даних комп'ютерної інтелектуальної системи підтримки оператора енергоблоку АЕС». Комбінаторні конфігурації та їхні застосування: Матеріали XXVII Міжнародного науково-практичного семінару, присвяченого 125-річчю Національного університету «Запорізька політехніка» (Запоріжжя-Кропивницький-Київ, 4-6 червня 2025 р.). Запоріжжя: НУ «Запорізька політехніка», 2025. С.82-91.
3. Al-Azzeh, J., Ayyoub, B., Mesleh, A., Smirnova, T., Gnatyuk, S., Drieiev, O., Smirnov, O., Dorenskyi, O. «Cloud-Based Information System for Evaluating Caverns in the Process of Blasting Metal Surfaces of Details». International Review on Modelling and Simulations 18 (1), 2025. pp. 32-42.
4. Вінтенко Б.Ю., Смірнов О.А., Миронець І.В., Смірнова Т.В., Коваленко О.В., Мацуй А.М. «Модель шляхів отримання вхідних даних комп'ютерної інтелектуальної системи підтримки оперативного персоналу АЕС». Центральнотураїнський науковий вісник. Технічні науки. 2025. Вип. 11(42), ч. II. С.52-62.
5. Вінтенко Б.Ю., Смірнов О.А., Миронець І.В., Смірнова Т.В. «Методи забезпечення відмовостійкості

- інтелектуальних систем підтримки оператора». VIII міжнародна науково-практична конференція «Інформаційна безпека та комп'ютерні технології», м. Кропивницький. 24-25 квітня 2025 р. – Кропивницький: ЦНТУ. – 2025. – С. 44-46.
6. Смірнов, О.А., Константинова, Л.В., Коноплицька-Слободенюк, О.К., Козірова, Н.В., Якименко, Н.М., Доренський, О.П., Буравченко, К.О. «Дослідження інструментів штучного інтелекту для роботи з базами даних та аналізу даних». Кібербезпека: освіта, наука, техніка. 2025. №3(27), С. 429–448.)
 7. Smirnov O., Fedorov E., Neskrodieva A., Neskrodieva T. «Intellectual Classification method of Gymnastic Elements Based on Combinations of Descriptive and Generative Approache». CEUR Workshop Proceedings Volume 3664, 2024, Pages 11-23.
 8. Вінтенко, Б., Миронець, І., Смірнов, О., Коваленко, А., Коноплицька-Слободенюк, О., Смірнова, Т., Константинова, Л. «Дослідження застосування систем підтримки оперативного персоналу об'єкту критичної інфраструктури при керуванні енергоблоком АЕС з реактором типу ВВЕР-1000». Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2024. № 2(26), С. 6-26.
 9. Вінтенко, Б., Миронець, І., Смірнов, О., Кравчук, О., Козірова, Н., Савеленко, Г., Коваленко, А. «Дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». Кібербезпека: освіта, наука, техніка. 2024. №3(23), С. 111-131.
 10. Kuznetsov O., Ilchenko O., Kryvinska N., Buravchenko K., Smirnov O., Savchenko Iu. «An Empirical Assessment of Leading Blockchain Financial Services». 2023 IEEE 1st Ukrainian Distributed Ledger Technology Forum (UADLTF), Kyiv, Ukraine, 2023, pp. 1-6,
 11. Kuznetsov, O., Kryvinska, N., Ilchenko, O., Smirnova, T., Ulianovska, Y. «Comparative Analysis of Cryptocurrency Trading Platforms Using the Analytic Hierarchy Process». CEUR Workshop Proceedings, 2023, 3628, pp. 106-115.
 12. Malyukov V., Bebesko B., Lakhno V., Smirnov O., Malyukova I., Mohylnyi H. «Managing the Purchase-Sale Process of Digital Currencies Under Fuzzy Conditions». Lecture Notes in Networks and Systems, 2023, 729 LNNS, pp. 104–112.
 13. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». Advanced Information Systems, 2023, 7(2), pp. 49-56.
 14. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchey, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». CEUR Workshop Proceedings, Volume 3530, 2023, pp. 256-265.
 15. Smirnov, O., Odarchenko, R., Smirnova, T., Bondar, S., Volosheniuk, D. «Optimal Structure Construction of Private 5G Network for the Needs of Enterprises». Lecture Notes on Data Engineering and Communications Technologies, 2023, 178, pp. 208–223.
 16. Вінтенко Б.Ю., Смірнов О.А., Коваленко А.С., Смірнов С.А., Буравченко К.О. «Дослідження вимог міжнародних стандартів IEC60880 та IEC62138 з розробки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». Системи управління, навігації та зв'язку, 2023, вип. 3(73), С. 155-166.
 17. Вінтенко, Б., Миронець, І., Смірнов, О., Кравчук, О., Козірова, Н., Савеленко, Г., Коваленко, А. «Дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». Кібербезпека: освіта, наука, техніка. 2024. №3(23), С. 111-131.
 18. Вінтенко Б.Ю., Смірнов О.А., Коваленко О.В., Смірнов С.А., Коваленко А.С. «Дослідження нормативних документів та галузевих стандартів розробки програмного забезпечення комп'ютерних систем управління АЕС, важливих для безпеки». Системи управління, навігації та зв'язку, 2023, вип. 2(72), С. 170-178.
 19. Аль-Мудхафар Акіл Абдулхуссейн М., Смірнова Т.В., Буравченко К.О., Смірнов О.А. «Метод оцінки та підвищення користувальницького досвіду абонентів в програмно-конфігурованих мережах на основі використання машинного навчання». Сучасні інформаційні системи, 2023, том 7, № 2, С. 49-56.
 20. Вінтенко Б.Ю., Смірнов О.А., Коваленко О.В., Смірнов С.А. «Дослідження нормативної документації та стандартів розробки програмного забезпечення комп'ютерних систем управління АЕС, важливих для безпеки». VI міжнародна науково-практична конференція «Інформаційна безпека та комп'ютерні технології», м. Кропивницький. 20-21 квітня 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 35-36.
 21. Smirnov, O., Karapetyan, A., Fedorov, E., «Creating Neural Network and Single Solution Human-Based Metaheuristic Methods of Solving the Traveling Salesman Problem». CEUR Workshop Proceedings, Volume 3312, 2022, pp. 47-58.
 22. Smirnov O., Kuznetsov A., Kryvinska N., Kiian A., Kuznetsova K. «Full Non-Binary Constant-Weight Codes». SN Computer Science, Vol 2, 337, 2021. <https://doi.org/10.1007/s42979-021-00739-w>.
 23. Smirnov O., Kovalenko O., Kovalenko A., Kavun S. «Quantitative Risk Assessment Method Development in the Context of the SDLC-model». 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), 2021, pp. 203-208, doi: 10.1109/PICST54195.2021.9772143
 24. Smirnova T., Gnatyuk S., Berdibayev R., Avkurova Zh., Iavich M. «Cloud-Based Cyber Incidents Response System and Software Tools». Communications in Computer and Information Science, 2021, vol 1486. Springer, Cham. pp 169-184.
 25. Smirnov, O., Kuznetsov, A., Potii, O., Poluyanenko, N., Stelnyk, I., Mialkovsky, D. «Combining and filtering

- functions in the framework of nonlinear-feedback shift register». International Journal of Computing; 2020, Volume 19, Issue 2 – Research Institute for Intelligent Computer Systems – 2020. – P. 247-256.
26. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
27. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177.
28. Smirnov, O., Shekhanin, K., Kuznetsov, A., Krasnobayev, V. «Detecting Hidden Information in FAT». International Journal of Computer Network and Information Security (IJCNIS). Vol. 12, No. 3, 2020. PP.33-43.
29. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645.
30. Smirnov O. Kuznetsov A., Zaichenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019; Odessa; Ukraine; 9-13 September 2019. P.22-28.
31. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.

УДК 004

Я.Рябовол, магістр гр. КІ-24М,*Центральноукраїнський національний технічний університет*

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ВІРТУАЛІЗАЦІЇ ОБ'ЄДНАНИХ КОМУНІКАЦІЙ У МЕРЕЖІ

У статті розроблено програмне забезпечення, яке призначено для системи віртуалізації об'єднаних комунікацій у мережі. Метою розробки є дослідження та принципи побудови системи віртуалізації об'єднаних комунікацій у мережі. Об'єктом дослідження є процес віртуалізації об'єднаних комунікацій у мережі. Предметом дослідження є методи віртуалізації об'єднаних комунікацій у мережі. Методи дослідження базуються на методах теорії побудови комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи віртуалізації об'єднаних комунікацій у мережі. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

віртуалізація, об'єднані комунікації, мережа

Постановка проблеми. Уніфіковані комунікації (UC) – це інтеграція двох або більше систем зв'язку в реальному часі в одну платформу. Інтеграція основних систем зв'язку в одну загальну систему корпоративного рівня забезпечує більше, ніж просто економію коштів. Ці інтерактивні послуги та програми зв'язку в реальному часі через Інтернет-протокол (IP) стали критично важливими для підвищення доступності та ефективності співробітників, покращення підтримки клієнтів та сприяння гнучкості бізнесу. Однак деякі малі та середні підприємства (МСБ) ще далекі від впровадження цього рішення через високу вартість початкового розгортання та постійної підтримки. Хмарне рішення UC, UC як послуга (UCaaS), зараз саме по собі є технологією, що розвивається, на ринку та здійснило революцію в IT-індустрії, будучи потужною платформою, на яку багато компаній обирають перенести свої локальні рішення UC. Рішення UCaaS має потенціал для зменшення капітальних та операційних витрат, пов'язаних з власним розгортанням UC.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи віртуалізації об'єднаних комунікацій у мережі.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи віртуалізації об'єднаних комунікацій у мережі.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем віртуалізації об'єднаних комунікацій у мережі.
- Дослідження системи віртуалізації об'єднаних комунікацій у мережі.
- Програмна реалізація системи віртуалізації об'єднаних комунікацій у мережі.

Об'єктом дослідження є процес віртуалізації об'єднаних комунікацій у мережі.

Предметом дослідження є методи віртуалізації об'єднаних комунікацій у мережі.

Методи дослідження базуються на методах теорії побудови комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Стек уніфікованих комунікацій став стратегічною екосистемою для співпраці підприємств. Йдеться вже не про вибір інструментів, а про створення рішень уніфікованих комунікацій, які відповідають вашим робочим процесам, вимогам клієнтів і планам зростання.

Основні компоненти:

- UCaaS (Уніфіковані комунікації як послуга): основа, що інтегрує голос, відео та обмін повідомленнями.
- Технології для переговорних кімнат: розумні пристрої та системи для гібридної співпраці.
- Управління проектами: Інструменти робочого процесу, інтегровані в комунікаційні платформи.
- CCaaS: Контакт-центри на базі штучного інтелекту для покращення взаємодії з клієнтами.
- CPaaS: API для налаштованих робочих процесів комунікації.

У сучасному цифровому робочому середовищі уніфіковані комунікації (UC) забезпечують набагато більше, ніж просто консолідовані комунікації. Сучасні платформи UC призводять до фундаментальної трансформації того, як працюють та досягають успіху бізнеси.

Оптимізація витрат та рентабельність інвестицій

Економія коштів є ключовою перевагою сучасного впровадження уніфікованих комунікацій (UC). Організації відмовляються від значних капіталовкладень у локальні системи на користь гнучких хмарних рішень, які пропонують передбачувані операційні витрати. Переваги уніфікованих комунікацій виходять за рамки зниження накладних витрат на ІТ. Вони також максимізують існуючі технологічні інвестиції завдяки розумним інтеграціям. Компанії, що впроваджують UC, постійно повідомляють про значну економію на транспортних витратах та витратах на енергію завдяки консолідованій інфраструктурі.

Удосконалення цифрового робочого місця

Покращення робочого місця стало центральним елементом ціннісної пропозиції UC. Сучасні платформи використовують штучний інтелект для надання таких функцій, як переклад у режимі реального часу, автоматична транскрипція та інтелектуальне шумозаглушення. Ці інструменти створюють безперебійний досвід співпраці, незалежно від того, чи працюють співробітники з дому, в офісі чи в дорозі. Сучасні платформи UC також надають інформацію про моделі роботи та час, який вони витрачають на зосередження уваги, підтримуючи добробут співробітників так, як це ніколи не могли зробити традиційні засоби комунікації.

Можливості бізнес-аналітики

Аналітика вирізняє найкращі рішення для уніфікованих комунікацій. Тепер організації можуть аналізувати моделі комунікації для оптимізації робочих процесів та вимірювання ефективності зустрічей. Ці аналітичні дані допомагають керівникам приймати обґрунтовані рішення щодо використання інструментів та стратегій співпраці в команді, сприяючи постійному вдосконаленню способів виконання роботи.

Безпека та відповідність вимогам

Обидві концепції значно еволюціонували в платформах UC. Архітектура нульової довіри та наскрізне шифрування захищають конфіденційні комунікації, тоді як розширений захист від загроз оберігає від складних кіберзагроз. Найновіші рішення UC також спрощують дотримання вимог щодо функцій автоматичного запису та архівування, що є надзвичайно важливим для регульованих галузей.

Трансформація клієнтського досвіду

Покращення клієнтського досвіду (CX) за допомогою уніфікованих комунікацій (UC) створює конкурентні переваги. Сучасні платформи забезпечують безперебійну омніканальну підтримку, що посилюється завдяки чат-ботам на базі штучного інтелекту та аналізу настроїв. Організації тепер можуть відстежувати шлях клієнтів по каналах та забезпечувати послідовну, високоякісну взаємодію на кожній точці контакту.

Гнучкість та масштабованість

Мабуть, найголовніше, що сучасні уніфіковані комунікації забезпечують інфраструктуру, готову до майбутнього. Організації можуть легко інтегрувати новітні

технології, такі як AR/VR для захопливої співпраці або пристрої Інтернету речей для інтелектуальних рішень на робочому місці. Архітектури, що в першу чергу базуються на API, дозволяють створювати індивідуальні інтеграції, адаптовані до унікальних потреб бізнесу, а регулярні оновлення функцій гарантують, що системи залишатимуться актуальними без серйозних переробок.

Уніфіковані комунікації (UC) – це не просто черговий IT-проект. Це основа цифрової трансформації. Компанії, які правильно це роблять, не просто покращують комунікації – вони переосмислюють те, як виконується робота.

Ця еволюція показує, як уніфіковані комунікації (UC) перетворилися з простих інструментів комунікації на інтелектуальні платформи, що сприяють цифровій трансформації та підтримують сучасні моделі роботи. Зі зростанням технологій UC залишатиметься центральним елементом успіху бізнесу, дозволяючи організаціям адаптуватися та процвітати у все більш цифровому світі.

Ландшафт уніфікованих комунікацій розвивається з шаленою швидкістю, зумовлений інноваціями штучного інтелекту, вимогами гібридної роботи та зміною очікувань співробітників. Для керівників підприємств, які орієнтуються в цьому динамічному середовищі, розуміння цих головних тенденцій – це не просто бути в курсі подій, а отримання конкурентної переваги завдяки покращеній співпраці та комунікації.

Агенти зі штучним інтелектом та інші пілоти

Корпоративні команди запрошують помічників зі штучним інтелектом у свої щоденні робочі процеси. Ці цифрові команди виконують все: від планування зустрічей до забезпечення перекладу в режимі реального часу. Copilot від Microsoft та AI Companion від Zoom демонструють, як агенти зі штучним інтелектом розширюють людські можливості, підвищуючи продуктивність та зменшуючи навантаження від рутинних завдань.

Генеративний ШІ

GenAI революціонує створення контенту та комунікацію. Великі мовні моделі тепер допомагають складати електронні листи, підсумовувати зустрічі та створювати документацію. Підприємства використовують цю технологію для масштабування комунікацій, зберігаючи при цьому узгодженість та якість у всіх каналах.

Гібридне/сучасне робоче місце

Еволюція гібридної роботи вимагає більш складних рішень для уніфікованих комунікацій (UC). Організації шукають платформи, які забезпечують безперебійний досвід роботи вдома, в офісі та в мобільному середовищі. Акцент зміщується на створенні рівності між віддаленими та офісними учасниками за допомогою розширених функцій співпраці.

Інтеграції та API

Платформи уніфікованих комунікацій стають центральними нервовими системами для бізнес-операцій. Відкриті API та системи CPaaS дозволяють створювати налаштовані робочі процеси та глибоку інтеграцію з основними бізнес-додатками. Ця взаємопов'язаність руйнує ізолюваність та створює уніфікований цифровий досвід, що підвищує продуктивність.

Сучасні конференц-зали

Фізичні простори для зустрічей перетворюються на розумні центри співпраці. Камери на базі штучного інтелекту, просторовий звук та цифрові дошки створюють захопливий досвід, який скорочує розрив між учасниками, що присутні особисто, та учасниками, які працюють віддалено. Посилюється увага до створення рівноправних гібридних вражень.

Міграція в хмару

Заміна застарілих систем триває, оскільки організації переходять на хмарні рішення для уніфікованих комунікацій (UC), а термін дії контрактів на COVID закінчується. Сучасні платформи UCaaS пропонують підвищену гнучкість, масштабованість та інноваційний потенціал. Підприємства надають пріоритет хмарній міграції, щоб забезпечити майбутнє своєї комунікаційної інфраструктури.

Відповідність

Нормативні вимоги стають складнішими, особливо щодо захисту та безпеки даних. Постачальники уніфікованих систем реагують на це розширеними функціями забезпечення відповідності, включаючи складні політики зберігання даних, журнали аудиту та засоби контролю за суверенітетом даних. Це стає критично важливим для регульованих галузей та глобальних операцій.

Гібридна безпека робочого місця

Проблеми безпеки розвиваються разом із розподіленою робочою силою. Архітектури нульової довіри, наскрізне шифрування та розширений захист від загроз стають стандартом. Посилюється увага до безпеки зв'язку між кількома пристроями та місцями без шкоди для зручності користувача.

Досвід співробітників

Платформи уніфікованих комунікацій дедалі більше зосереджуються на добробуті та залученості. Інструменти для вимірювання цифрової втоми, заохочення здорових моделей роботи та сприяння інклюзії стають важливими. Акцент зміщується з чистої продуктивності на практики сталої співпраці.

Залучення клієнтів

Інтеграція UC з платформами взаємодії з клієнтами (найчастіше з рішеннями CCaaS) створює безперервну омніканальну взаємодію. Маршрутизація на базі штучного інтелекту, аналіз настроїв та автоматизовані відповіді підвищують ефективність обслуговування клієнтів. Зростає увага до створення узгодженого, персоналізованого досвіду на всіх точках контакту.

Захопиви враження

Межа між фізичною та цифровою співпрацею розмивається, оскільки платформи уніфікованих комунікацій (UC) впроваджують технології розширеної реальності (XR) – уявіть, що ви бачите статус членів команди, терміни проєктів та нотатки до зустрічей, що пливуть у вашому полі зору. Провідні постачальники UC вже інтегрують можливості просторових обчислень, а такі рішення, як Microsoft Mesh, демонструють, як аватари та 3D-простори можуть зробити віддалену співпрацю природною.

Штучний інтелект та доповнена реальність (AR) – це не просто функції сучасних уніфікованих комунікацій, це фундаментальні зміни в тому, як ми співпрацюватимемо. Уявіть собі зустрічі, де мовні бар'єри миттєво зникають, а віддалені учасники відчують фізичну присутність завдяки розумним окулярам. Це не наукова фантастика – зараз 2025 рік.

Вибір правильного рішення для уніфікованих комунікацій (UC)

Сучасним підприємствам потрібно зробити більше, ніж просто визначити уніфіковані комунікації в їхньому нинішньому вигляді. Їм потрібно визначити, що вони насправді для них означають і як вони збираються розгортати правильні системи. Наш великий каталог уніфікованих комунікацій може допомогти у визначенні постачальників. Але вам також потрібна дорожня карта.

Спочатку визначте свої вимоги

Основа успішного вибору UC починається з розуміння унікальних потреб вашої організації. Почніть з визначення поточних моделей комунікації та проблемних точок у різних відділах. З якими комунікаційними проблемами команди стикаються щодня?

Які робочі процеси потребують оптимізації? Задokumentуйте конкретні варіанти використання, від базової співпраці в команді до складних взаємодій з клієнтами. Це створює ваші базові вимоги та допомагає уникнути надмірних інвестицій у непотрібні функції.

Оцініть свою інфраструктуру

Перш ніж вибрати платформу UC, оцініть свою технічну базу. Сучасні рішення UC вимагають надійної мережевої інфраструктури для підтримки відеоконференцій та співпраці в режимі реального часу. Враховуйте підключення вашого глобального офісу, вимоги до мобільної робочої сили та існуючі інвестиції в обладнання. Зверніть особливу увагу на

вимоги до інтеграції з вашими основними бізнес-додатками – найкраще рішення УС буде безперервно працювати з вашим існуючим технологічним стеком.

План зростання

Хоча вирішення сьогоднішніх завдань є важливим, ваша платформа УС повинна підтримувати потреби завтрашнього дня. Подумайте, як ваші комунікаційні вимоги можуть розвиватися протягом наступних трьох-п'яти років. Шукайте платформи, що пропонують масштабовані моделі ліцензування та гнучкі варіанти розгортання. Регулярні оновлення функцій та потужні можливості API свідчать про те, що постачальник прагне інновацій. Чітка дорожня карта продукту допомагає вам узгодити вашу довгострокову бізнес-стратегію з еволюцією платформи.

Найкраща платформа уніфікованих комунікацій не завжди та, що має найбільше функцій. Успіх полягає у відповідності технологій унікальній ДНК вашої організації. Почніть зі своїх робочих процесів, а не зі списку функцій.

Безпека та відповідність вимогам

У сучасному цифровому середовищі безпека не може бути другорядною. Сучасні платформи уніфікованих комунікацій повинні балансувати між доступністю та надійним захистом. Оцініть підхід кожного постачальника до зберігання даних, шифрування та автентифікації. Для регульованих галузей сертифікація відповідності не підлягає обговоренню. Адміністративний контроль та комплексні можливості моніторингу допомагають підтримувати безпеку без шкоди для зручності використання.

Практичне оцінювання

Просто читання списків функцій та перегляду демонстрацій недостатньо. Скористайтесь можливостями підтвердження концепції, що пропонуються основними постачальниками УС. Протестуйте платформу у своєму середовищі, зберіть відгуки потенційних користувачів та перевірте можливості інтеграції. Цей практичний досвід показує, як рішення працює в реальних умовах, і допомагає виявити потенційні проблеми впровадження.

Розуміння загальної вартості

Справжня вартість платформи УС виходить за рамки щомісячної плати за кожного користувача. Враховуйте послуги з впровадження, вимоги до навчання та потенційні оновлення мережі. Враховуйте поточні витрати на управління та будь-які додаткові модулі, які вам можуть знадобитися. Не забудьте зрозуміти витрати на вихід – що знадобиться для переходу на платформу, якщо це буде потрібно? Такий комплексний огляд допомагає уникнути бюджетних несподіванок.

Оберіть правильного партнера

Успіх залежить як від постачальника, так і від технології. Шукайте партнерів, які демонструють фінансову стабільність та сильний інноваційний досвід. Оцініть їхню репутацію в сфері підтримки клієнтів та стан спільноти користувачів. Регулярні оновлення платформи свідчать про постійні інвестиції, а чіткі плани забезпечення безперервності бізнесу демонструють довгострокову відданість.

Пам'ятайте, що ідеальне рішення для уніфікованих комунікацій (УС) відповідає вашим конкретним потребам, бюджету та планам зростання. Приділіть час ретельній оцінці варіантів відповідно до ваших вимог, а не просто вибирайте лідера ринку чи найдешевший варіант. Ваш вибір впливатиме на щоденну діяльність протягом багатьох років – зробіть його важливим.

Успішне впровадження уніфікованих комунікацій вимагає стратегічного планування та бездоганного виконання. Ось як зробити це правильно:

Розумна оцінка

Вивчіть свої поточні робочі процеси та проблемні точки, перш ніж вибирати інструменти уніфікованих комунікацій. Зосередьтеся на рішеннях, які покращують існуючі процеси, а не нав'язують непотрібні зміни. Відобразіть шляхи користувачів, щоб визначити критичні точки інтеграції.

Зміна лідерства

Створіть ентузіазм завдяки чіткій комунікації щодо переваг УС. Визначте лідерів відділу, які можуть продемонструвати свої досягнення та підтримати колег. Створіть структурований план впровадження з вимірюваними етапами впровадження.

Безшовна інтеграція

Забезпечте гармонійну роботу вашої платформи УС з основними бізнес-інструментами. Надайте пріоритет рішенням, що пропонують надійні API та попередньо вбудовані інтеграції. Ретельно протестуйте у вашому середовищі перед повним розгортанням.

Розширення прав і можливостей користувачів

Надайте різноманітні варіанти навчання – від коротких відеоуроків до практичних семінарів. Створіть ресурси з можливістю пошуку для поширених запитань. Виміряйте моделі використання, щоб визначити, де потрібна додаткова підтримка.

Безпека та відповідність

Впроваджуйте безпеку з нульовою довірою з першого дня. Увімкніть такі функції, як єдиний вхід та наскрізне шифрування, за замовчуванням. Документуйте заходи щодо відповідності вимогам, особливо для регульованих галузей. Регулярні аудити безпеки захищають системи.

Управління змінами – ваша секретна зброя. Я бачив, як технічно ідеальні розгортання зазнавали невдачі, бо забували про людський фактор. Спочатку завоюйте серця та розуми, а потім впроваджуйте технології.

Ключ до успіху УС полягає в тому, щоб ставитися до нього як до бізнес-трансформації, а не просто до технологічного оновлення. Зосередьтеся на взаємодії з користувачем, зберігаючи при цьому безпеку та відповідність вимогам корпоративного рівня.

Проблеми впровадження УС: критичні питання, на які слід звернути увагу

Сучасні розгортання УС стикаються з кількома ключовими проблемами:

Продуктивність мережі:

Мультимедійні комунікації вимагають надійної інфраструктури. Організаціям потрібна достатня пропускна здатність і низька затримка для якісних відеодзвінків і співпраці в режимі реального часу. Впроваджуйте політики QoS, щоб пріоритезувати УС-трафік і оптимізувати продуктивність мережі для гібридних робочих сценаріїв.

Складність інтеграції

Сучасні платформи уніфікованих комунікацій повинні безперебійно працювати з різноманітними бізнес-інструментами та застарілими системами. Обирайте рішення з потужними можливостями API та підтримкою відкритих стандартів. Уникайте прив'язки до постачальника, надаючи пріоритет сумісності та гнучкості для майбутніх потреб.

Безпека та конфіденційність

Платформи уніфікованих комунікацій об'єднують конфіденційні комунікації, створюючи нові виклики безпеці. Впроваджуйте:

- Архітектура безпеки з нульовою довірою.
- Наскрізне шифрування.
- Детальний контроль доступу.
- Регулярні аудити безпеки.
- Моніторинг відповідності.

Досвід користувача

Успіх залежить від безпроблемного впровадження користувачами. Зосередьтеся на:

- Інтуїтивно зрозумілі інтерфейси на різних пристроях.
- Очистіть шляхи міграції зі застарілих інструментів.
- Комплексне, але цілеспрямоване навчання.
- Помітні швидкі перемоги для стимулювання впровадження.

- Регулярний збір відгуків.

Еволюція технологічного стеку

Слідкуйте за швидкими інноваціями в уніфікованих комунікаціях:

- Можливості інтеграції штучного інтелекту.
- Хмарно-орієнтовані архітектури.
- Підтримка периферійних обчислень.
- Розширена аналітика.
- Функції автоматизації.

Організації, які проактивно вирішують ці виклики, зберігаючи при цьому зосередженість на бізнес-цілях, забезпечують собі успіх у сфері уніфікованих комунікацій (UC). Регулярна оцінка та коригування вашої стратегії уніфікованих комунікацій забезпечує постійне узгодження з потребами, що змінюються

Якщо ви коли-небудь пробували придбати технологію об'єднаних комунікацій, ви вже знаєте: варіантів не бракує. Те, що починається як просте «нам потрібен кращий спосіб спілкування та зустрічей», швидко перетворюється на плутанину аббревіатур, інструментів, що дублюються, та заяв постачальників, які звучать однаково.

Саме тому ми створили наші посібники з UC Marketplace, щоб допомогти вам приймати рішення швидше та з більшою впевненістю.

Почніть з платформи

Ваша платформа UC або об'єднує все разом, або заважає. Це рівень, де працюють голосові, відео, чат та інтеграції, часто поєднані з нескінченними інструментами для співпраці та іншими програмами.

Деякі компанії схилиються до очевидних назв, таких як Microsoft Teams, Zoom, Webex. Іншим потрібен більший контроль, інше ліцензування або щось, що краще поєднується з їхніми існуючими інструментами.

- Найкращі постачальники платформ UC.
- Найкращі постачальники UCaaS.

Оберіть інструменти для співпраці, які відповідають вашій команді

Зустрічі вже не такі, як раніше, і це не погано. Сучасним командам потрібна гнучкість: люди вдома, люди в офісі, а часто й ті, й інші одночасно. Програмне забезпечення, яке ви використовуєте для об'єднання цих людей, має більше значення, ніж будь-коли.

Йдеться не лише про вибір найкращих платформ для зустрічей. Вам потрібно подумати про те, як ви можете підтримати гібридні команди, які хочуть використовувати власні платформи для зустрічей, та обладнати свої приміщення правильним обладнанням та інструментами.

- Постачальники гібридних платформ для зустрічей.
- Найкращі рішення для самостійного придбання власного майна (BYOM).
- Найкращі пристрої та кінцеві точки UC.
- Найкращі пристрої та комплекти для кімнат для переговорів.

Опанування обладнання для конференц-залів

Навіть у гібридному світі люди все ще зустрічаються в кімнатах, і коли це відбувається, процес має працювати безперебійно. Занадто часто це не так. Мікрофони випадають, екрани зависають, чиєсь обличчя розміром з поштову марку. Правильне обладнання вирішує все це. Вам не потрібно переборщувати. Але вам потрібно відповідати розміру вашої кімнати, вашому використанню та наявній конфігурації.

Ми розбили це за розміром кімнати:

- Найкращі постачальники послуг для великих конференц-залів.
- Найкращі постачальники середніх конференц-залів.
- Провідні рішення для невеликих конференц-залів.

Інструменти для управління всім

Щойно ваша платформа налаштована, хтось має підтримувати її роботу. Саме тут і стають у пригоді інструменти керування послугами UC. Вони допомагають із забезпеченням, моніторингом, підтримкою користувачів та середовищами з кількома постачальниками, які не завжди добре взаємодіють одне з одним одразу після встановлення.

Якщо ви керуєте проектами та комунікаціями одночасно? Вам також знадобляться інструменти, які чітко інтегруються з вашим стеком уніфікованих комунікацій.

- Найкращі постачальники послуг управління UC.
- Найкращі платформи для управління проектами.

Поєднання точок: CCaaS та CPaaS

Уніфіковані комунікації швидко стають все більш узгодженими з ширшим технологічним стеком. Якщо ви керуєте контакт-центром або створюєте індивідуальні способи зв'язку з клієнтами, саме тут на допомогу приходять CCaaS та CPaaS.

- Найкращі постачальники CCaaS.
- Найкращі постачальники CPaaS.

Безпека, відповідність вимогам та інфраструктура за лаштунками

Контролери меж сеансів, інструменти для забезпечення відповідності вимогам та системи SIP-транкінгу для хмарного голосового зв'язку легко не помітити, але вони відіграють величезну роль у вашому технологічному стеку. Якщо ви керуєте корпоративним голосовим зв'язком, ці постачальники забезпечують чудові результати:

- Найкращі постачальники SBC.
- Інструменти безпеки та відповідності UC.
- Найкращі постачальники SIP-транкінгу.

Майбутнє UC: як штучний інтелект, XR та периферійні обчислення трансформують бізнес-комунікації до 2030 року

Платформи, які ми використовуємо сьогодні, перетворюються на невидимі, адаптивні системи, які передбачають наші потреби, оптимізують нашу взаємодію та розмивають межу між цифровим та фізичним простором. Для підприємств завдання зрозуміле: впроваджувати ці інновації з балансом безпеки, масштабу та орієнтації на людину. Ось що відбудеться і що це означає для вашої стратегії.

Інтелектуальний зв'язок

Наступне покоління платформ уніфікованих комунікацій (UC) буде визначатися інтеграцією штучного інтелекту. Розумні помічники керуватимуть рутинними завданнями, такими як планування, ведення нотаток та подальші дії, звільняючи людей від зосередження на змістовній взаємодії.

Переклад і транскрипція в режимі реального часу стануть стандартом, долаючи мовні бар'єри в глобальному бізнесі. Штучний інтелект аналізуватиме моделі комунікації для оптимізації робочих процесів і прогнозування потреб, а розумні звіти про зустрічі автоматично генеруватимуть корисну інформацію.

Захопиви враження

Розширена реальність змінить те, як ми співпрацюємо віддалено. Віртуальні простори для зустрічей замінять традиційні відеодзвінки, забезпечуючи природну взаємодію у спільних цифрових середовищах. Цифрові двійники дозволять практичну співпрацю за допомогою 3D-моделей та візуалізацій даних.

Розумні окуляри Ray-Ban від Meta пропонують уявлення про це майбутнє – де окуляри з підтримкою доповненої реальності (AR) проектуватимуть віртуальні дисплеї, перекладатимуть розмови в режимі реального часу та покращуватимуть зустрічі за допомогою цифрових накладок. Уявіть, що ви дивитеся на стіл колеги та бачите його статус доступності, що ширяє над ним, або перетворюєте будь-яку стіну на віртуальний простір для співпраці. Ці інструменти занурення зроблять віддалену співпрацю такою ж ефективною, як і перебування в одній кімнаті.

Інновації в периферійних обчисленнях

Архітектура периферійних обчислень революціонізує продуктивність уніфікованих комунікацій (UC). Обробляючи дані ближче до користувачів, периферійні обчислення забезпечують майже нульову затримку для взаємодії в режимі реального часу та покращену якість відео.

Такий розподілений підхід підвищує надійність у зонах з низькою пропускну здатністю та забезпечує безперешкодний перехід між пристроями. Можливості периферійних мереж будуть вирішальними для підтримки розширених функцій, таких як накладання доповненої реальності та обробка штучним інтелектом, зберігаючи при цьому швидкість реагування.

Оточення інтелекту

Майбутні робочі простори будуть інтелектуально адаптуватися до наших комунікаційних потреб. Розумні кімнати автоматично налаштовуватимуть освітлення, акустику та конфігурації дисплеїв для оптимального проведення зустрічей. Будь-яка поверхня може стати простором для співпраці завдяки проєктованим інтерфейсам.

Контекстно-залежні системи керуватимуть сповіщеннями та пріоритетами на основі активності та уподобань користувача, тоді як датчики навколишнього середовища забезпечуватимуть оптимальний комфорт для продуктивності. Інструменти комунікації стануть майже невидимими, вплетеними в модні окуляри та предмети повсякденного вжитку, що зробить уніфіковані комунікації більш природними та менш залежними від технологій.

Еволюція безпеки

Оскільки платформи уніфікованих комунікацій стають складнішими, безпека повинна розвиватися паралельно. Квантово-стійке шифрування захищатиме від нових загроз, а біометрична автентифікація стає нормою.

Архітектура нульової довіри буде стандартною, а системи на базі штучного інтелекту постійно відстежуватимуть потенційні порушення безпеки. Автоматизовані інструменти відповідності забезпечать дотримання правил захисту даних, що постійно змінюються, у всіх глобальних операціях.

До 2030 року уніфіковані комунікації (UC) стануть невидимими, але всюдисущими. Уявіть, що ви заходите в кімнату та миттєво зв'язуєтесь зі своєю глобальною командою за допомогою амбієнтних обчислень та доповненої реальності (AR). Технології відходять на другий план, а співпраця займає центральне місце.

Ландшафт уніфікованих комунікацій (UC) у 2030 році буде різнобарвним від сьогодення. Успіх залежатиме від балансу інноваційних функцій з безпекою, конфіденційністю та користувацьким досвідом. Організації, які впроваджують ці новітні технології, зберігаючи при цьому зосередженість на практичних потребах бізнесу, матимуть найкращі можливості для процвітання в цю нову еру комунікацій.

Найпотужніші платформи UC будуть не тими, що мають найбільше функцій, а тими, які ви ледве помітите, бо вони працюють настільки інтуїтивно, що ви навіть забудете про їхнє існування.



Рисунок 1 – Структурна схема системи

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів віртуалізації об'єднаних комунікацій у мережі.

Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем віртуалізації об'єднаних комунікацій у мережі.
- Досліджена система віртуалізації об'єднаних комунікацій у мережі.
- На основі отриманих результатів досліджень створена програмна реалізація системи віртуалізації об'єднаних комунікацій у мережі.

Розроблені алгоритми дозволяють успішно вирішувати завдання віртуалізації об'єднаних комунікацій у мережі. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Kuznetsov, O., Frontoni, E., Kryvinska, N., Chevardin, V., Smirnov, O. «Wireless Network Encryption Stream Ciphers, Computational Modeling, and Security Analysis». Computational Modeling and Simulation of Advanced Wireless Communication Systems, 2024, pp. 379–402.
2. Kuznetsov, O., Frontoni, E., Kryvinska, N., Smirnov, O., Imoize, G.L. «Computational Modeling of Enhanced Spread Spectrum Codes for Asynchronous Wireless Communication». Computational Modeling and Simulation of Advanced Wireless Communication Systems, 2024, pp. 403–447.
3. Смірнова Т.В., Коноплицька-Слободенюк О.К., Буравченко К.О., Смірнов С.А., Кравчук О.В., Козірова Н.Л., Смірнов О.А. «Дослідження технологій забезпечення кібербезпеки хмарних сервісів IaaS, PaaS та SaaS». Кібербезпека: освіта, наука, техніка. 2024. №4(24), С. 6-27.
4. Батрак О., Смірнова Т., Гнатюк В., Одарченко Р., Смірнов О. «Дослідження показників ефективності функціонування та перспектив розвитку систем ІР-телефонії». Підводні технології, 2024, № 13, с. 28-35.
5. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». Advanced Information Systems, 2023, 7(2), pp. 49-56.
6. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchey, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». CEUR Workshop Proceedings, Volume 3530, 2023, pp. 256-265.
7. Smirnov, O., Odarchenko, R., Smirnova, T., Bondar, S., Volosheniuk, D. «Optimal Structure Construction of Private 5G Network for the Needs of Enterprises». Lecture Notes on Data Engineering and Communications Technologies, 2023, 178, pp. 208–223.
8. Аль-Мудхафар Акіл Абдулхуссейн М., Смірнова Т.В., Буравченко К.О., Смірнов О.А. «Метод оцінки та підвищення користувацького досвіду абонентів в програмно-конфігурованих мережах на основі використання машинного навчання». Сучасні інформаційні системи, 2023, том 7, № 2, С. 49-56.
9. Smirnov, O., Neskoriyeva, T., Fedorov, E., Rudakov, K., Neskoriyeva, A. «Method Detection Audit Data Anomalies on Basis Restricted Cauchy Machine» CEUR Workshop Proceedings, Volume 3187, 2022,
10. Smirnov O., Smirnova T., Anas M. Al-Oraiqat, Drieiev O., Polishchuk L., Sheroz Khan, Yassin M. Y. Hasan, Aladdein M. Amro, Hazim S. AlRawashdeh «Method for Determining Treated Metal Surface Quality Using

- Computer Vision Technology». Sensors (Basel, Switzerland) Volume 22, Issue 16, 6223, 2022.
11. Smirnov O., Kuznetsov A., Kryvinska N., Kiian A., Kuznetsova K. «Full Non-Binary Constant-Weight Codes». SN Computer Science, Vol 2, 337, 2021. <https://doi.org/10.1007/s42979-021-00739-w>
 12. Smirnov O., Kuznetsov A., Zhora V., Onikiychuk A., Pieshkova O. «Hiding Messages in Audio Files Using Direct Spread Spectrum». 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2021, Cracow, Poland, 22-25 September 2021. P. 414-418.
 13. Smirnov O., Kuznetsov A., Lokotkova I., Kuznetsova T., Florov S., Lebid O. «Using Orthogonal Signals to Hide Information in Images». 4 IEEE International Conference on Advanced Information and Communication Technologies (AICT) - 2021, Lviv, Ukraine, September 21-25, 2021. P. 255-260.
 14. Smirnov, O., Kuznetsov, A., Potii, O., Poluyanenko, N., Stelnyk, I., Mialkovsky, D. «Combining and filtering functions in the framework of nonlinear-feedback shift register». International Journal of Computing; 2020, Volume 19, Issue 2 – Research Institute for Intelligent Computer Systems – 2020. – P. 247-256.
 15. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
 16. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». Journal of theoretical and applied information technology Vol.98. No 21, 2020, P. 3334-3346.
 17. Smirnov O., Kuznetsov A., Kovalchuk D., Kuznetsova T. «New technique for data hiding in cover images using adaptively generated pseudorandom sequences». CEUR Workshop Proceedings Volume 2654, 2020, Pages 1-14.
 18. Smirnov O., Kuznetsov A., Onikiychuk A., Makushenko T., Anisimova O., Arischenko A. «Adaptive pseudorandom sequence generation for spread spectrum image steganography». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 161-165.
 19. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177.
 20. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587.
 21. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». CEUR Workshop Proceedings Volume 2616, 2020, Pages 366-379.
 22. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645.
 23. Smirnov, O., Kuznetsov, A., Gorbacheva, L., Babenko, V., «Hiding data in images using a pseudo-random sequence», CEUR Workshop Proceedings Volume 2608, 2020, Pages 646-660.
 24. Zhurakovskiy, B., Tsopa, N., Batrak, Y., Odarchenko, R., Smirnova, T «Comparative analysis of modern formats of lossy audio compression». Workshop Proceedings, 2020, 2654, стр. 315-327.
 25. Smirnov O. Kuznetsov A., Zaichenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019; Odessa; Ukraine; 9-13 September 2019. P.22-28.
 26. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.
 27. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019 . P.517-522.
 28. Smirnov, O., Krasnobayev, V., Yanko, A., Kuznetsova, T. «Methods of nulling numbers in the system of residual classes». CEUR Workshop Proceedings, Vol 2588, P. 90-106, 2019.
 29. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Averchev, A., Pastukhov, M., Kuznetsova, K., «Formation of Pseudorandom Sequences with Special Correlation Properties», 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT -2019/ Lviv, Ukraine, 2-6 July, 2019, P. 395-399.
 30. Smirnov, O., Kuznetsov, A., Kavun, S., Babenko, B., Nakisko, O., Kuznetsova, K., «Malware Correlation Monitoring in Computer Networks of Promising Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 347-352.
 31. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Pastukhov, M., Kuznetsova, K., Prokopovych-Tkachenko, D., «Discrete Signals with Special Correlation Properties», CEUR Workshop Proceedings Volume 2353, CEUR Workshop Proceedings 2019, Pages 618-629.
 32. Smirnov A.A., Kuznetsov A.A., Danilenko D.A., Berezovsky A., «The statistical analysis of a network traffic for the intrusion detection and prevention systems», Telecommunications and Radio Engineering. – Volume 74, Issue 1. – Begel House Inc. – 2015. – P. 61-78.

УДК 004

О.Семенюк магістр гр. КІ-24М,

Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ЗБЕРІГАННЯ ДАНИХ SAN НА ОСНОВІ СТАНДАРТУ FC GEN

У статті розроблено програмне забезпечення, яке призначено для системи зберігання даних SAN на основі стандарту FC Gen. Метою розробки є дослідження та принципи побудови системи зберігання даних SAN на основі стандарту FC Gen. Об'єктом дослідження є процес зберігання даних SAN на основі стандарту FC Gen. Предметом дослідження є методи зберігання даних SAN на основі стандарту FC Gen. Методи дослідження базуються на методах теорії побудови комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи зберігання даних SAN на основі стандарту FC Gen. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

SAN, FC Gen

Постановка проблеми. У світі IT-інфраструктури сховище даних є критично важливим; саме там зберігаються дані, існують безпечні копії, і це основа продуктивності програм. Незалежно від того, скільки ядер процесора чи скільки пам'яті може мати сервер, кожен сервер очікує на дані.

Отже, сфера застосування цього середовища включає ранні дискові накопичувачі, стрічки для безпечного та економічно ефективного резервного копіювання даних, а також програмні реалізації, що забезпечують доступ, продуктивність та безпеку. Крім того, обов'язки адміністратора сховища включають захист копій даних за допомогою конфігурацій RAID або рішень для реплікації між сайтами.

Мантра адміністраторів сховищ: «одна копія будь-якого набору даних – це єдина точка відмови, яка чекає на катастрофу». Втрата даних ніколи не є прийнятним варіантом з точки зору програми.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи зберігання даних san на основі стандарту FC GEN.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи зберігання даних SAN на основі стандарту FC Gen.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем зберігання даних SAN на основі стандарту FC Gen.
 - Дослідження системи зберігання даних SAN на основі стандарту FC Gen.
 - Програмна реалізація системи зберігання даних SAN на основі стандарту FC Gen.
- Об'єктом дослідження є процес зберігання даних SAN на основі стандарту FC Gen.
Предметом дослідження є методи зберігання даних SAN на основі стандарту FC Gen.

Методи дослідження базуються на методах теорії побудови комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Протягом багатьох років стан середовищ зберігання даних в IT різко змінився. Короткий огляд змін проведе вас від ранніх стрічкових систем через еволюцію жорстких дисків (HDD) до розробки RAID-систем та корпоративних масивів. Однією з традиційно вірних речей було те, що сховища, засновані на структурних

блоках HDD, розвивалися повільно. Перехід від дисків зі швидкістю 5400 об/хв до дисків зі швидкістю 7200 об/хв як елемента продуктивності (більше даних під головою) за секунду знадобився десять років, щоб повністю заповнити центри обробки даних. Інші розробки включали щільність магнітної сигнатури на пластині диска та кількість пластин і головок на диск. Ця ретроспектива корисна лише тим, що вказує на те, що середовище зберігання даних в ІТ не розвивалося так швидко, як, скажімо, розробка процесорів або продуктивності та ємності пам'яті.

Ці розробки були в кремнії, а розробка накопичувачів була механічною. Як наслідок, закон Мура застосовувався до процесора та пам'яті, але не до сховища. Характер сховища почав змінюватися з появою твердотільних накопичувачів (SSD).

Спочатку прогрес був помірним. Блискучим кроком, що сприяв виходу на ринок, постачальники накопичувачів зробили платформу SSD такої ж форми/корпуса, як і існуючі жорсткі диски (HDD), з тими ж роз'ємами SCSI, SAS та SATA, що означало сумісність роз'ємів на серверній частині масиву для нової технології. Однак на ранніх етапах контролери корпоративних масивів та, у випадку вбудованих дискових накопичувачів у серверах, стек драйверів ОС не скористалися перевагами зміни продуктивності та інших характеристик дисків. Те, що стек ОС не використовував переваги нової технології, було однією з причин, чому ранні гібридні масиви, які використовували поєднання традиційних HDD та SSD-накопичувачів на серверній частині, були менш продуктивними, ніж очікували багато адміністраторів сховищ. Невідповідність очікуванням вплинула на рівень впровадження, і ІТ-організація не відчувала таких значних проблем з існуючими мережами зберігання даних, як очікувалося. Протягом понад 40 років в ІТ ми усуваємо вузькі місця в продуктивності процесора, швидкості/масштабу пам'яті, ємності/продуктивності сховища та швидкості мережі. Просте усунення одного вузького місця дозволяє знайти наступне, подібно до того, як розширення одного сегмента головної автомагістралі переміщує трафік до наступної вузької ділянки автомагістралі. В результаті багато клієнтів вважали, що приріст продуктивності порівняно з технологічними вартістю підходить лише для їхніх найвимогливіших застосувань.

Вартість за терабайт стала більш привабливою з появою середовища повністю флеш-масивів та вбудованих функцій, таких як стиснення, шифрування та дедуплікація. Крім того, новіші контролери корпоративних масивів були розроблені для характеристик продуктивності повністю флеш-пам'яті та значно збільшили як кількість операцій вводу/виводу за секунду (IOPS), так і затримку. До цього додалася щільність зберігання, яка дозволила їм об'єднати кілька стійок платформ HDD у часткову стійку SSD з перевагами зниження енергоспоживання та охолодження. Яким був наслідок? Спостерігається набагато швидший темп впровадження повністю флеш-масивів, які наразі становлять понад 70% від загального середовища поставок.

Цей технологічний зсув призводить до зміни вимог до проектування мереж зберігання даних, що актуально незалежно від використовуваної технології. Якщо очікується використання потужності та продуктивності цих платформ, то необхідно серйозно розглянути проектування.

Виділена інфраструктура мережі зберігання даних, яка забезпечує безвтратні, низькозатримкові, детерміновані, масштабовані та продуктивні послуги зберігання даних для програм, стає критично важливою. Адміністратори сховищ обговорюватимуть коефіцієнти розподілу даних для платформ зберігання, які являють собою кількість серверів та програм у мережі, що використовують певний масив або порт масиву для свого доступу до сховища.

Залежно від типів програм та їхніх потреб у продуктивності, це співвідношення може коливатися від невеликих одиниць до 40-50 серверів (сотень віртуальних машин). Як і в будь-якому сценарії забезпечення ресурсами, адміністратор сховища має справу з прогнозами того, скільки потужності та продуктивності використовуватиме будь-який сервер або програма. Але продуктивність програм є змінною; час доби, тиждень, місяць, а також сезонні або подіями викликають піки або падіння попиту на програми.

Ще один момент полягає в тому, що вся база програм не оновлюється одночасно. Типовий сценарій полягає в тому, що в середовищі одночасно існують кілька поколінь продуктивності. Наявність вікон обслуговування спонукає це до перепланування існуючих середовищ на нові сервери та сховища. Деякі застарілі програми можуть не мати середовища, яке працює під керуванням поточної операційної системи або версії програми. Одна може мати десятирічні або старіші операційні системи, підключені до НВА з двома або більше старішими поколіннями технологій. Як же тоді збалансувати цю все ще критично важливу програму з потребами та продуктивністю новіших машин?

Відповідь полягає в поєднанні топології, збалансованого виділення ресурсів, детального моніторингу та автоматизованого пом'якшення наслідків.

Найбільш гнучкою конфігурацією є топологія «ядро-край». Така архітектура дозволяє значне масштабування, зберігаючи при цьому низьку кількість переходів, тобто кількість передач даних з однієї платформи на іншу. Локальність підключення сховища для високопродуктивних програм – це міркування, яке спонукає деяких адміністраторів сховищ розміщувати порти сховища на тому ж блейд-сервері, комутаторі або групі портів, що й сервер програм. Однак така конструкція впливає на гнучкість ІТ-відділу для переміщення програми з однієї серверної платформи на іншу (не є тривіальним міркуванням у високо віртуалізованому середовищі, де платформи гіпервізора можуть часто переносити програми між серверними платформами).

Ще однією альтернативною топологією є повністю сітчаста конструкція; кожен комутатор має прямий ISL до кожного іншого комутатора в структурі. Повна сітчаста конструкція є проблематичною для середовищ з багатьма комутаторами, оскільки вона використовує цінні порти для ISL, які в іншому випадку використовувалися б для підключення серверів та сховища. Платформи Director мають міжшасі (ICL), що забезпечує виняткову пропускну здатність та масштабування між шасі без використання портів. Повна сітчаста конструкція гарантує, що жоден кінцевий пристрій не знаходиться на відстані більше одного переходу від будь-якого іншого кінцевого пристрою.

З точки зору продуктивності, важливо зазначити, що поява повністю флеш-центрів обробки даних також означає, що нові технології зберігання даних, засновані на продуктивності, ємності або обидва варіанти, з'являються з інтервалом від 18 до 24 місяців. Оновлення технологій не означає повну заміну існуючих платформ, а радше те, що ваша мережа зберігання даних повинна бути здатною вмістити приблизно дві такі ітерації за 4-5-річний цикл амортизації капіталу. Однією з переваг Fibre Channel SAN є подвійне резервування апаратного забезпечення та ізольований характер архітектур SAN. Архітектури тканин А та В передбачають, що жоден дефект пристрою, планове технічне обслуговування, випадкова подія людини чи зловмисна діяльність повністю не виведуть підключення до сховища з офлайн-режиму. Підтримка мережі сховища в режимі онлайн дозволяє безперебійне оновлення технологій, що стосується технологічних оновлень елементів мережі зберігання даних та підключеного сервера та сховища.

Однією з додаткових змін, необхідних для повністю флеш-центру обробки даних, є покращений моніторинг, частково завдяки зменшенню затримки, критичності даних та великої кількості даних, що передаються в сучасних SAN.

Процес планування SAN подібний до будь-якого процесу планування проекту та включає такі фази:

- Фаза I: Збір вимог.
- Фаза II: Розробка технічних специфікацій.
- Фаза III: Оцінка витрат на проект.
- Фаза IV: Аналіз рентабельності інвестицій (ROI) або загальної вартості володіння (TCO) (за необхідності).
- Фаза V: Створення детального плану проектування та впровадження SAN.

Вибираючи критерії, які слід відповідати, слід залучити користувачів, експертів з серверів та сховищ даних (SME) та інших відповідних експертів, щоб зрозуміти роль

структури. Оскільки більшість SAN працюють протягом тривалого часу, перш ніж їх оновлювати, врахуйте майбутнє зростання, оскільки SAN складні для реархітектури. Розгортання нових SAN або розширення існуючих для задоволення додаткових робочих навантажень у структурах вимагає критичної оцінки бізнес- та технологічних вимог. Правильна увага до планування забезпечить, щоб SAN після розгортання відповідала всім поточним та майбутнім бізнес-цілям, включаючи доступність, простоту розгортання, продуктивність, майбутнє зростання бізнесу та вартість.

Критичним аспектом успішного впровадження, який часто ігнорується, є постійне управління інфраструктурою. Визначення SME системного рівня для всіх компонентів, що складають SAN, та належне й актуальне навчання з цих компонентів має вирішальне значення для ефективного проектування та операційного управління інфраструктурою.

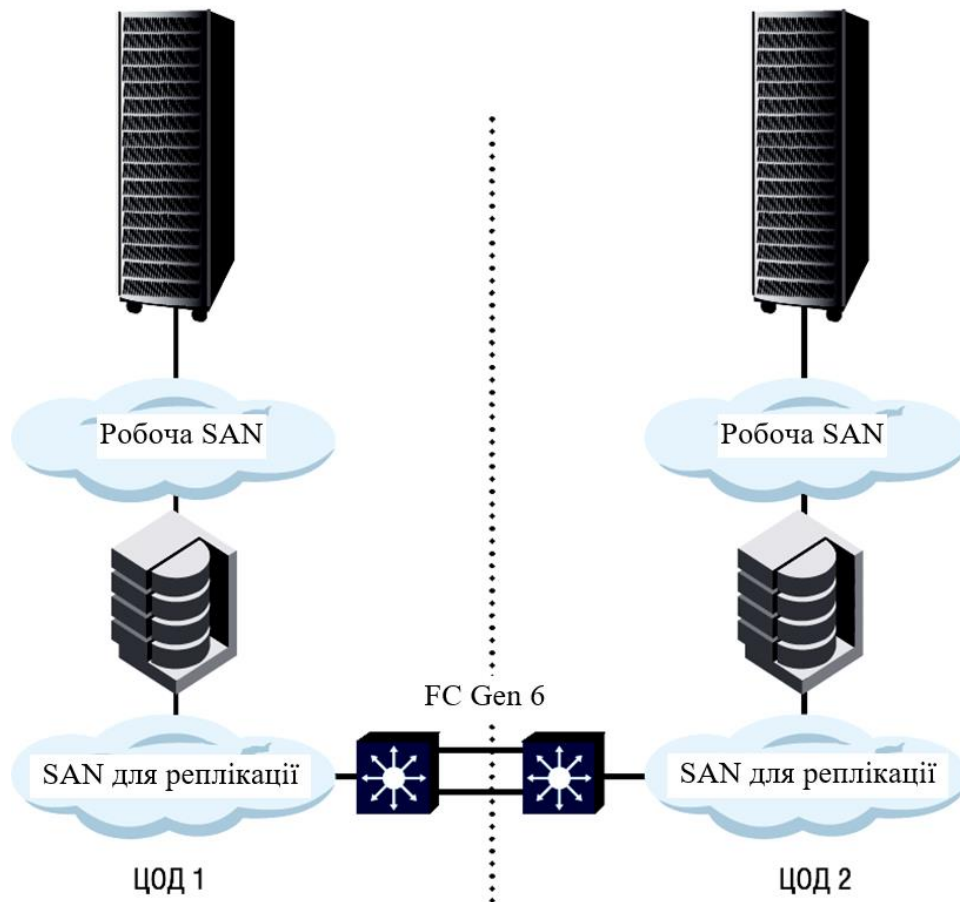


Рисунок 1 – Структурна схема системи

Під час проектування нової SAN або розширення існуючої SAN слід враховувати такі параметри:

1. Віртуалізація додатків:

– Які додатки працюватимуть у середовищі віртуальних машин (VM)?

– Скільки VM працюватиме на фізичному сервері?

– За яких умов VM будуть мігрувати (робочий та неробочий час; чи потрібен додатковий процесор або пам'ять для підтримки часу відгуку)?

– Чи є потреба в твердотільних носіях для покращення часу відгуку на читання?

2. Однорідні/неоднорідні серверні та сховищні платформи:

– Чи використовуються блейд-сервери чи стійкові сервери?

– Чи впроваджено автоматичне розподілення на рівні?

– Які версії Brocade Fabric OS® (FOS) підтримуються в середовищі зберігання даних від різних постачальників?

– Який запланований цикл оновлення серверів та платформ зберігання даних (2 роки або 3 роки)?

3. Масштабованість:

– Скільки портів користувачів потрібно зараз?

– Скільки пристроїв підключатиметься через шлюз доступу?

– Скільки ISL та Brocade UltraScale ICL потрібно для мінімізації перевантаження в мережі?

– Які відстані для з'єднань ISL та ICL потрібно підтримувати?

– Чи масштабується мережа на межі ядра?

4. Резервне копіювання та стійкість до аварій:

– Чи є централізоване резервне копіювання? (Це визначає кількість ISL, необхідних для мінімізації перевантаження при пікових навантаженнях.)

– Який вплив резервного копіювання на чутливі до затримки програми?

– Чи базується рішення для ліквідації аварій на міжміських ISL метрополітену FC чи на рішенні FC over Internet Protocol (FCIP)?

5. Діагностика та керованість:

– Який основний інтерфейс керування для SAN (CLI, Brocade SANnav або інструмент стороннього виробника)?

– Як часто оновлюватимуться Brocade FOS та SANnav?

– Як перевіряється цілісність кабелів та оптичних елементів?

6. Захист інвестицій:

– Чи потрібна підтримка для додавання комутаторів Gen 7 до структури Gen 6?

– Чи потрібна підтримка для технологій зберігання даних, таких як NVMe поверх структур?

– Яка підтримка сумісності пристроїв потрібна?

– Чи потрібна сумісність для інших технологій, таких як UCS?

Типова архітектура SAN складається з периферійних пристроїв, мережевих пристроїв та кабелів. Топологія зазвичай описується з точки зору взаємопов'язаних комутаторів, таких як згорнуте ядро, ядро-край та повна мережа. Рекомендована топологія SAN для оптимізації продуктивності, доступності, управління та масштабованості – це багаторівнева топологія "ядро-край". Підхід "ядро-край" забезпечує хорошу продуктивність без зайвих взаємозв'язків. На високому рівні багаторівнева топологія має велику кількість периферійних комутаторів, що використовуються для підключення пристроїв, та меншу кількість основних комутаторів, що використовуються для маршрутизації трафіку між периферійними комутаторами, як показано на рисунку 1.

Fibre Channel over Ethernet (FCoE) забезпечує передачу трафіку Fibre Channel по локальній мережі Ethernet. Інкапсуляція фреймів FC у кадри Ethernet дозволяє сполучати блоковий трафік систем зберігання з іншим трафіком LAN. У результаті спрощується мережна інфраструктура ЦОД і знижуються витрати, оскільки не потрібно обслуговувати кілька мереж. Однак, як вважають деякі фахівці, незалежно від того, яка технологія використовується, фабрика повинна працювати у виділеній мережі зберігання й ні про яку конвергенцію з мережею передачі даних не може бути мови – ризики переважають вигоди у вартості рішення.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів зберігання даних SAN на основі стандарту FC Gen. Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем зберігання даних SAN на основі стандарту FC Gen.

– Досліджена система зберігання даних SAN на основі стандарту FC Gen.

– На основі отриманих результатів досліджень створена програмна реалізація системи зберігання даних SAN на основі стандарту FC Gen.

Розроблені алгоритми дозволяють успішно вирішувати завдання зберігання даних SAN на основі стандарту FC Gen. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Smirnova, T., Gnatyuk, S., Yudin, O., Sydorenko, V., Polozhentsev, A., «The Model for Calculating the Quantitative Criteria for Assessing the Security Level of Information and Telecommunication Systems». CEUR Workshop Proceedings Volume 3156, 2022, Pages 390-399.
2. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». Проблеми інформатизації та управління, № 2(70). 2022. С. 28-37.
3. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 3(69). С. 93-98.
4. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Вісник Хмельницького національного університету. Серія: «Технічні науки», № 2 (307). С. 46-52. 2022.
5. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 1(67). С. 84-89.
6. Smirnova T., Gnatyuk S., Berdibayev R., Avkurova Zh., Iavich M. «Cloud-Based Cyber Incidents Response System and Software Tools». Communications in Computer and Information Science, 2021, vol 1486. Springer, Cham. pp 169-184.
7. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
8. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». Journal of theoretical and applied information technology Vol.98. No 21, 2020, P. 3334-3346.
9. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177.
10. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587.
11. Smirnov, O., Markovets, O. Vovk, N., Turchyn, Y., «Model of informational support for social network administrators' content creation». CEUR Workshop Proceedings Volume 2616, 2020, Pages 125-136.
12. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». CEUR Workshop Proceedings Volume 2616, 2020, Pages 366-379.
13. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645.
14. Smirnov O. Kuznetsov A., Zaichenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019; Odessa; Ukraine; 9-13 September 2019. P.22-28.
15. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.
16. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019 . P.517-522.
17. Smirnov, O., Odarchenko, R., Abakumova, A., Usik, P., Kundyzy, M., «QoE optimization technique for media delivery in 5G networks». 2019 IEEE International Scientific-Practical Conference Problems of

- Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019. P.597-601.
18. Smirnov, O., Krasnobayev, V., Yanko, A., Kuznetsova, T. «Methods of nulling numbers in the system of residual classes». CEUR Workshop Proceedings, Vol 2588, P. 90-106, 2019.
 19. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Averchev, A., Pastukhov, M., Kuznetsova, K., «Formation of Pseudorandom Sequences with Special Correlation Properties», 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT -2019/ Lviv, Ukraine, 2-6 July, 2019, P. 395-399.
 20. Smirnov, O., Kuznetsov, A., Kiian, A., Zamula, A., Rudenko, S., Hryhorenko, V., «Variance Analysis of Networks Traffic for Intrusion Detection in Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 353-358.
 21. Smirnov, O., Kuznetsov, A., Kavun, S., Babenko, B., Nakisko, O., Kuznetsova, K., «Malware Correlation Monitoring in Computer Networks of Promising Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 347-352.
 22. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Pastukhov, M., Kuznetsova, K., Prokopovych-Tkachenko, D., «Discrete Signals with Special Correlation Properties», CEUR Workshop Proceedings Volume 2353, CEUR Workshop Proceedings 2019, Pages 618-629.
 23. Smirnov A.A., Kuznetsov A.A., Danilenko D.A., Berezovsky A., «The statistical analysis of a network traffic for the intrusion detection and prevention systems», Telecommunications and Radio Engineering. – Volume 74, Issue 1. – Begel House Inc. – 2015. – P. 61-78.
 24. Смірнов О.А., Смірнова Т.В., Буравченко К.О., Кравченко С.С., Горбов В.О., «Хмарна система підтримки прийняття рішень технологічного процесу відновлення поверхонь конструкцій і деталей машин». Сучасні інформаційні системи. 2021. Т. 5, № 4. С. 79-95
 25. Смірнов О.А., Усік П.С., Миронець І.В., Буравченко К.О., Якименко Н.М. «Метод підвищення ефективності розподіленої обробки даних у комп'ютерних системах операторів стільникового зв'язку» Вісник Черкаського державного технологічного університету. Технічні науки. №4. С. 103-110. 2020.
 26. О.А.Смірнов, Т.В.Смірнова, Л.І. Поліщук, К.О. Буравченко, А.О.Макевнін, «Дослідження хмарних технологій як сервісів», Кібербезпека: освіта, наука, техніка. № 3(7). С. 43-62. 2020.
 27. Смірнов О.А., Коноплицька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Поліщук Л.І. Інформаційна безпека в комп'ютерних мережах. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2020. – 294 с.
 28. О.А. Смірнов, П.С. Усік, «дослідження перспектив використання технологічних рішень в мережах 5g» у Кібербезпека та інформаційні технології: монографія. – Х. : ТОВ «ДІСА ПЛЮС», 2020.С. 122-135.
 29. Смірнов О.А., Дресєва Г.М., Дресєв О.М., Смірнова Т.В. «Фрактальний аналіз генератора самоподібного трафіку на основі ланцюга Маркова». Центральнотрапійський науковий вісник. Технічні науки. № 2(33). с. 161-172, 2019.
 30. Смірнов О.А., Коноплицька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В. Поліщук Л.І. Проектування комп'ютерних систем та мереж. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2019. – 264 с.
 31. Smirnov, O., Kuznetsov, A., Kuznetsova, K. Synthesis of Discrete Signals with Improved Correlation Properties. Монографія: In.: ISCI'2019: Information Security in Critical Infrastructures. Collective monograph. Edited by Ivan D. Gorbenko and Alexandr A. Kuznetsov, ASC Academic Publishing, USA, 2019, pp. 281-299. – ISBN: 978-0-9989826-8-7 (Hardback), ISBN: 978-0-9989826-9-4 (Ebook).
 32. Смірнов О.А., Дресєва Г.М. Метод генерування фрактального трафіку за допомогою моделі генератора на графі. Монографія: Інформаційна безпека та інформаційні технології : монографія / за заг. ред. В. С. Пономаренка. – Х. : Вид. Рожко С.Г. 2019. С. 123-139

УДК 004

М.Скрипка, магістр гр. КН-24М,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ІНТЕЛЕКТУАЛЬНОГО КЕРУВАННЯ ЦИФРОВИМИ ПРАВАМИ НА ОСНОВІ DRM

У статті розроблено програмне забезпечення, яке призначено для системи інтелектуального керування цифровими правами на основі DRM. Метою розробки є дослідження та принципи побудови системи інтелектуального керування цифровими правами на основі DRM. Об'єктом дослідження є процес інтелектуального керування цифровими правами на основі DRM. Предметом дослідження є методи інтелектуального керування цифровими правами на основі DRM. Методи дослідження базуються на методах захисту інтелектуальної власності, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи інтелектуального керування цифровими правами на основі DRM. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

інтелектуальне керування цифровими правами, DRM

Постановка проблеми. Управління цифровими правами (DRM) стосується алгоритмів та процесів, створених для забезпечення дотримання авторських прав під час споживання цифрового контенту. Без DRM кінцевий користувач може легко скопіювати ваш контент. Цей процес зазвичай називають піратством. Таким чином, це необхідно в архітектурі онлайн-розповсюдження відео, але споживач не бачить цього.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи інтелектуального керування цифровими правами на основі DRM.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи інтелектуального керування цифровими правами на основі DRM.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем інтелектуального керування цифровими правами на основі DRM.
- Дослідження системи інтелектуального керування цифровими правами на основі DRM.
- Програмна реалізація системи інтелектуального керування цифровими правами на основі DRM.

Об'єктом дослідження є процес інтелектуального керування цифровими правами на основі DRM.

Предметом дослідження є методи інтелектуального керування цифровими правами на основі DRM.

Методи дослідження базуються на методах захисту інтелектуальної власності, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Розмір ринку управління цифровими правами стрімко зростає останніми роками. Він зростає з 6,66 млрд доларів у 2025 році до 7,94 млрд доларів у 2026 році зі сукупним річним темпом зростання (CAGR) 19,2%. Зростання за історичний період можна пояснити розширенням споживання цифрових медіа, зростанням розповсюдження онлайн-контенту, збільшенням випадків цифрового піратства,

впровадженням моделей ліцензування програмного забезпечення, розвитком потокових сервісів.

Очікується, що ринок управління цифровими правами швидко зростатиме протягом наступних кількох років. У 2030 році він зросте до 15,95 мільярда доларів США зі складним річним темпом зростання (CAGR) 19%. Зростання в прогнозований період можна пояснити зростанням попиту на безпечне цифрове розповсюдження, зростаючим впровадженням управління правами на основі блокчейну, розширенням платформ іммерсивного цифрового контенту, зростанням інвестицій у передові технології шифрування, посиленням регуляторної уваги до захисту інтелектуальної власності. Основні тенденції в прогнозований період включають зростання впровадження хмарних рішень DRM, зростання попиту на технології захисту контенту, зростаючу інтеграцію DRM зі потоковими платформами, розширення моделей контенту на основі підписки, посилену увагу до боротьби з піратством.

Ринок управління цифровими правами зростає через зростання проблем безпеки. Широке використання ПК та ноутбуків приваблює хакерів, які шукають несанкціонованого доступу до корпоративних та урядових мереж, прагнучи викрасти критично важливу інформацію для фінансової та бізнес-вигоди. Корпорації все частіше застосовують підходи до управління бізнес-даними в режимі реального часу, включаючи передачу та зберігання на мобільних пристроях, хмарі, USB-накопичувачах та дисках. Як повідомляє InfoSecurity, прогнозується, що глобальні збитки від програм-вимагачів у 2023 році перевищать 30 мільярдів доларів, що підкреслює зростаючу загрозу. Складність та витонченість кібератак посилюють труднощі виявлення. Управління цифровими правами також застосовується організаціями охорони здоров'я та фінансових послуг для забезпечення дотримання стандартів конфіденційності та захисту даних, таких як HIPAA та Закон Гремма-Ліча-Блайлі. Очікується, що ця зростаюча стурбованість безпекою стимулюватиме зростання ринку в секторі управління цифровими правами.

Великі компанії на ринку управління цифровими правами зосереджуються на розробці інноваційних рішень, таких як послуги з управління цифровими правами, для встановлення авторства та контролю прав використання. Служба управління цифровими правами (DRM) – це технологія, призначена для захисту та регулювання розповсюдження та використання цифрового контенту, запобігання несанкціонованому доступу, копіюванню або обміну медіафайлами, такими як музика, відео або електронні книги. Наприклад, у липні 2024 року Wacom Co., Ltd., японська компанія-розробник програмного забезпечення, яка виробляє графічні планшети та пов'язані з ними продукти, запустила нову послугу управління цифровими правами. Ця послуга DRM від Wacom Co., Ltd. забезпечує покращений захист цифрового контенту, особливо корисна для творчих професіоналів, забезпечуючи безпечний доступ і контроль використання художніх творів і дизайнів. Вона включає безперебійну інтеграцію з пристроями Wacom, що спрощує обмін контентом і співпрацю, а також захищає інтелектуальну власність за допомогою надійних інструментів шифрування та керування дозволами.

У квітні 2024 року американська компанія-розробник програмного забезпечення Agora, Inc., що спеціалізується на комунікаційних програмних рішеннях, співпрацювала з EZDRM для впровадження рішень для управління цифровими правами (DRM), призначених для захисту контенту в прямому ефірі. Це партнерство має на меті підвищити безпеку контенту в прямому ефірі, забезпечуючи захист у режимі реального часу для прямих трансляцій шляхом безперешкодної інтеграції інтерактивної платформи мовлення Agora з надійною технологією DRM EZDRM. Ця інтеграція забезпечує безпечну доставку контенту, запобігаючи несанкціонованому доступу або піратству під час прямих трансляцій. EZDRM – це американська компанія, яка надає послуги з управління цифровими правами як послугою (DRMaaS).

Північна Америка була найбільшим регіоном на ринку управління цифровими правами у 2025 році. Очікується, що Азіатсько-Тихоокеанський регіон буде найшвидше зростаючим регіоном у прогнозований період. Ринок управління цифровими правами

включає доходи, отримані суб'єктами господарювання від надання таких послуг, як ліцензії на програмне забезпечення та ключі, протоколи автентифікації користувачів та IP-автентифікації, проксі-сервери, віртуальні приватні мережі (VPN), регіональні обмеження або геоблокування. Ринкова вартість включає вартість пов'язаних товарів, що продаються постачальником послуг або включені до пропозиції послуг. Враховуються лише товари та послуги, що продаються між суб'єктами господарювання або кінцевим споживачем.

Ринкова вартість визначається як доходи, які підприємства отримують від продажу товарів та/або послуг на визначеному ринку та в певній географічній зоні через продажі, гранти або пожертви у валюті (у доларах США, якщо не зазначено інше).

Доходи для певної географічної області – це споживчі значення, що представляють собою доходи, отримані організаціями у певній географічній області на ринку, незалежно від того, де вони виробляються. Вони не включають доходи від перепродажу вздовж ланцюга постачання, як далі вздовж ланцюга постачання, так і як частину інших продуктів.

Музика в Інтернеті

Крім стандартних підходів DRM, деякі магазини пропонують DRM-схему підписки. Наприклад, сервіс Sony Music Unlimited або онлайн музичний магазин Napster. Користувачі можуть завантажувати і прослуховувати необмежену кількість музики доти, поки діє підписка. Однак із закінченням підписки всі файли перестають відтворюватися.

У зв'язку з тим, що схеми DRM у різних виробників відрізняються між собою, іноді стає неможливим програвати музику від різних виробників на одному пристрої (пристрій може просто не підтримуватися DRM-схемою). Рішенням подібних проблем займаються, наприклад, в Англії. Так Ендрю Гауерс склав список пропозицій по поліпшенню політики захисту авторських прав (англ. Gowers Review of Intellectual Property), що містить 54 пункту. Цей список перебуває у відкритому доступі, і ознайомитися з ним може будь-який бажаючий. Серед всіх інших виправлень пункти з 8 по 12 містять пропозиції по створенню деяких виключень для сумнівного використання авторських прав, наприклад, бібліотеками (розглядається можливість переходити від однієї схеми DRM до іншої). Згодом планувалося ввести подібні виключення й для звичайних користувачів. Взагалі проблема з різними DRM у програвачах стояла досить гостро, наприклад, Apple відмовилися від DRM-захисту в музиці повністю, завдяки чому музика з iTunes програватиметься спокійно на будь-якому пристрої, що підтримує формат AAC. Деякі магазини, наприклад, німецький Musicload, також оголосили про відмову від DRM, тому що з'ясувалося, що 3 з 4 дзвінків у їхню службу підтримки надходило від незадоволених DRM-користувачів. [17]

Телевізійні програми

Ця концепція була розроблена компанією Fox Broadcasting в 2001 році й була підтримана МРАА і Федеральним Агентством по зв'язку (ФАС) США. Однак у травні 2005 року Апеляційний Суд США ухвалив, що ФАС не має достатню владу для накладення подібних обмежень на телеіндустрію в США.

Куди більшого успіху ця система домоглася, коли була прийнята Проектом Цифрового Відео Віщання – консорціумом, що включає більше 250 вещателів, виробників, операторів мережі, розроблювачів програмного забезпечення й керуючих органів більше 35 країн. Цей консорціум намагався розробити нові цифрові стандарти для DRM у телемовленні. Одним з найбільш перспективних стандартів є варіант із поліпшеним прапором передачі, розроблений для європейського телебачення DVB-CPCM (DVB Content Protection and Copy Management, укр. захист умісту й керування копіюванням). Цей стандарт був наданий на розгляд європейським урядам в 2007 році. Всі нормативні частини на даний момент уже схвалені для публікації Керівною Радою DVB і будуть опубліковані ETSI як офіційний європейський стандарт ETSI TS 102 825-X (X – номер підрозділу). На сьогоднішній день ще ніхто не взяв на себе забезпечення Сумісності й Надійності (англ. Compliance and Robustness) для даного стандарту (однак розробки в даному напрямку ведуться багатьма компаніями), що не дозволяє сьогодні впровадити цю систему повсюдно.

[1]

У США постачальниками кабельного телебачення використовується стандарт CableCard, що обмежує доступ користувача тільки тими послугами, на які він підписаний.

Текст, документи, електронні книги

Керування цифровими правами на підприємстві – це застосування технологій DRM для керування доступом до корпоративних документів (файли Microsoft Word, PDF, AutoCAD, електронні листи, сторінки внутрішньої мережі інтранет). Ці технології, більше відомі як Керування Інформаційними Правами (англ. Information Rights Management), в основному використовуються для запобігання несанкціонованого використання документів, що є інтелектуальною власністю підприємства (наприклад, з метою промислового шпигунства або випадкового витоку інформації). Звичайно ця система убудована в програмне забезпечення системи керування вмістом, однак деякі корпорації (наприклад, Samsung Electronics) розробляють свої власні системи DRM.

Електронні книги, призначені для читання на ПК, мобільних пристроях або спеціальних «читалок», звичайно використовують DRM з метою обмежити копіювання, печатка або викладання книг у загальний доступ. Звичайно такі книги обмежені кількістю пристроїв, на яких їх можна прочитати, а деякі видавці взагалі забороняють будь-яке копіювання або печатку. Деякі компанії й оглядачі вважають, що наявність DRM створює безліч проблем для видання книг. [3]

Цикл шифрування

Щоб розпочати цикл «безпеки», зв'язок між програмним забезпеченням для кодування, що запитує, та сервером ліцензій шифрується.

Кожен сегмент шифрується відповідно до специфікації MPEG Common Encryption (CENC) для ISO-BMFF.

Що таке ISO-BMFF?

ISO-BMFF – це стандартизований формат файлів, який служить контейнером для аудіо- та відеоконтенту. Відомою реалізацією ISO-BMFF (і часто використовується як його синонім) є формат файлів MP4 або фрагментований MP4 (fMP4). У робочому процесі DRM мультимедійний контент шифрується, а контейнер ISO-BMFF покращується за допомогою метаданих та алгоритмів шифрування, специфічних для DRM.

Системи DRM використовують ISO-BMFF для зберігання та транспортування зашифрованих медіаданих і забезпечують пов'язання з ліцензією DRM. Коли користувачі намагаються отримати доступ до захищених медіаданих, система DRM перевіряє, чи має користувач на це право, залежно від пов'язаної ліцензії.

Коротше кажучи, це забезпечує безпечне зберігання, доставку та контроль цифрових медіафайлів у рамках DRM.

Сегменти можуть бути повністю зашифровані або частково зашифровані, коли шифруються лише деякі кадри або навіть лише частини кадрів.

Стандарт MPEG-CENC визначає, як шифрується сегмент, і відображає, який ключ дешифрування потрібно використовувати для якого сегмента (або його частин), пов'язуючи з ним ідентифікатор ключа. MPEG-CENC використовується для потоків DASH та HLS, якщо сегменти мають формат контейнера fMP4.

Стандартне шифрування контенту виконується за допомогою алгоритму Advanced Encryption Standard (AES) з використанням 128-бітних ключів. Залежно від використовуваної системи DRM, вона використовується або в режимі лічильника (CTR), або в режимі ланцюжка блоків шифрування (CBC).

Ці два режими відрізняються тим, як шифрується корисне навантаження.

Важливо зазначити, що шифруються лише необроблені аудіо- та відеодані в сегменті, а метадані, додані в контейнер, – ні.

Існує три основні постачальники DRM: Google Widevine, Apple FairPlay та Microsoft Playready.

Їхнє застосування може значно відрізнятися залежно від багатьох унікальних факторів – необхідність вибору постачальника, який відповідає потребам дистриб'ютора

контенту щодо доставки та відтворення (залежно від того, які пристрої підтримуються), може значно ускладнити процес впровадження DRM.

Для підвищення безпеки та зменшення ризику зворотного проектування систем DRM зазвичай немає чітких повідомлень журналу.

Фактично, частини процесу розглядаються як чорна скринька, і в результаті налагодження може бути ще складнішим на пристроях (наприклад, SmartTV або телеприставках) зі старими версіями програмного забезпечення DRM.

У браузері або операційній системі контент потім буде розшифровано модулем розшифрування контенту (CDM), який розшифровує кожен зашифрований аудіо- та відеосегмент.

Цикл дешифрування

Коли веб-плеєр ідентифікує контент, захищений DRM, він викликає процеси та інтерфейси, визначені розширеннями зашифрованого медіа (EME), які використовуються в браузерах для ініціювання процесу запиту ліцензії.

EME використовується для взаємодії з модулем розшифрування контенту (CDM), який реалізований у браузері та може покладатися або не покладатися на функції операційної системи, такі як HDCP.

Під час відтворення контенту, захищеного DRM, запити на ліцензію генеруються CDM та передаються програвачу через EME.

Всю роботу з розшифрування виконує CDM. Найголовніше, що розшифрований контент залишається в CDM – він не є і не повинен бути доступним для програмного забезпечення для відтворення, оскільки інакше можна було б створити розшифровані копії контенту.

Для відтворення захищеного контенту, після виявлення того, що контент захищений, програвач або програмне забезпечення для відтворення надсилає запит на ліцензію на сервер ліцензування.

Якщо ліцензія кешується локально, цей запит можна пропустити, і замість нього можна використовувати кешовану ліцензію.

Запит на ліцензію, що надсилається програвачем програмного забезпечення для відтворення, завжди містить метадані, які однозначно ідентифікують відтворюваний контент, а формат цих метаданих залежить від використовуваного DRM-рішення.

Ці метадані DRM можуть міститися або в маніфесті (наприклад, MPEG-DASH або вбудовані в HLS), або в конфігурації програвача, або в окремих сегментах.

Хоча це не є обов'язковою вимогою, запит зазвичай містить додаткові дані із пристрою, що запитує, такі як ідентифікатор, який можна використовувати для його унікальної ідентифікації.

Якщо надана вся обов'язкова інформація, сервер може надати ліцензію програвачу або програмному забезпеченню для відтворення з ключами розшифрування, необхідними для безпечного відтворення запитуваного контенту на клієнті.

Повернена ліцензійна угода може містити інформацію про необхідний рівень безпеки розшифрування контенту, наприклад: розшифрування контенту за допомогою програмного забезпечення значно менш безпечне, ніж розшифрування за допомогою апаратного забезпечення.

З точки зору гравця, отримання ліцензії за допомогою EME починається зі створення клієнтом відтворення так званого ключового сеансу. Використовуючи цей ключовий сеанс та метадані DRM, взяті з сегментів, маніфесту або інших джерел, гравець запускає процес запиту ліцензії за допомогою EME.

Потім CDM генерує підписане ключове повідомлення, яке програвач або програмне забезпечення для повернення коштів надсилає на сервер ліцензій.

Сервер ліцензій повертає запитувану ліцензію, а також приймає рішення про те, чи надано клієнту права на відтворення запитуваного контенту; якщо ні, відтворення зупиняється та відображається помилка.

Або ж сервер ліцензій може визначити, що, наприклад, програвач може відтворювати лише SD-версії контенту.

Якщо запит ліцензії був успішним, клієнт оновлює ключовий сеанс повернутою ліцензією.

Потім розшифрування контенту повністю обробляється CDM.

За деяких обставин ліцензія кешується на певний час і може бути використана для відтворення захищеного контенту офлайн (наприклад, Netflix).

Робочий процес дуже схожий для невеб-платформ, таких як нативні додатки для Android, iOS або tvOS. Кожна платформа має власний набір API, подібних до EME on Web, для взаємодії з базовою інтегрованою CDM.

Ліцензія та розшифровані дані не повинні бути доступні клієнтам, окрім користувача ліцензованого контенту.

Таким чином, закриті ключі та розшифровані дані зберігаються в безпечному середовищі в браузері, операційній системі або навіть на обладнанні (якщо підтримується), як-от у надійних середовищах виконання.

Використання різних форматів контейнерів, таких як fMP4 та MPEG-2 TS, ускладнювало розповсюдження однакового контенту на всіх платформах.

Однак швидке впровадження CMAF та стандартизація CENC серед виробників обладнання та розробників програмного забезпечення зменшують складність впровадження для галузі.

Хоча CMAF та CENC все ще дозволяють використання AES CTR та AES CBC, постачальники DRM поступово переходять до використання AES CBC.

Запобігання копіюванню контенту, захищеного авторським правом, у інших правовласників

Припустімо, ви розміщуєте онлайн-платформу відео на вимогу, яку можна використовувати для перегляду всіляких голлівудських фільмів. Власник прав на контент, який ви розповсюджуєте, не хоче, щоб ваші користувачі могли просто створювати копії цього контенту.

Таким чином, постачальник платформи може бути зобов'язаний за контрактом використовувати певну форму захисту контенту для дотримання прав власника прав на контент.

Це часто трапляється з мовниками, які не лише розміщують власний контент, але й, наприклад, транслюють прямі трансляції телепередач чи інші фільми чи серіали. Системи DRM можуть використовуватися для захисту контенту від незаконного копіювання користувачами цього сервісу.

Вибір найкращих DRM-сервісів

Існує кілька варіантів контролю доступу до вашого цифрового контенту, обмежуючи його лише авторизованими користувачами. Постачальники DRM пропонують рішення та послуги творцям контенту, видавцям та дистриб'юторам.

Вони спеціалізуються на розробці та впровадженні технологій, інструментів і систем, що забезпечують захист, розповсюдження та управління вашим цифровим контентом. Вони також забезпечують дотримання умов ліцензування та законів про авторське право.

Такі рішення, як шифрування, контроль доступу, управління ліцензіями, захист контенту та моніторинг, можуть бути надані хорошим партнером з DRM.

Набір послуг розробляємої системи інтелектуального керування цифровими правами на основі DRM виглядає так:

- Інтеграція системи DRM: Постачальники DRM інтегрують свої технології в існуючі платформи розповсюдження контенту, веб-сайти або потокові платформи, забезпечуючи безперебійну функціональність DRM та захист цифрового контенту.

- Шифрування контенту: Рішення для шифрування захищають цифровий контент від неавторизованих користувачів та онлайн-піратства. Гарний партнер застосує надійні

алгоритми шифрування для захисту вашого контенту під час зберігання, передачі та відтворення.

– Керування ліцензіями: Системи керування ліцензіями займаються створенням, видачею та керуванням ліцензіями DRM. Ці системи гарантують, що користувачі мають необхідні дозволи та права для доступу до вашого захищеного контенту.

– Забезпечення дотримання прав: ці механізми забезпечують дотримання прав використання, визначених ліцензіями DRM. Це може включати обмеження кількості пристроїв, на яких можна отримати доступ до вашого контенту, забезпечення обмеженого за часом доступу або контроль можливості копіювання чи обміну контентом.

– Аналітика та моніторинг: Постачальники DRM пропонують інструменти аналітики та моніторингу для відстеження використання контенту, виявлення потенційних порушень та збору інформації про поведінку користувачів.

Зрозуміло, що управління цифровими правами – це складна тема, до якої не існує універсального підходу. Але це невід’ємна частина відеороботи для кожного, хто хоче захистити або монетизувати свій цифровий відеоконтент. Це сфера постійного розвитку, оскільки ті, хто має намір займатися піратством, шукають нові способи обійти захист вашого контенту заради власної вигоди. У даній роботі система керування цифровими правами на основі DRM реалізується за рахунок використання методів стеганографії. Структурна схема розробленого програмного забезпечення представлена на рисунку 1. В якості даних, що вбудовуються може використовуватися будь-яка інформація: текст, повідомлення, невелике зображення тощо, які дозволяють підтверджувати та захищати авторські права. Роль контейнеру буде відігравати будь-яке кольорове цифрове зображення, яке потребує захисту у рамках забезпечення авторських прав, що задовольняє стандартним вимогам до контейнерів для стегоповідомлень.

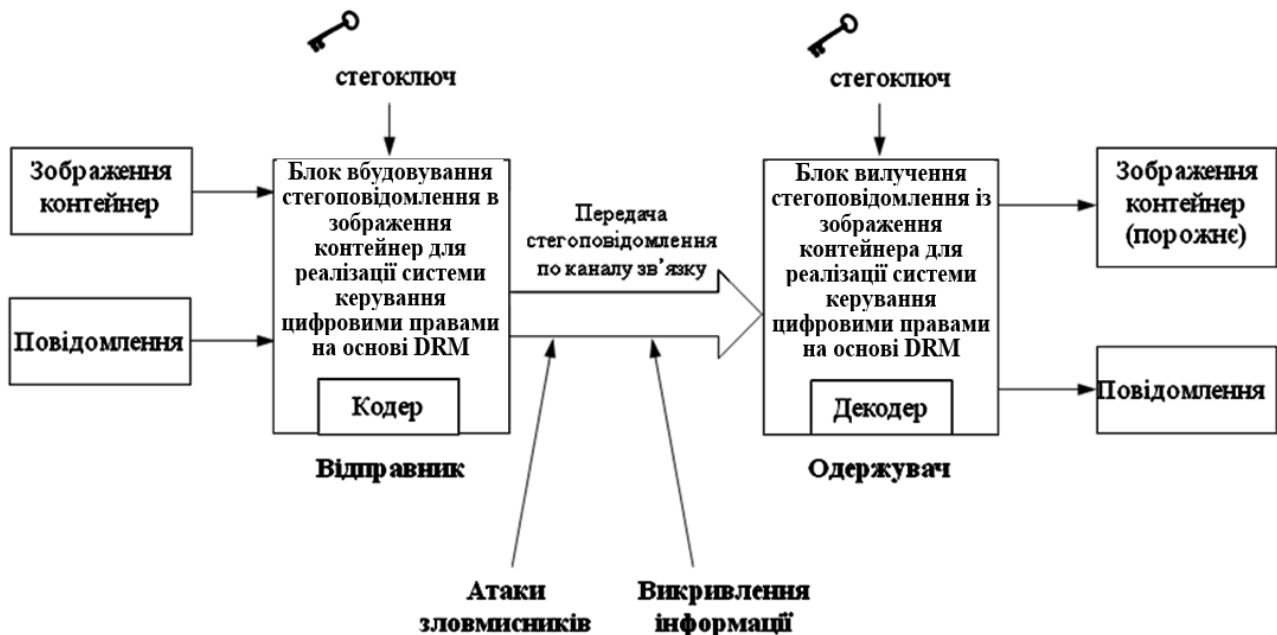


Рисунок 1 – Структурна схема системи

Стегоключ – секретний ключ, необхідний для приховування інформації. Залежно від кількості рівнів захисту (наприклад, вбудовування заздалегідь зашифрованого повідомлення) в стегосистемі може бути один або декілька стегоключів. Вбудовування повідомлення в зображення контейнер відбувається за допомогою стегокодера, який крім приховування інформації здійснює також і перешкодостійке кодування. Після цього зображення з прихованим повідомленням передається по каналу зв'язку, де може зазнавати атак зломисників, а також викривлень інформації в наслідок перешкод у каналі зв'язку або застосувань алгоритмів стиснення з втратами. Вилучення повідомлення із зображення

контейнера здійснюється за допомогою стегодетектора. Стегодекодер перевіряє наявність прихованого повідомлення і в разі його існування, вилучає інформацію.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів інтелектуального керування цифровими правами на основі DRM. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем інтелектуального керування цифровими правами на основі DRM.
- Досліджена система інтелектуального керування цифровими правами на основі DRM.
- На основі отриманих результатів досліджень створена програмна реалізація системи інтелектуального керування цифровими правами на основі DRM.

Розроблені алгоритми дозволяють успішно вирішувати завдання інтелектуального керування цифровими правами на основі DRM. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Kuznetsov, O., Smirnov, O., Akhmetov, B., Alimseitova, Z., Imoize, A.L. «Deep Learning Frontiers in Copy-Move Forgery Detection: Advances, Challenges, and Future Directions». *Advancements in Cybersecurity Next Generation Systems and Applications*, 2025. 202-229.
2. Lakhno, V., Malyukov, V., Smirnov, O., Bebesheko, B., Chubaievskiy, V., Zhumadilova, M., Malyukova, I., Smirnov, S. «Multifactorial Model for Targeted Attacks Counteracting Within the Framework of a Multi-Step Quality Game with Fuzzy Information». *8th International Symposium on Intelligent Informatics, ISI 2023*, 2025. vol 389. pp 377-389. Springer, Singapore.
3. Kuznetsov, O., Smirnov, O., Mormul, M., Kotukh, Y., Zvieriev, V. «Comparative Research on Cryptocurrency Efficiency: An Objective Analysis of Key Metrics». *International Journal of Computing* 23(4), 2024. pp. 563-573.
4. Kuznetsov O., Frontoni E., Kuznetsova K., Smirnov O., Kostenko V. «Blockchain applications in metaverse environments: new horizons». *Advanced Metaverse Wireless Communication Systems*. pp. 255-293. 2024.
5. Kuznetsov, O., Frontoni, E., Chevardin, V., Smirnov, O., Imoize, A.L. «Advancing metaverse security with cryptographic innovations». *Advanced Metaverse Wireless Communication Systems*. pp 351-386. 2024.
6. Kuznetsov O., Frontoni E., Kuznetsova Y., Smirnov O., Moskovchenko I. «Trust-Based Security Architecture for Edge Computing: A Simulation Study of Dynamic Trust Evolution and Attack Detection». *CEUR Workshop Proceedings*, 2024, 3909, pp. 227–241.
7. Kuznetsov, O., Frontoni, E., Kryvinska, N., Chevardin, V., Smirnov, O. «Wireless Network Encryption Stream Ciphers, Computational Modeling, and Security Analysis». *Computational Modeling and Simulation of Advanced Wireless Communication Systems*, 2024, pp. 379–402.
8. Kuznetsov, O., Frontoni, E., Kryvinska, N., Smirnov, O., Imoize, G.L. «Computational Modeling of Enhanced Spread Spectrum Codes for Asynchronous Wireless Communication». *Computational Modeling and Simulation of Advanced Wireless Communication Systems*, 2024, pp. 403–447.
9. Ткаченко, О., Ільченко, А., Улічев, О., Мелешко, Є., Смірнов, О. «Правові засади поширення інформаційних впливів в соціальних мережах». *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2024. № 2(26), С. 170–188.
10. Смірнова Т.В., Коноплицька-Слободенюк О.К., Буравченко К.О., Смірнов С.А., Кравчук О.В., Козірова Н.Л., Смірнов О.А. «Дослідження технологій забезпечення кібербезпеки хмарних сервісів IaaS, PaaS та SaaS». *Кібербезпека: освіта, наука, техніка*. 2024. №4(24), С. 6-27.
11. Вінтенко, Б., Миронець, І., Смірнов, О., Кравчук, О., Козірова, Н., Савеленко, Г., Коваленко, А. «Дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». *Кібербезпека: освіта, наука, техніка*. 2024. №3(23), С. 111-131.
12. Kuznetsov, O., Frontoni, E., Kandiy, S., Smirnova, T., Prokopov, S., Bilanovych, A. «New Cost Function for S-boxes Generation by Simulated Annealing Algorithm». *Lecture Notes on Data Engineering and Communications Technologies*, 2023. vol 180. pp. 310-320. Springer, Cham.
13. Kuznetsov, O., Frontoni, E., Kandiy, S., Smirnov, O., Ulianovska, Y., Kobylanska, O. «Heuristic Search for Nonlinear Substitutions for Cryptographic Applications». *Lecture Notes on Data Engineering and Communications Technologies*, 2023. vol 180. Springer, Cham. pp. 288-298.
14. Kuznetsov, O., Kuznetsova, Y., Smirnov, O., Kostenko, O., Zvieriev, V. «Evaluating Hashing Algorithms in the Age of ASIC Resistance». *CEUR Workshop Proceedings*, 2023, 3628, pp. 93-105.
15. Kuznetsov O., Frontoni E., Kuznetsova Ye., Smirnov O., Chevardin V. «Achieving Enhanced Security in

- Biometric Authentication: A Rigorous Analysis of Code-Based Fuzzy Extractor». CEUR Workshop Proceedings, Volume 3624, 2023, pp. 330-339.
16. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchov, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». CEUR Workshop Proceedings, Volume 3530, 2023, pp. 256-265.
 17. Kuznetsov, O., Kandiy, S., Frontoni, E., Smirnov, O. «Trade-offs in Post-Quantum Cryptography: A Comparative Assessment of BIKE, HQC, and Classic McEliece». CEUR Workshop Proceedings, Volume 3504, 2023, pp. 1-11.
 18. Смірнов О.А., Козлов Я.О., Смірнова Т.В. «Дослідження застосування SIEM-систем для забезпечення кібербезпеки та захисту інформації». II Міжнародна науково-практична Інтернет-конференція «Інновації та перспективні шляхи розвитку інформаційних технологій (ІПШРІТ-2023)» м.Черкаси 6 грудня 2023 року – Черкаси: ЧДТУ. – 2023. – С.251-252.
 19. Козлов Я.О., Смірнова Т.В., Смірнов О.А. «Дослідження SIEM-систем для забезпечення кібербезпеки». VII міжнародна науково-практична конференція “Інформаційна безпека та комп’ютерні технології” до 30-ти річчя кафедри кібербезпеки та програмного забезпечення, м. Кропивницький. 1 листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 26.
 20. Козлов Я.О., Козірова Н.Л., Смірнов О.А. «Дослідження структури та принципу роботи SIEM-системи». VII міжнародна науково-практична конференція “Інформаційна безпека та комп’ютерні технології” до 30-ти річчя кафедри кібербезпеки та програмного забезпечення, м. Кропивницький. 1 листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 59.
 21. Вінтенко Б.Ю., Смірнов О.А., Коваленко О.В., Смірнов С.А., Коваленко А.С. «Дослідження нормативних документів та галузевих стандартів розробки програмного забезпечення комп’ютерних систем управління АЕС, важливих для безпеки». Системи управління, навігації та зв’язку, 2023, вип. 2(72), С. 170-178.
 22. Смірнова Т.В., Гнатюк С.О., Бердибасв Р.Ш., Сидоренко В.М., Жигаревич О.К., «Система корелювання подій та управління інцидентами кібербезпеки на об’єктах критичної інфраструктури». Кібербезпека: освіта, наука, техніка, №3(19), 2023, С. 176-196.
 23. Smirnov, O., Neskorodieva, T., Fedorov, E., Rudakov, K., Neskorodieva, A. «Method Detection Audit Data Anomalies on Basis Restricted Cauchy Machine» CEUR Workshop Proceedings, Volume 3187, 2022,
 24. Smirnov, O., Lakhno, V., Akhmetov, B., Chubaievskyi, V., Khorolska, K., Bebesko, B. «Selection of a Rational Composition of Information Protection Means Using a Genetic Algorithm». In: Rajakumar, G., Du, K.L., Vuppapapati, C., Beligiannis, G.N. (eds) Intelligent Communication Technologies and Virtual Mobile Networks. Lecture Notes on Data Engineering and Communications Technologies, vol 131. 2023. Springer, Singapore. pp. 21-34.
 25. Smirnov O.A., Al-Oraiqat A.M., Ulichev O.S., Meleshko Ye.V., Al-Rawashdeh H.S., Polishchuk L.I. «Modeling strategies for information influence dissemination in social networks». Journal of Ambient Intelligence and Humanized Computing Volume 13, Issue 5. Springer, Cham. 2022, pp. 2463-2477.
 26. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції ґешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв’язку, 2022, № 3(69). С. 93-98.
 27. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції ґешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Вісник Хмельницького національного університету. Серія: «Технічні науки», № 2 (307). С. 46-52. 2022.
 28. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції ґешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв’язку, 2022, № 1(67). С. 84-89.
 29. Смірнов О.А., Коноплицька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Книшук А.В. «Вступ до кібербезпеки»: навчальний посібник – Кропивницький: ЦНТУ – 2022. – 968 с.
 30. Теорія та практика сучасного інформаційно-психологічного протистояння: навчальний посібник / [В.М. Петрик, С.О. Гнатюк, М.М. Присяжнюк та ін.]; за заг. ред. С.О. Гнатюка, В.М. Петрика та О.А. Смірнова. – Полтава, 2022. – 334 с.
 31. Smirnov O., Kuznetsov A., Zhora V., Onikiychuk A., Pieshkova O. «Hiding Messages in Audio Files Using Direct Spread Spectrum». 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2021, Cracow, Poland, 22-25 September 2021. P. 414-418
 32. Smirnov O., Kuznetsov A., Lokotkova I., Kuznetsova T., Florov S., Lebid O. «Using Orthogonal Signals to Hide Information in Images». 4 IEEE International Conference on Advanced Information and Communication Technologies (AICT) - 2021, Lviv, Ukraine, September 21-25, 2021. P. 255-260.

УДК 004

Р.Слабінога, магістр гр. КН-24М,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ІНТЕЛЕКТУАЛЬНОГО МОНІТОРИНГУ ТА ЗАПОБІГАННЯ АКТИВНОСТІ ДОДАТКІВ

У статті розроблено програмне забезпечення, яке призначено для системи інтелектуального моніторингу та запобігання активності додатків. Метою розробки є дослідження та принципи побудови системи інтелектуального моніторингу та запобігання активності додатків. Об'єктом дослідження є процес інтелектуального моніторингу та запобігання активності додатків. Предметом дослідження є методи інтелектуального моніторингу та запобігання активності додатків. Методи дослідження базуються на методах інтелектуального моніторингу, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи інтелектуального моніторингу та запобігання активності додатків. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

інтелектуальний моніторинг, запобігання активності, додатки

Постановка проблеми. Малоімовірно, що ваш комп'ютер буде заражений вірусом, але в той же час існує небезпека зараження іншими типами шкідливих програм і онлайн-погроз. Трояни-вимагачі зашифровують важливі файли й чекають оплати викупу, перш ніж розблокувати доступ до них. Банківські трояни втручаються в онлайн транзакції й намагаються украсти кошти. Зараження ботнетом зробить ваш комп'ютер ланкою в ланцюзі пристроїв, використовуваних для організації DDoS-атак. З цих і багатьох інших причин, ви повинні захистити свій комп'ютер за допомогою антивірусу.

Багато які із представлених антивірусів є безкоштовними тільки для некомерційного використання. Якщо ви хочете захистити комп'ютери в організації, то прийдеться придбати платну версію. У цьому випадку варто розглянути перехід на повноцінний комплексний антивірус. Зрештою, від цього залежить безпека вашого бізнесу. Якщо захистити потрібно великі підприємства, то на допомогу приходять SaaS-рішення, які дозволяють централізовано виконувати моніторинг і управляти захистом всіх комп'ютерів у компанії.

Ваш антивірус повинен надійно видаляти шкідливі програми, що вкоренилися в системі, але його основне завдання – запобігання нових заражень троянами-шифрувальниками, ботнетами, троянами й іншими видами погроз. Всі представлені в даному рейтингу антивіруси пропонують захист реального часу проти шкідливих атак. Багато продуктів пропонують надійний веб-захист, що блокує доступ до джерел шкідливих об'єктів і запобігає уведенню конфіденційних даних на шахрайських сайтах.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи інтелектуального моніторингу та запобігання активності додатків.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи інтелектуального моніторингу та запобігання активності додатків.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем інтелектуального моніторингу та запобігання активності додатків.
- Дослідження системи інтелектуального моніторингу та запобігання активності додатків.

– Програмна реалізація системи інтелектуального моніторингу та запобігання активності додатків.

Об'єктом дослідження є процес інтелектуального моніторингу та запобігання активності додатків.

Предметом дослідження є методи інтелектуального моніторингу та запобігання активності додатків.

Методи дослідження базуються на методах інтелектуального моніторингу, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Розглянемо реалізацію системи моніторингу й запобігання активності додатків, що була реалізована у вигляді антивірусу.

Автономний антивірус включає систему запобігання вторгнень HIPS. У тесті протидії 30 експлойтам, програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, виявив і заблокував більше половини з них, що краще результатів Bitdefender і Kaspersky. Norton заблокував дві-третьої атак, причому все з них на мережному рівні.

Складна система контролю пристроїв більше підходить для корпоративних середовищ, чим для звичайних споживачів, хоча сам продукт більше орієнтований на домашніх користувачів. Технічно підковані люди можуть запобігти підключенню зовнішніх пристроїв, включаючи карт-рідери, Bluetooth і зовнішні USB-пристрої. Для довірених пристроїв можна створювати виключення.

На сторінці “Сервіс” користувачеві доступні файли журналу подій і список доданих у карантин файлів. Інші інструменти призначені для агентів технічної підтримки при віддаленому усуненні проблем. Серед таких утиліт – запущені процеси, графік активності файлової системи й інструмент для створення знімків стану системи для наступного порівняння.

Базовий фаєрвол

Під час тестування фаєрвол коректно перевірив всі системні порти в схований режим і успішно протистояв веб-атакам. Проте, програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, не впорався з тестом, у якому використовувалися запити команди ping – це означає, що кіберзлочинець зможе з'ясувати реальну IP-адресу комп'ютера.

Ще однією перевіркою роботи двостороннього фаєрвола є випробування на блокування спроб зловживання мережними підключеннями. Програмний контроль програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, може працювати в декількох режимах. Стандартний автоматичний режим дозволяє весь вихідний трафік і блокує підозрілий вхідний трафік.

При перемиканні в інтерактивний режим, програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, поводить як традиційний фаєрвол, тобто при кожній спробі доступу в мережу з боку невідомої програми, продукт виводить користувацький запит подальшої дії. Проте, функція контролю має кілька розширених опцій. Фаєрвол може застосувати ваш вибір один раз, створити на його основі постійне правило або запам'ятати вибір до завершення роботи програми. За замовчуванням, вибір не запам'ятовується, тобто користувачеві прийде щораз реагувати на запити.

Після натискання по посиланню докладної інформації, користувачеві показується інформація про видавця, репутацію файлу й віддаленому комп'ютері й портах. При виборі розширених налаштувань можна редагувати правила фаєрвола за допомогою окремих IP-адрес і номерів портів. Звичайним користувачам ці можливості не припадуться.

Багато продуктів, зокрема Norton і Kaspersky, приймають рішення програмного контролю самостійно й не покладаються на недосвідчених користувачів. ZoneAlarm Extreme Security 2017 для обробки додатків використовує масивну базу даних відомих надійних файлів і автоматично налаштовує програмний контроль. В інтерактивному режимі фаєрволу

програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, потрібно вручну визначати правила для всіх програм і навіть для компонентів Windows – не найкращий підхід.

Один зі способів уникнути нескінченного потоку запитів – використовувати режим навчання. У даному режимі програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, виконує моніторинг всіх програм, які одержують доступ у мережу й створює правила дозволу доступу. Режим навчання автоматично завершиться через два тижні, хоча даний період можна змінювати. Після цього запитів буде помітно менше. Також можна розглянути вибір режиму на основі політик, що блокує всі підключення за винятком тих, які дозволені правилами фаєрвола.

Мережний захист у програмному продукті моніторингу й запобігання активності додатків, що був розроблений у даній роботі, NOD32 Internet Security є розширеною в порівнянні з можливостями автономного антивірусу. Проте, у тесті експлоїтів, обидва продукти показали однакові результати.

По вкрай мері, фаєрвол програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, успішно пручався прямим таргетованим атакам. Комплексний антивірус має два видимих процеси й одну службу, але в процесі тестування знайти спосіб для їхнього відключення за допомогою шкідливих технік не вдалося.

Фаєрвол програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, відверто розчарував. Він не зміг захистити від витоку реальної IP-адреси, а програмний контроль не повністю справляється зі своїм завданням. В інтерактивному режимі програма завалює користувача запитамі. Це традиційний фаєрвол на базі застарілих технологій. Багато сучасних продуктів пропонують більше передові рішення.

Захист домашньої мережі

При виборі панелі “Захист домашньої мережі” у головному вікні антивірусу з'являється зображення карти мережі. Виявлені пристрої відображаються у вигляді іконок у концентричних колах. При цьому маршрутизатор і локальний пристрій показуються в самому центрі. Наступне коло показує недавно підключені пристрої, а саме далеке коло – пристрою, підключені за останній місяць.

Якщо програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, не може одержати ім'я, то відображає IP-адреса. Майстер мережі дозволяє з'ясувати, що ховається за IP-адресу й допомагає додати зрозумілу назву. З режиму детального перегляду можна вибрати посилання усунення проблем, щоб подивитися заблокований фаєрволом трафік з даного пристрою.

Натисніть кнопку “Сканувати маршрутизатор”, щоб програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, перевірив налаштування безпеки вашого роутера. Буде запущено кілька тестів на проникнення, націлених на роутер. При виявленні проблем, програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, відразу ж запропонує їх усунути.

Захист банківських платежів

Програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, приділяє особливу увагу даної функції, тому що одна із трьох панелей на головному екрані присвячена захисту банкінгу. При виборі панелі відкривається захищена версія вашого браузера за замовчуванням із зеленою рамкою й баннером “Захищене” на верхній панелі. Браузер відкриває сторінку, що пояснює мета даної функції й рекомендує використовувати її тільки для інтернет-банкінгу й проведення фінансові транзакції, а не для звичайного серфінгу. Після установки антивірусу потрібно виконувати перезавантаження комп'ютера, щоб захист банківської оплати запрацював. Функція підтримує роботу з Chrome, Firefox і Internet Explorer. Користувачі Opera, Vivaldi і інших браузерів не зможуть її скористатися.

Також, як і функція "Безпечні платежі" у продуктах "Лабораторії Касперського", захист банківських платежів автоматично активується при відвідуванні відомого фінансового сайту у звичайному, незахищеному браузері. Програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, запропонує запустити безпечний браузер і запитає, потрібно чи запам'ятати цей вибір на постійній основі.

Обмежений батьківський контроль

Доступ до системи батьківського контролю програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, схований глибоко в налаштуваннях. У лівому навігаційному меню потрібно вибрати пункт "Налаштування", а потім потрібно перейти в розділ "Засоби безпеки". Після включення ви побачите список облікових записів Windows. Щоб завершити конфігурацію, потрібно вказати, які аккаунти належать дорослим, а які – дітям.

Залежно від віку дитини, програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, визначає, які із трьох десятків категорій умісту будуть піддаватися блокуванню. При детальному розгляді правил можна побачити, що кожна категорія має вікові обмеження – для всіх, 12+, 18+ або заборонене. Зверніть увагу, що навіть для облікових записів дорослих будуть блокуватися категорії Кримінал і Шкідливе ПЗ. Одночасно в області видимості перебуває всього три категорії, тому налаштування системи викликає серйозні труднощі.

При тестуванні контент-фільтр працював надійно. Фільтр працює в будь-якому браузері й не відключається простими мережними командами, які були успішні з деякими конкурентами. Під час випробування не вдалося виявити сайти, які уникли блокування. При блокуванні програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, показує в браузері просте попередження, схожі оповіщення відображаються при виявленні фішинг-погрози або шкідливого сайту. Дитина не зможе запросити перегляд заблокованого сайту, як це можна зробити в Symantec Norton Family Premier.

Програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, обробляє захищені HTTPS сайти іншим образом. Він не може підмінити заблокований ресурс інформаційною сторінкою, тому в браузері з'являється повідомлення про помилку, а спливаюче повідомлення пояснює, що відбулося.

В основному додатку програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, батьки можуть переглядати список заблокованих сайтів із вказівкою дати й часу спроби відвідування, обліковому запису й категорії контенту.

На цьому можливості батьківського контролю закінчуються. Тут ви не знайдете функцію керування контактами в месенджерах, аналітики соціальних мереж або контролю відеоігор по їхньому рейтингу. Крім того, недоступне керування часом використання Інтернету й комп'ютера. Батьківський контроль сильно урізаний, але працює добре.

Точний антиспам

Автономний антивірус програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, має ефективний убудований захист електронної пошти. Компонент сканує вхідну пошту POP3 і IMAP і вихідну пошту SMTP на предмет шкідливих програм. Програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, підтримує інтеграцію з Outlook, Outlook Express / Windows Mail або Windows Live Mail для розширеного контролю. При виявленні шкідливого ПЗ інструмент видаляє небезпечне вкладення й додає його назва до теми повідомлення. У комплексному антивірусі є ще повноцінний спам-фільтр.

Щоб включити антиспам, перейдіть у Налаштування > Захист Інтернету й виберіть іконку шестирні поруч із секцією "Захист від спаму". Налаштувань не так багато. Користувач може включити розширений захист від спаму, що повинна поліпшити точність. Дана функція відключена за замовчуванням, тому що серйозно знижує швидкість обробки пошти. Можна

поміняти стандартну мітку [SPAM] і включити оцінку спаму. За замовчуванням антиспам імпортує список контактів і адресатів ваших повідомлень у виключення. Також туди містяться листи, які були вручну визнані не спамом. Доступно ручне редагування білого й чорного списку адресатів. У сучасних умовах спам-фільтр потрібний не всім, тому що багато поштових провайдерів уже мають дану функцію. Якщо вам усе ще потрібний окремий антиспам, то програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, прекрасно справляється із цим завданням.

Захист веб-камери

Повідомлення про випадки стеження за допомогою веб-камери з'являються із тривожною регулярністю. Звичайно, можна заклеїти камеру ізолентой, але якщо ви часто берете участь у веб-конференціях, постійне заклеювання й відклеювання може стомити.

Захист веб-камери в програмному продукті моніторингу й запобігання активності додатків, що був розроблений у даній роботі, є доповненням програмного контролю, але більше простим у використанні. Користувач може заблокувати будь-які спроби доступ до камери й відключати захист тільки під час користування Skype. Якщо витратити небагато часу на налаштування, то можна вказати, які програми можуть одержувати доступ до камери й включити відображення оповіщення перед наданням доступу. Перевірити функцію в дії не вдалося, але для користувачів веб-камер вона може бути реально корисною.

Невеликий вплив на продуктивність

Програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, показав середній вплив на ресурси системи. У тесті виміру часу завантаження системи, антивірус сповільнив час завантаження всього на 11 відсотків, що краще середнього показника.

Розширений фаєрвол

Фаєрвол програмного продукту моніторингу й запобігання активності додатків, що був розроблений у даній роботі, справляється з базовими завданнями – відбиття атак на порти й перемикання всіх системних портів у схований режим. За замовчуванням програмний контроль обмежується дозволом вихідного трафіка й блокуванням підозрілого вхідного трафіка. В інтерактивному режимі при кожній спробі виходу в Інтернет з боку нової програми з'являється діалогове вікно із запитом подальшої дії. Фаєрволи в Kaspersky і Norton уміє автоматично обробляти дозволу для відомих надійних і шкідливих програм і пильно стежать за невідомими застосунками. Такий підхід є більше передовим, чим просто покласти ці обов'язки на плечі користувача. З позитивної сторони, не вдалося знайти спосіб для програмного відключення захисту ESET.

При запуску інструмента "Захист домашньої мережі" з'являється пророблена карта домашньої мережі з усіма підключеними пристроями. Ваш пристрій і роутер показуються в центрі, а інші пристрої розташовуються в концентричних колах залежно від залежності від дати підключення. При виборі кнопки сканування маршрутизатора програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, перевірить налаштування безпеки роутера й запропонує виправлення потенційних проблем.

Також як "Безпечні платежі" в Kaspersky, захист банківських операцій у програмному продукті моніторингу й запобігання активності додатків, що був розроблений у даній роботі, автоматично вступає в дію при відвідуванні фінансового сайту. Продукт пропонує запустити сайт у захищеному браузері з можливістю запам'ятати цей вибір.

Система батьківського контролю налаштовується окремо для кожного облікового запису Windows. Залежно від віку дитини застосовуються профілі, які дозволяють блокувати деякі з більше 30 категорій умісту. Можна самостійно налаштовувати фільтрацію. Категорії Кримінал і Шкідливе ПЗ блокуються навіть для аккаунтів дорослих. Компонент добре відробив при тестуванні, але не пропонує розширених функцій, а займається лише фільтрацією контенту й реєстрацією активності.

Спам-фільтр обробляє поштові аккаунти POP3 і IMAP і підтримує інтеграцію з популярними поштовими клієнтами. При використанні підтримуваного поштовика потрібно

налаштувати правило для автоматичної переадресації небажаної пошти в папку спаму. Ваші контакти автоматично попадають у список виключень і ніколи не блокуються. Також доступний чорний список для джерел спаму.

Боїтеся стеження за допомогою веб-камери? Програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, вам готовий допомогти. Ви можете відключити використання веб-камери, коли вона вам не потрібна й дозволити доступ для окремих програм. Програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, може також попереджати при кожній спробі доступу до веб-камери.

Споконвічно здавалося, що додаткові функції повинні не кращим образом позначитися на продуктивності в порівнянні з комплексом початкового рівня. Однак, проведені випробування не виявили помітної різниці. Продукт небагато знижує швидкість завантаження системи й файлових ситуацій, але при реальному використанні помітна з не відчувалася.

Потужний менеджер паролів

Менеджер паролів заснований на Sticky Password Premium, але одержав далеко не всі функції Sticky Password. Наприклад, користувач може синхронізувати паролі між декількома комп'ютерами й Mac, але не пропонує підтримку мобільних пристроїв. Також відсутня функція синхронізація паролів у бездротовій мережі Wi-Fi.

Спочатку потрібно створити майстер-пароль. Спливаюча підказка повідомляє, що майстер-пароль повинен складатися із заголовних, малих літер і цифр, а його довжина повинна бути не менш 8 знаків. Увести пароль можна за допомогою віртуальної клавіатури, щоб перестраховатися від кейлоггерів. Під час моніторингу були перехоплені лише координати курсору, тому небажаний глядач ніколи не довідається, по яких клавішах ви кликали.

Можна налаштувати розблокування менеджера паролів при підключенні якого-небудь USB або Bluetooth пристрою. Проте, це не двофакторна автентифікація, тому що даний спосіб повністю заміняє введення майстр-пароля.

Менеджер паролів підтримують інтеграцію з Chrome, Firefox, Internet Explorer і значним списком менш популярних браузерів: Pale Moon, Comodo Dragon і SeaMonkey. Програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, уміє імпортувати паролі із браузерів, але на відміну від оригінальної версії Sticky Password, не імпортує закладки. Також підтримується імпорт даних з RoboForm, KeePass, LastPass, Dashlane.

Програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, захоплює облікові дані при авторизації на безпечних сайтах. Під час захвата користувач може задати зрозумілу назву для запису й визначити підходящу для неї категорію. Нову групу в цей момент створити не вийде на відміну від LastPass. Однак, в основному вікні менеджера паролів можна створити будь-яку кількість груп, включаючи вкладені групи. Ці категорії стануть пунктами й підпунктами основного меню списку паролів, що розкривається при натисканні по кнопці браузерного розширення.

При повторному відвідуванні програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, пропонує заповнити ваші облікові дані. Продукт упевнено обробляє події зміни паролів. Проте, при відвідуванні сайту з нестандартною формою авторизації, просто зберегти уведені дані не вийде, хоча дана можливість передбачена в LastPass і Sticky Password.

Програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, також захоплює облікові дані при створенні нового аккаунта. Убудований генератор допомагає створити захищений пароль для облікового запису. За замовчуванням програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, генерує 15-значний пароль, що містить заголовні букви, малі літери й цифри. Для посиленого захисту можна додати спецсимволи.

Також як RoboForm, LastPass і деякі інші продукти, програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, уміє захоплювати й підставляти паролі додатків. Просто перетягнете курсор у вигляді хрестика у вікно введення пароля, уведіть дані й збережете запис. Потім програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, сам подбає про автоматичний вхід.

Користувач може створювати кілька профілів – колекцій персональних даних для заповнення веб-форм. Для кожного профілю потрібно ввести персональну, контактну інформацію й ділові дані. При бажанні можна додати реквізити банківських рахунків або кредитних карт. При відвідуванні сторінки з веб-формою, програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, виводить червону границю навколо полів заповнення. Просто натисніть по кнопці панелі інструментів і виберіть бажаний профіль заповнення. Як і багато інших програм, програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, заповнює не всі форми, але в цілому справляється успішно. RoboForm Everywhere 7 спеціалізується на заповненні форм, підтримує більше типів полів, чим конкуренти й допускає кілька записів для одного типу поля.

Програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, не пропонує наочної аналітики паролів, як у випадку з LastPass, Dashlane, або LogMeOnce Password Management. Замість цього він попереджає про паролі з низьким рівнем безпеки. Але не варто всерйоз покладатися на даний рейтинг, тому що 6-значний пароль, що використовує два набори символів буде вважатися нормальним. Слабкий пароль “Monkey” не з'явиться в списку попереджень.

У програмному продукті моніторингу й запобігання активності додатків, що був розроблений у даній роботі, відсутній ще кілька функцій оригінального Sticky Password. Тут недоступна онлайн консоль для керування пристроями. Наприклад, не можна заблокувати менеджер на загубленому пристрої або заборонити додавання нових пристроїв. Функція захищених заміток дозволяє зберігати важливу інформацію, що буде синхронізуватися між пристроями. Портативну версію менеджера паролів теж не вдасться створити в ESET. Навіть без цих функцій, менеджер паролів програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, є потужних інструмент, що по своїх можливостях перевершує багато автономних рішень.

Безпечне шифрування даних

Існує велика кількість ризиків втрати даних. Деякі трояни крадуть приватні дані й відправляють їх кіберзлочинцям. Загублений ноутбук може привести до витоку даних. Нарешті, ваші документи можуть бути доступні цікавим членам родини або колегам по роботі. Кращий спосіб захистити важливі дані – використовувати захищене шифрування. Програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, саме пропонує таку функцію.

Як і схожа функція в Bitdefender Internet Security 2017, Захист даних у програмному продукті моніторингу й запобігання активності додатків, що був розроблений у даній роботі, створює будь-яку кількість віртуальних зашифрованих дисків. Вам залишається ввести назву диска й розташування файлу, що буде містити дані віртуального диска. Ви можете вибрати доступні значення ємності диска: 500 Мб, 1 Гб, 5 Гб, 10 Гб, або 100 Гб або можете вказати довільний обсяг. Додайте пароль, і все готово до роботи.

Сторінка для введення паролів нагадує, що у випадку втрати пароля, ви втратите доступ до ваших файлів, і навіть фахівці програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, не зможуть допомогти. Проте, доступна опція для автоматичної розшифровки диска для поточного облікового запису Windows. Для посиленої безпеки рекомендується відключити цю опцію, якщо ваш аккаунт Windows не захищений дуже сильним паролем.

При розблокуванні, віртуальний диск працює, як і будь-який інший локальний диск. Ви можете переміщати файли на диск і з диска, редагувати вміст і виконувати будь-які інші дії. На відміну від інших аналогічних компонентів в інших продуктах, програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, не має функції примусового блокування захищеного сховища. Це відбувається автоматично при виході з облікового запису або при перезавантаженні комп'ютера.

Немає ніякого сенсу в шифруванні файлів, якщо ви залишаєте незашифровані оригінали. Багато рішень для шифрування поставляються разом з файловими шредерами, які безпечно видаляють оригінальний об'єкт без можливості відновлення. Kaspersky уміє автоматично видаляти оригінали при шифруванні їхніх копій. На жаль, але в програмному продукті моніторингу й запобігання активності додатків, що був розроблений у даній роботі, інструмент безпечного очищення відсутній. Можна використовувати клавіатурне сполучення Shift+Del, у цьому випадку файл буде видалений минаючи кошик, але це не убезпечить від потенційного відновлення.

Створити віртуальне зашифроване сховище можна й на переносному USB-накопичувачі. Процес аналогічний, але не потрібно вказувати ім'я й обсяг. Нова папка з назвою Encrypted з'явиться на флешці, і програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, буде автоматично запитувати пароль при підключенні пристрою. Також можна налаштувати автоматичне розблокування для поточного облікового запису.

Антизлодій

Антизлодій – розповсюджена функція для мобільних антивірусів, у десктопних версіях захист від крадіжки зустрічається нечасто. Bitdefender є одним з деяких конкурентів, які можуть визначати місце розташування, блокувати й стирати дані на пристроях Windows. Функція Антизлодій у програмному продукті моніторингу й запобігання активності додатків, що був розроблений у даній роботі, не підтримує віддалене очищення, але вміє визначати геолокацію пристрою, блокувати його й знімати зображення з веб-камери й скріншоти екрана.

Керування функціями захисту від крадіжки здійснюється на веб-порталі. Спочатку буде запропоновано пройти кроки оптимізації. Якщо на вашім ноутбукі або планшеті Windows настроєний автоматичний вхід без введення пароля, то буде запитана активація входу по паролі. Крім того, буде створений “фантомний аккаунт”.

Програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, кожних 10 минут буде одержувати дані про статус пристрої. Якщо ви пометете пристрій як загублене, то програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, виконає комплекс мір: система буде перезавантажена й буде виконаний автоматичний вхід в “фантомний аккаунт”. Почнеться збір даних про геолокації й передача скріншотів екрана. При бажанні можна вивести повідомлення, наприклад, із проханням повернути пристрій по контактній адресі. Моніторинг буде тривати протягом 14 днів. Програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, повідомить по електронній пошті про закінчення періоду моніторингу.

Під час тестування функція працювала максимально коректно. Після перезавантаження список реальних аккаунтів не відображався й був доступний тільки “фантомний”. Одержати доступ до реальних користувальницьких файлів не вдалося. Система дійсно була заблокована. Програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, кожних 10 хвилин захоплював зображення екрана, і актуальні скріншоти відразу ж з'являлися в онлайн консолі. Роботу функції зняття фотографій з веб-камери перевірити не вдалося через відсутність пристрою.

Для визначення місця розташування програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, аналізує сигнали бездротових мереж. У випадку підключення через Ethernet локація не буде розпізнана. У довідковій

системі повідомляється, що в цьому випадку можна перевірити список IP-адрес, до яких підключається пристрій і визначити зону пошуку. Під час тестування місця розташування пристрої було визначено некоректно – посередині ставка в 13 кілометрах від його реальної локації.

Захист від крадіжки – дійсно корисна функція для ноутбуків. Всі ноутбуки оснащуються модулями бездротового зв'язку, а значить ви зможете відстежити їхнє знаходження. Якщо ви встановили програмний продукт моніторингу й запобігання активності додатків, що був розроблений у даній роботі, на ноутбук, не забудьте пройти кроки оптимізації, просто на випадок, якщо вам знадобляться функції Антизловдія.

Кібербезпека стала першочерговою проблемою в комерційних системах введення даних, чому зловмисники все частіше потребують програмне забезпечення-вразливості програмного та апаратного забезпечення для компрометації інформаційно-технологічної інфраструктури. Нещодавні досягнення свідчать про сплеск використання нових вразливостей для зловмисної діяльності, підкреслюючи критичну потребу в надійному захисті від зловмисних загроз програмного забезпечення

Шкідливе програмне забезпечення – широкий термін, що охоплює шкідливе програмне забезпечення – це фрагмент коду, розроблений кіберзлочинцями для проникнення в комп'ютерні системи без згоди користувача, що є несанкціонованим доступ до даних, знищення файлів та інші шкідливі дії [1], [2]. Зростання інформаційних технологій посилює серйозність шкідливого програмного забезпечення як основну загрозу.

Традиційні методики визначення на основі програмного забезпечення, які базуються на аналізі сигнатур стикаються з такими недоліками продуктивності, як обмеження статичного аналізу, неможливість виявлення обфускованих та важких обчислювальних витрат, особливо на системи з обмеженими ресурсами.

Ці проблеми сприяють через обмеження обчислювальної потужності та пропускну здатності зв'язку середовища інтегрованих систем [3], [4], [5]. Для вирішення цих викликів вкрай необхідно розвивати ефективні та економічно вигідні контрзаходи кібербезпеки, зосереджуючись на захисті інформаційних користувачів та пом'якшення нових кіберзагроз [6].

Це забезпечує парадигму переходу до інтеграції заходів безпеки в базове апаратне забезпечення, встановлюючи підхід «знизу вгору» для зміцнення комп'ютерного використання пристроїв, а не ставлення до безпеки як до другорядної [7]. У системах, дали успішних програм у різних галузях, особливо в підвищенні системи безпеки [8], [9], [10].

Нещодавні дослідження підкреслюють важливість визначення шкідливих дій на рівнях апаратного забезпечення та архітектури процесорів через його швидкість, ефективність та меншу видимість для наявних експлуатацій зловмисника.

З цим призначено апаратно-допоміжне шкідливе програмне забезпечення Методи виявлення (HMD), зокрема, з використанням машинного навчання з використанням функції продуктивності апаратного лічильника (HPC), з'являється як рішення недоліків традиційного програмного виявлення шкідливих програм [11], [12], [13], [14], [15].

Високопродуктивні процесори (HPC) – це спеціалізовані регістри в межах системи продуктивності. Блок моніторингу (PMU), вбудований в сучасні мікропроцесори, відстежують події апаратного забезпечення програми (наприклад, кількість виконаних циклів, інструкцій, пов'язаних з ними промахів кешу тощо)[16], [17], [18], [19].

Крім того, технології машинного навчання продемонстрували ефективність виявлення та класифікації аномалій у межах простору низького рівня оцінки. Використовуючи машинне навчання, системи можуть ефективно розпізнавати потенціал загрози та проактивно реагувати на зміни в поведінці в реальний час [7], [20].

Поточні дослідження в галузі інтелектуального виявлення шкідливих програм на Рівень апаратного забезпечення охоплюють різні обчислювальні платформи, такі як вбудовані системи, Інтернет речей і високонавантажені системи продуктивності.

Переважно використовуємо найсучасніші дослідження HMD-особливо наголошуємо на розробці та розробці стандартів передових методів машинного навчання для протидії еволюції загрози шкідливого програмного забезпечення.

У даній роботі наведено поглиблений аналіз апаратно-допоміжних методи виявлення шкідливого програмного забезпечення, зосереджені на останніх досягненнях у використанні штучного інтелекту та машинного навчання для покращення захисту систем від шкідливих нападів.

Зростання кількості та складності інфекцій шкідливим програмним забезпеченням впливає на окремих осіб та організації. Ці шкідливі програми з різноманітними функціональними можливостями розроблені для шкідливих цілей, таких як дистанційне керування, крадіжка даних, несанкціонований доступ, знищення файлів та проведення атак типу «відмова в обслуговуванні» [1], [10].

Наведемо огляд процесу підходів на основі машинного навчання, розроблених для підвищення кібербезпеки, зокрема в контексті апаратного виявлення шкідливого програмного забезпечення. Цей процес охоплює етапи від моніторингу програм для профілювання даних високопродуктивних обчислень, розробки функцій та навчання детекторів на основі машинного навчання та онлайн-выводу. Безперервне навчання моделей машинного навчання шляхом аналізу низькорівневих мікроархітектурних особливостей має на меті розпізнавання та протидію шкідливим шаблонам. Цей проактивний та інтелектуальний підхід захищає архітектуру процесора від потенційних загроз, що охоплюють не лише шкідливе програмне забезпечення, але й атаки по мікроархітектурних бічних каналах [21], [22].

Розробка ефективних апаратних детекторів шкідливого програмного забезпечення на основі машинного навчання починається з таких ключових кроків, як збір даних та вибір функцій [7], [11], [14], [16]. У сучасних мікропроцесорах можна збирати численні мікроархітектурні події, але вибір відповідних низькорівневих функцій є важливим для уникнення обчислювальної складності та затримок, пов'язаних з високовимірними наборами даних. Зокрема, ідентифікація суттєвих низькорівневих мікроархітектурних функцій є критично важливою для апаратного виявлення шкідливого програмного забезпечення з кількох причин:

- Велика кількість мікроархітектурних подій (наприклад, 100+ в Intel Xeon) призводить до високовимірних даних [14].

- Обробка необроблених наборів даних передбачає обчислювальну складність та спричиняє затримки [23].

- Вибір відповідних мікроархітектурних подій створює труднощі у визначенні нетривіальних подій для різних класів шкідливих програм [15].

Ця проблема ускладнюється обмеженою доступністю регістрів НРС у різних процесорах, зазвичай від 2 до 8.

Проблема обмеженої кількості регістрів НРС, тісно пов'язана з виявленням шкідливого програмного забезпечення під час виконання, обговорює значну проблему HMD, розглянуту в нещодавніх роботах [14], [15]. Вона включає визначення мінімального набору НРС, які точно фіксують характеристики шкідливих атак, тим самим мінімізуючи непотрібні обчислювальні витрати. Це прагнення забезпечує розробку ефективного контрзаходу безпеки на основі машинного навчання з мінімальним впливом на продуктивність системи. Щодо обмежень архітектури базового процесора, особливо в обчислювальних платформах з обмеженими ресурсами, таких як вбудовані системи та пристрої Інтернету речей з обмеженими регістрами НРС, ефективне, але точне виявлення під час виконання залежить від вибору критичних ознак. Нещодавні дослідження HMD, такі як [14], [15], [19], розглядали ефективне HMD під час виконання, визначаючи мінімальний набір основних подій лічильника продуктивності, необхідних для збору даних за один прогін.

Існує чотири основні кроки процесу розробки ознак:

– Очищення ознак включає аналіз необроблених даних для пошуку порожніх записів, викидів та будь-яких інших аномальних записів даних, щоб їх можна було видалити з процесу машинного навчання. Це також може забезпечити зворотний зв'язок для покращення збору даних.

– Нормалізація ознак є критичним кроком для масштабування табличних даних вздовж значень стовпців або рядків, запобігаючи домінуванню деяких даних або ознак з великими значеннями в процесі навчання. Цей метод є ефективним, особливо для алгоритмів машинного навчання, які чутливі до значень відстані між ознаками. Поширені методи нормалізації включають нормалізацію L1/L2 та нормалізацію MinMax.

– Вибір ознак включає аналіз важливості ознак, аналіз кореляції ознак та вибір найкращих ознак. Цей процес зазвичай виконується офлайн та ефективно тестується для цільової моделі машинного навчання.

– Вилучення ознак полягає у вилученні записів даних з найкращими ознаками для формулювання навчального набору даних. На етапі онлайн-виведення це означає вилучення онлайн-даних, які мають ті ж найкращі ознаки та розмірність, що й навчальний набір для обробки висновків за допомогою детекторів машинного навчання.

Вибрані ознаки високопродуктивних обчислень використовуються для навчання окремих детекторів на основі машинного навчання. Класифікатор прагне встановити кореляцію між значеннями ознак та поведінкою програми, прагнучи передбачити наявність шкідливих шаблонів (доброякісних або типу атаки). Кілька методів вибору ознак відіграли важливу роль у попередніх зусиллях НМД на основі машинного навчання. До них належать такі методи, як оцінка атрибутів кореляції [14], [24], [25], [15], [26], [27], аналіз головних компонент [15], [26], [28], оцінка коефіцієнта підсилення [16], [19], [29] та оцінка Фішера [30], [12].

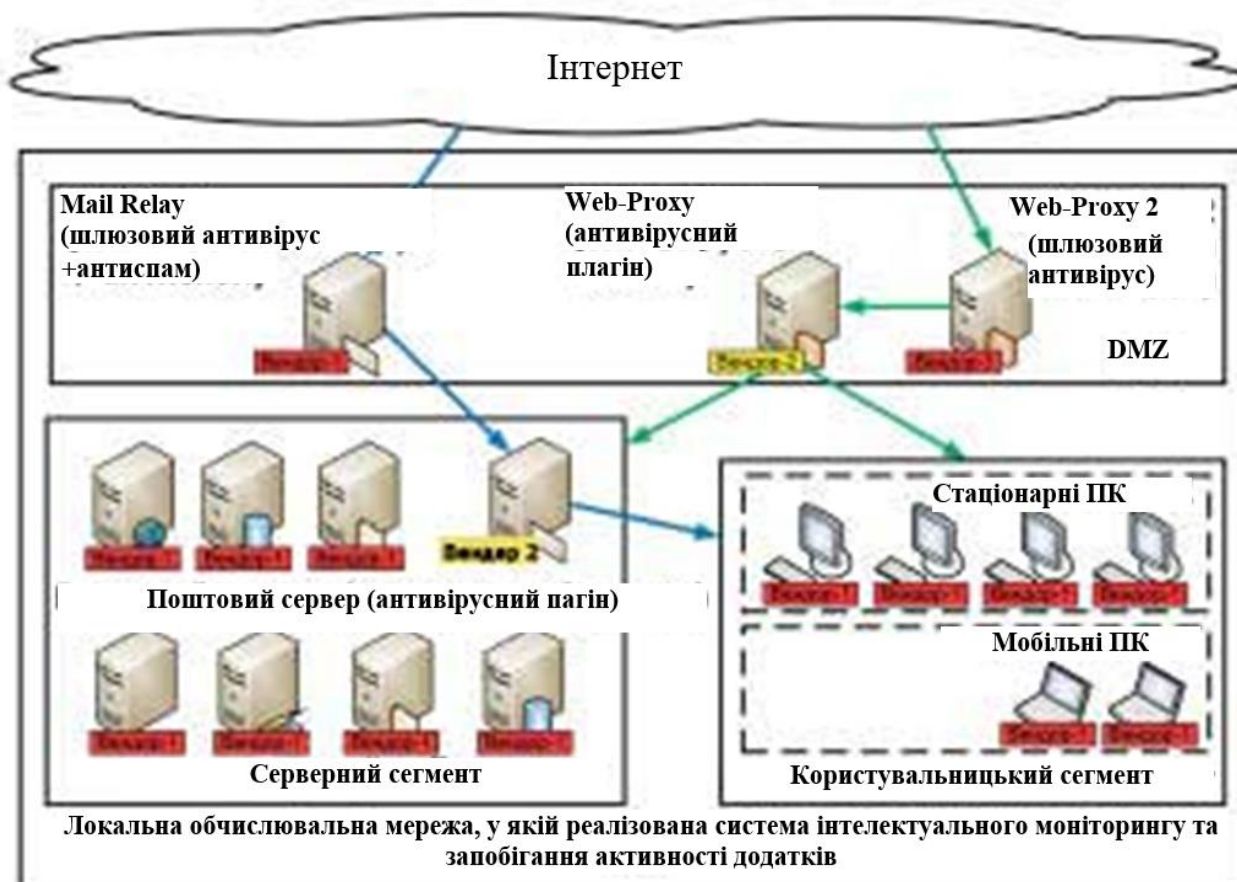


Рисунок 1 – Структурна схема системи

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів інтелектуального моніторингу та запобігання активності додатків. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем інтелектуального моніторингу та запобігання активності додатків.
- Досліджена система інтелектуального моніторингу та запобігання активності додатків.
- На основі отриманих результатів досліджень створена програмна реалізація системи інтелектуального моніторингу та запобігання активності додатків.

Розроблені алгоритми дозволяють успішно вирішувати завдання інтелектуального моніторингу та запобігання активності додатків. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Усік, П.С., Смірнова, Т.В., Буравченко, К.О., Смірнов, О.А., Улічев, О.С., Смірнов, С.А. «Дослідження технологій забезпечення кібербезпеки банківських систем з використанням штучного інтелекту». Кібербезпека: освіта, наука, техніка. 2025. Том 1 № 29. С.704–716, 2025
2. Kuznetsov, O., Frontoni, E., Kuznetsova, K., Arnesano, M., Smirnov, O. «A secure biometric authentication architecture for blockchain-driven cyber-physical systems». Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications, 2025, pp. 193–224.
3. Kuznetsov, O., Atzeni, G., Arnesano, M., Randieri, C., Smirnov, O. «Secure IoT-based smart wheelchair system: From implementation to security enhancement strategy». Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications, 2025, pp. 225–257.
4. Kuznetsov, O., Smirnov, O., Kuznetsova, T., Shaikhanova, A., Svatowsky, I. «Privacy-utility trade-offs in IoT networks: A comparative analysis of differential privacy mechanisms for sensor data aggregation». Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications, 2025, pp. 589–622.
5. Lakhno, V., Malyukov, V., Smirnov, O., Bebesko, B., Chubaievskiy, V., Zhumadilova, M., Malyukova, I., Smirnov, S. «Multifactorial Model for Targeted Attacks Counteracting Within the Framework of a Multi-Step Quality Game with Fuzzy Information». 8th International Symposium on Intelligent Informatics, ISI 2023, 2025. vol 389. pp 377-389. Springer, Singapore.
6. Kuznetsov O., Frontoni E., Kuznetsova Y., Smirnov O., Moskovchenko I. «Trust-Based Security Architecture for Edge Computing: A Simulation Study of Dynamic Trust Evolution and Attack Detection». CEUR Workshop Proceedings, 2024, 3909, pp. 227–241.
7. Kuznetsov, O., Frontoni, E., Kryvinska, N., Chevardin, V., Smirnov, O. «Wireless Network Encryption Stream Ciphers, Computational Modeling, and Security Analysis». Computational Modeling and Simulation of Advanced Wireless Communication Systems, 2024, pp. 379–402.
8. Kuznetsov, O., Frontoni, E., Kryvinska, N., Smirnov, O., Imoize, G.L. «Computational Modeling of Enhanced Spread Spectrum Codes for Asynchronous Wireless Communication». Computational Modeling and Simulation of Advanced Wireless Communication Systems, 2024, pp. 403–447.
9. Ткаченко, О., Ільченко, А., Улічев, О., Мелешко, Є., Смірнов, О. «Правові засади поширення інформаційних впливів в соціальних мережах». Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2024. № 2(26), С. 170–188.
10. Смірнова Т.В., Коноплицька-Слободенюк О.К., Буравченко К.О., Смірнов С.А., Кравчук О.В., Козірова Н.Л., Смірнов О.А. «Дослідження технологій забезпечення кібербезпеки хмарних сервісів IaaS, PaaS та SaaS». Кібербезпека: освіта, наука, техніка. 2024. №4(24), С. 6-27.
11. Вінтенко, Б., Миронець, І., Смірнов, О., Кравчук, О., Козірова, Н., Савеленко, Г., Коваленко, А. «Дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». Кібербезпека: освіта, наука, техніка. 2024. №3(23), С. 111-131.
12. Батрак О., Смірнова Т., Гнатюк В., Одарченко Р., Смірнов О. «Дослідження показників ефективності функціонування та перспектив розвитку систем IP-телефонії». Підводні технології, 2024, № 13, с. 28-35.
13. Kuznetsov, O., Kryvinska, N., Ilchenko, O., Smirnova, T., Ulianovska, Y. «Comparative Analysis of Cryptocurrency Trading Platforms Using the Analytic Hierarchy Process». CEUR Workshop Proceedings, 2023, 3628, pp. 106-115.
14. Akhalaia, G., Iavich, M., Iashvili, G., Prisyazhnyy, D., Smirnova, T. «Secure Encrypted Connection on Georgian Website». CEUR Workshop Proceedings, 2023, 3550, pp. 313-320.
15. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving

- the user experience of subscribers in software-configured networks based on the use of machine learning». *Advanced Information Systems*, 2023, 7(2), pp. 49-56
16. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchov, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». *CEUR Workshop Proceedings*, Volume 3530, 2023, pp. 256-265.
 17. Kuznetsov, O., Kandiy, S., Frontoni, E., Smirnov, O. «Trade-offs in Post-Quantum Cryptography: A Comparative Assessment of BIKE, HQC, and Classic McEliece». *CEUR Workshop Proceedings*, Volume 3504, 2023, pp. 1-11.
 18. Smirnov, O., Lakhno, V., Akhmetov, B., Chubaievskiy, V., Khorolska, K., Bebesko, B. «Selection of a Rational Composition of Information Protection Means Using a Genetic Algorithm». In: Rajakumar, G., Du, K.L., Vuppapapati, C., Beligiannis, G.N. (eds) *Intelligent Communication Technologies and Virtual Mobile Networks. Lecture Notes on Data Engineering and Communications Technologies*, vol 131. 2023. Springer, Singapore. pp. 21-34.
 19. Смірнова Т.В., Гнатюк С.О., Бердибаєв Р.Ш., Сидоренко В.М., Жигаревич О.К., «Система корелювання подій та управління інцидентами кібербезпеки на об'єктах критичної інфраструктури». *Кібербезпека: освіта, наука, техніка*, №3(19), 2023, С. 176-196.
 20. Смірнов О.А. Козлов Я.О., Смірнова Т.В. «Дослідження застосування SIEM-систем для забезпечення кібербезпеки та захисту інформації». II Міжнародна науково-практична Інтернет-конференція «Інновації та перспективні шляхи розвитку інформаційних технологій (ІПШРІТ-2023)» м.Черкаси 6 грудня 2023 року – Черкаси: ЧДТУ.– 2023. – С.251-252.
 21. Козлов Я.О., Смірнова Т.В., Смірнов О.А. «Дослідження SIEM-систем для забезпечення кібербезпеки». VII міжнародна науково-практична конференція “Інформаційна безпека та комп’ютерні технології” до 30-ти річчя кафедри кібербезпеки та програмного забезпечення, м.Кропивницький. 1 листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 26.
 22. Козлов Я.О., Козірова Н.Л., Смірнов О.А. «Дослідження структури та принципу роботи SIEM-системи». VII міжнародна науково-практична конференція “Інформаційна безпека та комп’ютерні технології” до 30-ти річчя кафедри кібербезпеки та програмного забезпечення, м.Кропивницький. 1 листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 59.
 23. Вінтенко Б.Ю., Смірнов О.А., Коваленко О.В., Смірнов С.А., Коваленко А.С. «Дослідження нормативних документів та галузевих стандартів розробки програмного забезпечення комп’ютерних систем управління АЕС, важливих для безпеки». *Системи управління, навігації та зв’язку*, 2023, вип. 2(72), С. 170-178.
 24. Smirnov, O., Neskordieva, T., Fedorov, E., Rudakov, K., Neskordieva, A. «Method Detection Audit Data Anomalies on Basis Restricted Cauchy Machine» *CEUR Workshop Proceedings*, Volume 3187, 2022,
 25. Smirnov O.A., Al-Oraiqat A.M., Ulichev O.S., Meleshko Ye.V., Al-Rawashdeh H.S., Polishchuk L.I. «Modeling strategies for information influence dissemination in social networks». *Journal of Ambient Intelligence and Humanized Computing* Volume 13, Issue 5. Springer, Cham. 2022, pp. 2463-2477.
 26. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». *Проблеми інформатизації та управління*, № 2(70). 2022. С. 28-37.
 27. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» *Системи управління, навігації та зв'язку*, 2022, № 3(69). С. 93-98.
 28. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» *Вісник Хмельницького національного університету. Серія: «Технічні науки»*, № 2 (307). С. 46-52. 2022.
 29. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» *Системи управління, навігації та зв'язку*, 2022, № 1(67). С. 84-89.
 30. Smirnov O., Kuznetsov A., Zhora V., Onikiychuk A., Pieshkova O. «Hiding Messages in Audio Files Using Direct Spread Spectrum». 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2021, Cracow, Poland, 22-25 September 2021. P. 414-418
 31. Smirnov O., Kuznetsov A., Lokotkova I., Kuznetsova T., Florov S., Lebid O. «Using Orthogonal Signals to Hide Information in Images». 4 IEEE International Conference on Advanced Information and Communication Technologies (AICT) - 2021, Lviv, Ukraine, September 21-25, 2021. P. 255-260.

УДК 004

О. Сопіна, магістр гр. КІ-24Мз,

Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ЗБОРУ ТА ОБРОБКИ АНАЛІТИКИ ВІД МЕРЕЖІ WI-FI

У статті розроблено програмне забезпечення, яке призначено для системи збору та обробки аналітики від мережі Wi-Fi. Метою розробки є дослідження та принципи побудови системи збору та обробки аналітики від мережі Wi-Fi. Об'єктом дослідження є процес збору та обробки аналітики від мережі Wi-Fi. Предметом дослідження є методи збору та обробки аналітики від мережі Wi-Fi. Методи дослідження базуються на методах інформації, методах теорії комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи збору та обробки аналітики від мережі Wi-Fi. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

збір та обробка аналітики, Wi-Fi

Постановка проблеми. Мережі Wi-Fi стають не тільки засобом підключення користувачів, але й інструментом для навігації й збору різних даних. Такі дані дозволяють визначити, наскільки ефективно використовуються площі об'єкта (офісу, магазину, транспортного вузла та ін.), здійснювати персоніфікований маркетинг, контролювати роботу співробітників і т.д.

Один із проектів, де здійснюється збір даних у мережі Wi-Fi для наступної аналітики, вирішує кілька завдань, у тому числі облік часу присутності співробітників на робочих місцях. Це завдання реалізується за допомогою відстеження активності MAC-адреси корпоративного смартфона з SMS-повідомленнями керівництва про запізнення його власника. Крім того, система фіксує факт виявлення смартфона клієнта тільки він з'явиться на території салону на підставі його MAC-адреси. Це дозволяє реалізувати більше ефективну, проактивну роботу із клієнтом, коли на комп'ютер співробітника відразу виводиться вся історія взаємин з ним і іншою корисною інформацією.

Також функції аналітики реалізовані й у мережі Wi-Fi, з гіперлокацією забезпечує навігацію відвідувачів, а також функцію аудіогіду в мобільному застосунку. Співробітникам надається інформація з переміщень відвідувачів.

Рішення Wi-Fi розвиваються також у напрямку розширення різноманіття архітектур таких мереж, завдяки чому підвищується гнучкість реалізації мережі для замовників різного масштабу. Базовий варіант, вигідний для невеликих інсталяцій, – використання контролера, убудованого в точку доступу. Такі рішення є в портфелі продуктів всіх основних гравців ринку Wi-Fi, включаючи компанії Cisco і Ruckus.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи збору та обробки аналітики від мережі WI-FI.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи збору та обробки аналітики від мережі Wi-Fi.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем збору та обробки аналітики від мережі Wi-Fi.
- Дослідження системи збору та обробки аналітики від мережі Wi-Fi.
- Програмна реалізація системи збору та обробки аналітики від мережі Wi-Fi.

Об'єктом дослідження є процес збору та обробки аналітики від мережі Wi-Fi.

Предметом дослідження є методи збору та обробки аналітики від мережі Wi-Fi.

Методи дослідження базуються на методах інформації, методах теорії комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Wi-Fi аналітика – технологія збору, обробки й аналізу даних за допомогою Wi-Fi сенсорів. Всі мобільні пристрої із включеним Wi-Fi (а по статистиці це 50-60% всіх пристроїв) передають у простір сигнал з MAC-адресою – унікальним ідентифікатором мобільного телефону. До слова, він не ставиться до персональних даних. Спеціальні сенсори вловлюють сигнал, обробляють і передають у закодованому виді на хмарні сервери. Зібрана інформація впорядковується й аналізується. У такий спосіб ви одержуєте розгорнуту інформацію про своїх відвідувачів, їхній кількості й витраченому в магазині часу, частоті візитів, нових/лояльних клієнтах, перехожих, про збіглих без покупки, про прохідність точки й т.д.

Бездротова аналітика також може сполучати офлайн- і онлайн-дані й допомагає побачити реальний портрет (профіль) аудиторії: стать, вік, інтереси в інтернеті, тип/марку мобільного пристрою та ін. Зібрані аудиторії (MAC-адреси) завантажуються в DMP Google і MyTarget (Gmail.com) для таргетування на них інтернет-реклами. Клієнт може вибрати різні сегменти, наприклад, «регулярно минаючі повз мій магазин» і «що зайшли й пробули в магазині менш 2-х хвилин», і показувати їм різні, максимально персоніфіковані рекламні повідомлення.

Основні сфери застосування технології – ритейл, ТРЦ, фаст-фуди, ресторани, кафе, автоцентри, банки, e-commerce, реклама, BTL.

Що може Wi-Fi аналітика

Можна виділити три важливі можливості Wi-Fi аналітики:

1. Доганяти потрібну аудиторію в онлайні й офлайні. Усі знають, як працює ремаркетинг у пошукових системах в інтернеті – ви вводите запит «як відсвяткувати день народження дитини в Кропивницькому» і потім вас цілий місяць переслідують баннери дитячих розважальних центрів. Точно таку ж можливість «доганяти потрібну аудиторію» Wi-Fi аналітика надає й в офлайні. Наприклад, потенційний клієнт зайшов у магазин побутової техніки в пошуку холодильника. Походив по відділі, подивився різні моделі й пішов, нічого не купивши (не знайшов підходящий варіант, вирішив пошукати дешевше, не було необхідної суми). І отут його починає «переслідувати» реклама холодильників – в інтернеті або в digital indoor (внутрішня, інтер'єрна реклама на екранах).

2. Визначати/підрхувати, хто з побачивших рекламу фізично прийшов у магазин. Як звичайно оцінюється ефективність реклами? В інтернеті – переглядами, кліками, дзвінками, лідами, онлайн-покупками. У зовнішній і внутрішній рекламі – забійним питанням «звідки ви про нас довідалися?» і промокодами. А якщо ви рекламуєте товар, якому можна купити тільки в офлайн-магазині? Нові технології дозволяють зв'язати рекламу в інтернеті з офлайн-бізнесом клієнта. Завдяки їм ви можете визначити й порахувати, хто з побачивших рекламу, прийшов у звичайний магазин.

3. Таргетувати рекламу в інтернеті на офлайн-аудиторію. Маркетологи добре знають, як шукати цільову аудиторію в інтернеті: таргетинг по інтересах, соціально-демографічним показникам, геолокації й т.д. І багато хто з них знають, що незважаючи на всі ці інструменти, ефективність подібної реклами щороку знижується, а її вартість, навпаки, росте. Як зачепити аудиторію, що регулярно проходить повз наш магазин і не заходить у нього?

Або як «наздогнати» рекламою тих, хто зайшов, але в підсумку пішов без покупки? Один з дідівських способів – поставити біля магазину промоутера або ростову ляльку з рекламними листівками або рекламний показчик. Можна написати на вітрині «знижки 200%». Але все це вже не чіпляє. Тепер можна таргетувати рекламу в інтернеті на офлайн-аудиторію. Наприклад, на ті, хто брав участь у Кропивницькому напівмарафоні й любить біг.

І це все теж дозволяє зробити Wi-Fi аналітика. Насправді такими можливостями вже щосили користуються в усьому світі, у тому числі в Україні.

Як це працює

Приклад 1. Український автодилер (преміум сегмент) проводив «виїзний» 3-денний тест-драйв. У зоні експонування авто був установлений Wi-Fi сенсор, що збирав інформацію про минаючих мимо в радіусі 20 метрів, а також тих, хто бачив рекламу й/або брав участь у тест-драйві. Також Wi-Fi сенсори були встановлені в самому дилерському центрі. Дані збиралися з декількома цілями: оцінити ефективність заходу – визначити скільки в підсумку людей приїде в дилерський центр, використовувати зібрані дані для наступного таргетування реклами в інтернеті.

Результати кампанії:

- Зібрано 4866 унікальних mac-адрес.
- 13 чоловік прийшли в дилерський центр протягом 1,5 місяців після заходу.

Приклад 2. Великий ритейлер побутової техніки й електроніки, магазини якого перебувають у торгових центрах Кропивницька, збирав дані з метою:

- Одержати розгорнуту статистику й аналітику по відвідувачах магазинів (включаючи перехожих).
- Використовувати зібрані аудиторні сегменти для наступної комунікації в Інтернеті.
- Оцінити ефективність інтернет-реклами – порахувати скільки людей, її що побачили, прийшло в магазини клієнта.

До початку рекламної кампанії в інтернеті Wi-Fi сенсори збирали дані в магазинах кілька місяців. За цей час із всіх зібраних MAC-адрес були відібрані ті, хто проходив повз магазин більше двох разів на місяць, але жодного разу в нього не зайшов. Для кожного магазину було розроблено 5 баннерів з різними товарами й вказівкою адреси торгового центра, де перебуває магазин. Баннери розміщалися в інтернеті з таргетуванням на відвідувачів торгового центра, які проходили мимо «наших» магазинів. Тобто. люди бачили баннери з адресами торгових центрів, у яких регулярно бувають. Паралельно з рекламою в інтернеті сенсори збирали MAC-адреси відвідувачів «наших» магазинів і визначали тих, хто прийшов сюди завдяки побаченій рекламі.

Результати кампанії:

- 7% побачивших інтернет-рекламу фізично прийшли в магазини в період рекламної кампанії + 2 тижні.
- Кількість нових відвідувачів у цей період виросло на 6,5% у порівнянні з аналогічним періодом минулого місяця.
- Близько 50% нових відвідувачів у цей період прийшли завдяки рекламі (або як мінімум бачили рекламу).
- Частка тих, хто зайшов у магазини із загального потоку минаючих мимо серед тих, хто бачив рекламу, майже в 2 рази вище аналогічного показника по загальній аудиторії.

Хочу відзначити, що не треба критично ставитися до цифр, оцінювати їх з погляду багато/мало, ефективно/неефективно. Ця інформація дає поле для того, що і як потрібно поліпшувати.

Уявіть собі, ми можемо проаналізувати шлях покупців із продуктовими візками: як і де вони переміщалися. На підставі цього можна поліпшити мерчендайзинг, вивчити які товари з яких груп купують разом і багато чого іншого. Але сам цікаве починається тоді, коли людина вже приходить на касу: час, проведений у магазині, маршрут і його підсумкову покупку можна синхронізувати, і цю інформацію організація-замовник може також сполучити зі своєю програмою лояльності.

Офлайн метрики

Будь-який сучасний телефон має модуль Wi-Fi, і якщо він включений (а звичайно він включений), те без ведення власника починає відправляти множинні сигнали. Ці хлопці «ловлять» сигнали за допомогою встаткування TP-Link і свого прошивання. У сигналі

втримується MAC адреса телефону, потужність, з якої сигнал був відправлений, і час його відправлення. Є більше 15 різних офлайн-метрик, які можна розрахувати на основі цих даних. От деякі з них:

- **Entry rate** – метрика, що показує, скільки людей пройшло повз локацію і яку їхню частину зайшла в неї. Entry rate дозволяє оцінити потенціал локації, обсяги аудиторії, з якої працює бізнес, а також проаналізувати результативність тої або іншої маркетингової активності. Завдяки тому, що MAC адреса – це індивідуальний ідентифікатор телефону й, як правило, вона не повторюється, з його допомогою оцінюються такі параметри як «новий відвідувач», «повторний відвідувач» та ін.

- **Частотність** – це важливий параметр особливо для рітейла. Ця метрика показує частоту, з якої приходять нові або повторні відвідувачі в той або інший об'єкт, можна побачити цикл повторного відвідування.

- **Маршрути**. Якщо є кілька точок збору даних, можна проаналізувати маршрути відвідувачів, частку людей, що заходять у певні приміщення (магазини) і т.п. Можна поєднувати людей у групи й аналізувати, як вони, відвідавши орендаря X, направилися до орендаря Y, зайшли в кінотеатр і так далі – і на основі цієї інформації розвивати програму лояльності.

Зараз багато хто намагаються працювати з лояльною масою аудиторії, тому що купівельна спроможність населення знижується. У торгових центрах, наприклад, на 80-85% лояльна аудиторія, тому що відвідувачі – це в основному жителі прилеглих будинків або працівники офісів. Тому торгові центри намагаються залучати їх, преміювати за відвідування й стимулювати покупки.

- **Середній час**. Це те, що впливає на наші покупки, адже чим більше часу ми проводимо в магазині, тим вище ймовірність, що ми щось купимо. З торгового центра взагалі складно піти без покупки: там більше можливості провести величезна кількість часу й, відповідно, що-небудь придбати, сходити в кіно й т.д.

- **Перетинання** – ще одна дуже цікава метрика для бізнесу. Ця метрика показує куди ще ходять відвідувачі однієї локації усередині еко-системи Wi-Fi аналітики, включаючи парки розваг, спортивні об'єкти. Ці дані, наприклад, дозволяють компанії краще розуміти поведінковий портрет свого споживача.

Режими роботи

Устаткування TP-Link може працювати в різних режимах.

- **Надання доступу в інтернет для персоналу й відвідувачів**. Ми пропагуємо Wi-Fi не тільки як сервіс для відвідувачів, але і як вигідний ресурс для бізнесу й замовника. Зараз доступ в інтернет для відвідувачів – збиткова стаття для багатьох компаній. Ми ж бачимо можливість зробити надання Wi-Fi для відвідувачів дохідною статтею.

- **Інструмент рекрутингу в програму лояльності**. Wi-Fi – це спосіб комунікації із клієнтом. Комунікувати із клієнтом можна по-різному. Наприклад, користувач, що підключився до гостьового Wi-Fi, побачив баннер/відео й т.д. – це вже комунікація. Але ми йдемо ще далі, створюємо складні інтеграційні системи із замовником. Wi-Fi може бути інструментом рекрутингу в програму лояльності.

Наприклад, можна зробити зв'язування між системою Wi-Fi-аналітики й CRM-системою замовника й, коли відвідувач підключається до мережі, запускати кілька сценаріїв.

Один з таких сценаріїв – коли користувач повторно підключається до мережі замовника – наприклад, в іншій кав'ярні або ресторані однієї мережі. За законом про надання публічних Wi-Fi мереж при підключенні користувач зобов'язаний залишити контактні дані й підтвердити номер телефону. Оскільки система єдина, при першому підключенні MAC-адреса користувача й номер його телефону зберігається в загальній базі. І наступного разу, коли той же користувач скористається Wi-Fi в іншій кав'ярні мережі, йому не прийде проходити авторизацію повторно.

Ще один сценарій – у момент, коли користувач підключається до мережі замовника, у якого Wi-Fi використовується як інструмент рекрутингу в програмі лояльності, CRM системі вже передали питання: чи є цей користувач учасником вашої програми лояльності. Якщо «ні», тоді користувачеві показується анкета або будь-яка інша форма, де потрібно заповнити лише часткову інформацію (наприклад, ПІБ, статі, вік), а номер телефону там уже є. Йому залишається тільки підтвердити – і анкета відразу ж летить в CRM-систему, а на смартфоні або планшеті користувача відразу ж відкривається особистий кабінет. Такий сценарій полегшує взаємодія й підвищує ймовірність, що користувач стане учасником програми лояльності замовника.

Один великий клієнт системи Wi-Fi аналітики Shopster активно користується цим інструментом, але в цьому випадку відбувається не рекрутинг у програму лояльності, а наступне.

Тригерна платформа

Важлива синергія між продуктом аналітики й продуктом hotspot. Коли є зв'язування MAC адреса + номер телефону, далі система може працювати як **тригерна платформа**. Наприклад, візьмемо ювелірний магазин. Ми бачимо, що користувач проходить повз магазин з ювелірними прикрасами. Ми цю інформацію передаємо в CRM-систему замовника в режимі реального часу, і вона бачить, що такий номер є в базі й він часто купує ювелірні прикраси. Замовник розуміє, що він може комунікувати із цим користувачем: відправити SMS, наприклад, про наявні бонуси або повідомлення про закритий розпродаж. В підсумку потенційний покупець одержує цікаву пропозицію саме тоді, коли він проходить повз вітрину замовника. Виходить таке зв'язування програми лояльності, аналітики й hotspot.

При типовому сценарії SMS-ки з акціями майже завжди приходять не вчасно. Наприклад, ви будинку, а який-небудь відомий спортивний бренд надсилає SMS, про те, що на вашім рахунку скопилось 1000 бонусів і їх потрібно витратити до кінця вихідних. Навряд чи це спонукає вас зібратися, поїхати в магазин і щось купити. Ідея – зробити те, що зараз у світі інтернет-маркетингу називається «Супер Гео Комунікацією». Тобто система Wi-Fi аналітики працює як тригер – «ловить» MAC адресу й номер телефону користувача й передає в систему замовника. Останній же (якщо в нього є дозвіл) будує з користувачем комунікацію: відправляє SMS у потрібний момент.

Як це працює?

Устаткування TP-Link із прошиванням, установлене в різних магазинах і торгових центрах, ловить MAC адреси, які надалі передаються в розроблювальну в даній роботі систему, де відбувається розпізнавання по MAC адресі, який номер телефону йому належить. Заздалегідь сформований замовником текст SMS повідомлення від імені Wi-Fi.cntu.ua відправляється людині, що у певний момент проходить повз магазин. Імовірність «зачепити» минаючого повз людину істотно збільшується.

Інструмент сполучення онлайн з офлайн

Ще один новий продукт – інструмент сполучення онлайн із офлайн. Устаткування TP-Link разом із прошиванням стали містком, що з'єднує фізичний мир і мир інтернету. Не секрет, що в інтернеті всі сайти стежать за користувачами, вони вішають на них Cookie файли, а розроблювальна в даній роботі система збору аналітики від мережі Wi-Fi, ловить їх MAC адреси. Отож, розроблювальна в даній роботі система збору аналітики від мережі Wi-Fi, навчилася сполучати Cookie з MAC адресами: розроблювальна в даній роботі система збору аналітики від мережі Wi-Fi передає їх великим інтернет-площадкам, і розпізнавання відбувається на їхній стороні. От що це дає:

- Можна сформулювати більше чітке подання про інтереси й не тільки своєї цільової аудиторії.

- Можна оцінити ефективність інвестицій у рекламу (контекстна реклама, баннери й т.д.) – наприклад, конверсію від реклами в інтернеті. Раніше класичному офлайн-бізнесу це було досить складно зробити. Зараз Wi-Fi аналітика від розроблювальна в даній роботі система збору аналітики від мережі Wi-Fi може допомогти – за допомогою збору MAC адрес

в офлайн режимі, наприклад, можна виявити скільки людей з тих, хто подивився рекламу онлайн, відвідало офлайн-локацію, і багато чого іншого.

– Також ці дані можна використовувати з метою ретаргетинга – можна зібрати аудиторію, що прийшла в конкретний магазин, в один сегмент і надати її замовникові. Після цього замовник може дуже таргетовано або «Супер Гео» направити онлайн-комунікацію цим користувачам, затягти їх, стимулювати їхню зворотність і в такий спосіб розвивати лояльність. Це новий продукт, яким починають користуватися багато клієнтів.

Ще один продукт на стику мережного встаткування, ПЗ й Bluetooth технологій: у пристрій вставляється Bluetooth адаптер з модифікованим прошиванням, і з'являється можливість працювати з iBeacon або Eddystone, що забезпечує досить точну навігацію усередині приміщень (Indoor navigation).

Indoor navigation може існувати як самостійний продукт для відвідувачів (така навігація вже працює в одному із центральних ТРЦ Москви (клієнт розроблювальна в даній роботі система збору аналітики від мережі Wi-Fi)) або ж як допоміжне рішення для бізнесу (наприклад, трекинг персоналу).

Трекинг персоналу – це вузька потреба ритейла. У ритейлі затребувана консультаційна модель, тобто в магазині консультант повинен обов'язково поспілкуватися з відвідувачем для збільшення ймовірності покупки. Тому дуже важливо, щоб консультанти під час роботи перебували в торговельному залі, а не, скажемо, у підсобних приміщеннях або на складі. При впровадженні трекинг-системи ви побачите, де ходять співробітники, у яких зонах вони перебувають. Із цього вже можна будувати статистику. А ще можна запам'ятовувати маршрути відвідувачів через продуктові візки. На касі ж візок (а разом з нею й всю зібрану інформацію) можна однозначно «прив'язати» до номера клієнта в програмі лояльності, якщо він у ній бере участь. Це дає магазину ще більше шансів догодити своєму постійному клієнтові й заробити більше. У цьому випадку задіється вже більше серйозна математика: байєсовські фільтри, багато лінійної алгебри й машинне навчання.

Архітектура

Архітектура системи Wi-Fi аналітики розроблювальна в даній роботі система збору аналітики від мережі Wi-Fi складається із трьох шарів:

– Інфраструктурний. Він здійснює збір і відправлення даних. На цьому рівні важливо забезпечити контроль устаткування, достатню відказостійкість і моніторинг.

– Зберігання даних. Оскільки мова йде про роботу з більшим обсягом інформації, її потрібно правильно підготувати й коректно зберегти – щоб надалі швидко обробляти її.

– Бізнес-Логіки. Оскільки система має високу природну складність, важливо вміти коректно розраховувати складні аналітичні метрики на основі збережених даних.

Тепер самий час пройти по основних компонентах системи.

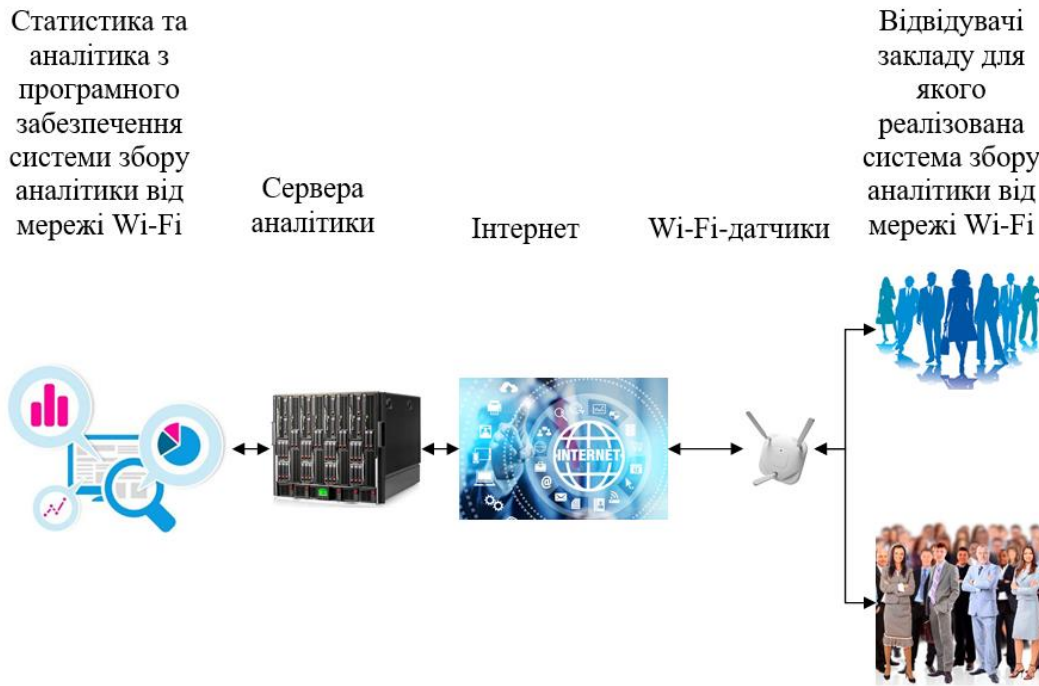


Рисунок 1 – Структурна схема системи

Серверна частина рішення

Серверна частина являє собою сукупність кластерів зберігання даних, сервера із сервісами передобробки, а також окремі інструменти, що забезпечують цільову функціональність кожної частини рішення. При цьому використовуються як віртуальні, так і фізичні сервера в декількох незалежних дата-центрах (chipcore (селектел), firstDEDIC, firstVDS).

Такий розподіл потужностей важливо, тому що необхідно обробляти величезну кількість даних.

Апаратна частина

Всі рішення можливо реалізувати на базі навіть одного пристрою TP-Link.

В 95% проектів розроблювальна в даній роботі система збору аналітики від мережі Wi-Fi у ритейлі, торгових центрах і на об'єктах HoReCa (а це порядку 2500 пристроїв у Києві, Кропивницькому, містах-мільйониках і інших невеликих містах) використовується встаткування TP-Link.

Устаткування TP-Link, що ми використовуємо, має характеристики, що дозволяють працювати у всіх режимах без збоїв і стабільно. Зараз ми працюємо на моделях TP-Link EAP115, EAP110 лінійки Auranet. Тестуються рішення вуличного виконання CPE210 v.1 і EAP 110-Outdoor.

В устаткування TP-Link гарний термін служби – воно стабільно працює протягом тривалого часу.

В основі системи закладений цілий набір цікавих алгоритмів, починаючи від «розумної» калібрування об'єктів і закінчуючи алгоритмами Data-Mining. Навіть банальні, здавалося б, завдання на рівні формування й обробки технічних логів за фактом не такі вже і прості. Багато сил розроблювачів і апаратних ресурсів пристроїв витрачається на боротьбу із шумами й радіоперешкодами. Порядку 60-70% сигналів – це сміття, що не буде брати участь в «корисних» розрахунках. Wi-Fi аналітика й прибуток – синоніми. За допомогою Wi-Fi аналітики можна одержати унікальні аналітичні дані, унікальні інструменти продажів. Більше того, це недорого й застосовно в різних умовах.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів збору та обробки аналітики від мережі Wi-Fi. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем збору та обробки аналітики від мережі Wi-Fi.
- Досліджена система збору та обробки аналітики від мережі Wi-Fi.
- На основі отриманих результатів досліджень створена програмна реалізація системи збору та обробки аналітики від мережі Wi-Fi.

Розроблені алгоритми дозволяють успішно вирішувати завдання збору та обробки аналітики від мережі Wi-Fi. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Kuznetsov O., Frontoni E., Kuznetsova Y., Chevardin V., Smirnov O. «Architectural foundations for adaptive security in edge computing systems». *Cybersecurity Defensive Walls in Edge Computing*, 2025. pp. 21-61.
2. Chulinda L., Smirnov O., Shapenko L., Ustynova I., Bohatiuk I., Kelyp S. «The role of innovation in ensuring the safety of international civil aviation». *Ceur Workshop Proceedings*, 2025, 4024, pp. 530–542.
3. Петрик В.М., Присяжнюк М.М., Аль-Файюмі Халед та ін. «Системи інформаційної зброї та технології інформаційної війни»: підручник / Петрик В.М., Присяжнюк М.М., Аль-Файюмі Халед, Жарков Я.М., Смірнов О.А., Буравченко К.О., Давидюк А.В., Кононович В.Г., Корчинский В.В., Кудирко В.М., Фесенко А.О.; за заг. ред. В.М. Петрика, М.М. Присяжнюка.– К.: Видавничий центр “Кафедра”, 2025.– 320 с.
4. Усік, П.С., Смірнова, Т.В., Буравченко, К.О., Смірнов, О.А., Улічев, О.С., Смірнов, С.А. «Дослідження технологій забезпечення кібербезпеки банківських систем з використанням штучного інтелекту». *Кібербезпека: освіта, наука, техніка*. 2025. Том 1 № 29. С.704–716, 2025
5. Kuznetsov, O., Frontoni, E., Kuznetsova, K., Arnesano, M., Smirnov, O. «A secure biometric authentication architecture for blockchain-driven cyber-physical systems». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 193–224.
6. Kuznetsov, O., Atzeni, G., Arnesano, M., Randieri, C., Smirnov, O. «Secure IoT-based smart wheelchair system: From implementation to security enhancement strategy». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 225–257.
7. Kuznetsov, O., Smirnov, O., Kuznetsova, T., Shaikhanova, A., Svatowsky, I. «Privacy-utility trade-offs in IoT networks: A comparative analysis of differential privacy mechanisms for sensor data aggregation». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 589–622.
8. Lakhno, V., Malyukov, V., Smirnov, O., Bebesko, B., Chubaievskiy, V., Zhumadilova, M., Malyukova, I., Smirnov, S. «Multifactorial Model for Targeted Attacks Counteracting Within the Framework of a Multi-Step Quality Game with Fuzzy Information». *8th International Symposium on Intelligent Informatics, ISI 2023*, 2025. vol 389. pp 377-389. Springer, Singapore.
9. Kuznetsov O., Frontoni E., Kuznetsova Y., Smirnov O., Moskovchenko I. «Trust-Based Security Architecture for Edge Computing: A Simulation Study of Dynamic Trust Evolution and Attack Detection». *CEUR Workshop Proceedings*, 2024, 3909, pp. 227–241.
10. Kuznetsov, O., Frontoni, E., Kryvinska, N., Chevardin, V., Smirnov, O. «Wireless Network Encryption Stream Ciphers, Computational Modeling, and Security Analysis». *Computational Modeling and Simulation of Advanced Wireless Communication Systems*, 2024, pp. 379–402.
11. Kuznetsov, O., Frontoni, E., Kryvinska, N., Smirnov, O., Imoize, G.L. «Computational Modeling of Enhanced Spread Spectrum Codes for Asynchronous Wireless Communication». *Computational Modeling and Simulation of Advanced Wireless Communication Systems*, 2024, pp. 403–447.
12. Ткаченко, О., Ільєнко, А., Улічев, О., Мелешко, Є., Смірнов, О. «Правові засади поширення інформаційних впливів в соціальних мережах». *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2024. № 2(26), С. 170–188.
13. Смірнова Т.В., Коноплицька-Слободенюк О.К., Буравченко К.О., Смірнов С.А., Кравчук О.В., Козірова Н.Л., Смірнов О.А. «Дослідження технологій забезпечення кібербезпеки хмарних сервісів IaaS, PaaS та SaaS». *Кібербезпека: освіта, наука, техніка*. 2024. №4(24), С. 6-27.
14. Вінтенко, Б., Миронець, І., Смірнов, О., Кравчук, О., Козірова, Н., Савеленко, Г., Коваленко, А. «Дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». *Кібербезпека: освіта, наука, техніка*. 2024. №3(23), С. 111-131.
15. Батрак О., Смірнова Т., Гнатюк В., Одарченко Р., Смірнов О. «Дослідження показників ефективності функціонування та перспектив розвитку систем IP-телефонії». *Підводні технології*, 2024, № 13, с. 28-35.
16. Kuznetsov, O., Kryvinska, N., Ilchenko, O., Smirnova, T., Ulianovska, Y. «Comparative Analysis of Cryptocurrency Trading Platforms Using the Analytic Hierarchy Process». *CEUR Workshop Proceedings*, 2023, 3628, pp. 106-115.
17. Akhalaia, G., Iavich, M., Iashvili, G., Prysiaznyy, D., Smirnova, T. «Secure Encrypted Connection on Georgian

- Website». CEUR Workshop Proceedings, 2023, 3550, pp. 313-320.
18. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». Advanced Information Systems, 2023, 7(2), pp. 49-56
 19. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchey, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». CEUR Workshop Proceedings, Volume 3530, 2023, pp. 256-265.
 20. Kuznetsov, O., Kandiy, S., Frontoni, E., Smirnov, O. «Trade-offs in Post-Quantum Cryptography: A Comparative Assessment of BIKE, HQC, and Classic McEliece». CEUR Workshop Proceedings, Volume 3504, 2023, pp. 1-11.
 21. Smirnov, O., Lakhno, V., Akhmetov, B., Chubaievskiy, V., Khorolska, K., Bebesko, B. «Selection of a Rational Composition of Information Protection Means Using a Genetic Algorithm». In: Rajakumar, G., Du, K.L., Vuppapapati, C., Beligiannis, G.N. (eds) Intelligent Communication Technologies and Virtual Mobile Networks. Lecture Notes on Data Engineering and Communications Technologies, vol 131. 2023. Springer, Singapore. pp. 21-34.
 22. Смірнова Т.В., Гнатюк С.О., Бердибаєв Р.Ш., Сидоренко В.М., Жигаревич О.К., «Система корелювання подій та управління інцидентами кібербезпеки на об'єктах критичної інфраструктури». Кібербезпека: освіта, наука, техніка, №3(19), 2023, С. 176-196.
 23. Смірнов О.А. Козлов Я.О., Смірнова Т.В. «Дослідження застосування SIEM-систем для забезпечення кібербезпеки та захисту інформації». II Міжнародна науково-практична Інтернет-конференція «Інновації та перспективні шляхи розвитку інформаційних технологій (ІПШРІТ-2023)» м.Черкаси 6 грудня 2023 року – Черкаси: ЧДТУ.– 2023. – С.251-252.
 24. Козлов Я.О., Смірнова Т.В., Смірнов О.А. «Дослідження SIEM-систем для забезпечення кібербезпеки». VII міжнародна науково-практична конференція “Інформаційна безпека та комп’ютерні технології” до 30-ти річчя кафедри кібербезпеки та програмного забезпечення, м. Кропивницький. 1 листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 26.
 25. Козлов Я.О., Козірова Н.Л., Смірнов О.А. «Дослідження структури та принципу роботи SIEM-системи». VII міжнародна науково-практична конференція “Інформаційна безпека та комп’ютерні технології” до 30-ти річчя кафедри кібербезпеки та програмного забезпечення, м. Кропивницький. 1 листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 59.
 26. Вінтенко Б.Ю., Смірнов О.А., Коваленко О.В., Смірнов С.А., Коваленко А.С. «Дослідження нормативних документів та галузевих стандартів розробки програмного забезпечення комп’ютерних систем управління АЕС, важливих для безпеки». Системи управління, навігації та зв’язку, 2023, вип. 2(72), С. 170-178.
 27. Smirnov, O., Neskrodieva, T., Fedorov, E., Rudakov, K., Neskrodieva, A. «Method Detection Audit Data Anomalies on Basis Restricted Cauchy Machine» CEUR Workshop Proceedings, Volume 3187, 2022,
 28. Smirnov O.A., Al-Oraiqat A.M., Ulichev O.S., Meleshko Ye.V., Al-Rawashdeh H.S., Polishchuk L.I. «Modeling strategies for information influence dissemination in social networks». Journal of Ambient Intelligence and Humanized Computing Volume 13, Issue 5. Springer, Cham. 2022, pp. 2463-2477.
 29. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». Проблеми інформатизації та управління, № 2(70). 2022. С. 28-37.
 30. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 3(69). С. 93-98.
 31. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Вісник Хмельницького національного університету. Серія: «Технічні науки», № 2 (307). С. 46-52. 2022.

УДК 004

О.Сосна, магістр гр. КІ-24М,

Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ КОНТРОЛЮ ІНТЕРНЕТ ШЛЮЗІВ НА БАЗІ ОС UBUNTU

У статті розроблено програмне забезпечення, яке призначено для системи контролю Інтернет шлюзів на базі ОС Ubuntu. Метою розробки є дослідження та принципи побудови системи контролю Інтернет шлюзів на базі ОС Ubuntu. Об'єктом дослідження є процес контролю Інтернет шлюзів на базі ОС Ubuntu. Предметом дослідження є методи контролю Інтернет шлюзів на базі ОС Ubuntu. Методи дослідження базуються на методах захисту інформації у комп'ютерних мережах, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи контролю Інтернет шлюзів на базі ОС Ubuntu. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

контроль Інтернет шлюзів, ОС Ubuntu

Постановка проблеми. У світі мереж шлюз за замовчуванням відіграє ключову роль у спрямуванні мережевого трафіку між вашою локальною мережею та ширшим Інтернетом. Ubuntu 20, як популярний дистрибутив Linux, дозволяє користувачам ефективно налаштовувати та керувати своїми мережевими параметрами. Дана робота проведе вас через процес зміни шлюзу за замовчуванням в Ubuntu 20, забезпечуючи вам повний контроль над вашим мережевим трафіком.

Перш ніж заглибитися в процес, важливо зрозуміти, що таке шлюз за замовчуванням. Шлюз за замовчуванням – це IP-адреса маршрутизатора, який з'єднує вашу локальну мережу з ширшим Інтернетом. Коли пристрою у вашій локальній мережі потрібно зв'язатися з пристроєм в іншій мережі, він надсилає дані до шлюзу за замовчуванням, який потім пересилає їх до потрібного пункту призначення.

Перш ніж почати, переконайтеся, що у вас є такі передумови:

- Система Ubuntu 20 працює.
- Адміністративний доступ до системи.
- IP-адреса нового шлюзу за замовчуванням.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи контролю інтернет шлюзів на базі ОС Ubuntu.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи контролю Інтернет шлюзів на базі ОС Ubuntu.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем контролю Інтернет шлюзів на базі ОС Ubuntu.
- Дослідження системи контролю Інтернет шлюзів на базі ОС Ubuntu.
- Програмна реалізація системи контролю Інтернет шлюзів на базі ОС Ubuntu.

Об'єктом дослідження є процес контролю Інтернет шлюзів на базі ОС Ubuntu.

Предметом дослідження є методи контролю Інтернет шлюзів на базі ОС Ubuntu.

Методи дослідження базуються на методах захисту інформації у комп'ютерних мережах, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Зі зростанням Інтернету речей (IoT) потреба в надійних, гнучких та ефективних шлюзах стає дедалі важливішою. Шлюз IoT діє як міст між пристроями IoT та хмарою, забезпечуючи безперебійну передачу даних та інтелектуальну обробку. Однією з найкращих платформ для розробки та розгортання шлюзів IoT є Ubuntu, універсальна та широко використовувана операційна система з відкритим кодом. У цій статті розглядаються переваги використання Ubuntu для шлюзів IoT та те, як він може революціонізувати ваші рішення IoT.

Що таке шлюз Інтернету речей?

Шлюз Інтернету речей (IoT) – це пристрій або програмна платформа, яка забезпечує зв'язок між пристроями Інтернету речей та хмарними сервісами. Він збирає, обробляє та передає дані, підтримуючи різні протоколи та керуючи підключеннями пристроїв. Ефективний шлюз Інтернету речей забезпечує низьку затримку, підвищує безпеку та спрощує локальну обробку даних.

Чому варто обрати Ubuntu для шлюзів Інтернету речей?

1. Переваги відкритого коду

Будучи програмою з відкритим вихідним кодом, Ubuntu дозволяє розробникам налаштовувати та модифікувати ОС відповідно до потреб конкретного проекту. Ця гнучкість є критично важливою в IoT-додатках, де задіяні різноманітні пристрої та протоколи.

2. Багата екосистема

Ubuntu підтримує широкий спектр бібліотек, фреймворків та інструментів, спеціально розроблених для розробки Інтернету речей. Від Python та Node.js до бібліотек машинного навчання, розробники мають доступ до безлічі ресурсів.

3. Зручний інтерфейс

Ubuntu пропонує зручний інтерфейс, що спрощує розробникам налаштування та керування шлюзами, незалежно від того, чи використовують вони Ubuntu Server, чи Ubuntu Core, розроблені спеціально для IoT-застосунків.

4. Надійна підтримка громади

Маючи сильну спільноту розробників та користувачів, Ubuntu надає розширені ресурси, підтримку з усунення несправностей та документацію, що може бути безцінним під час подолання труднощів.

5. Функції безпеки

Ubuntu включає різні заходи безпеки, включаючи регулярні оновлення, вбудовані брандмауери та дозволи користувачів, які життєво важливі для захисту даних і пристроїв у середовищі Інтернету речей.

Налаштування шлюзу Інтернету речей за допомогою Ubuntu

Щоб проілюструвати, як налаштувати шлюз Інтернету речей за допомогою Ubuntu, давайте розглянемо кілька важливих кроків:

1. Виберіть свою версію Ubuntu

Залежно від ваших потреб, виберіть між Ubuntu Server та Ubuntu Core. Ubuntu Core особливо підходить для пристроїв Інтернету речей завдяки своїй легкості та системі керування пакетами (snap).

2. Встановлення

Завантажте вибрану версію Ubuntu та дотримуйтесь інструкцій з встановлення. Переконайтеся, що у вас є необхідне обладнання, яке відповідає специфікаціям ваших пристроїв Інтернету речей.

3. Налаштуйте параметри мережі

Налаштуйте мережеве з'єднання, щоб ваш шлюз міг взаємодіяти з пристроями Інтернету речей та Інтернетом. Це може включати налаштування параметрів Wi-Fi або Ethernet.

4. Встановлення IoT-фреймворків

Залежно від вимог вашого проекту, ви можете встановити різні IoT-фреймворки, такі як:

Node-RED: Інструмент програмування на основі потоків для з'єднання пристроїв Інтернету речей.

MQTT: Легкий протокол обміну повідомленнями для невеликих датчиків та мобільних пристроїв, оптимізований для мереж з високою затримкою або ненадійних мереж.

Платформа Інтернету речей: Для візуалізації даних, зібраних з пристроїв Інтернету речей.

Розробка та розгортання додатків: Створюйте додатки, які використовують можливості обробки даних, аналітики та локального прийняття рішень. Python або JavaScript є популярним вибором для розробки цих додатків.

5. Захистіть свій шлюз

Впроваджуйте протоколи безпеки, такі як шифрування даних під час передачі та використання безпечних методів автентифікації, для захисту вашої екосистеми Інтернету речей.

Висновок

Використання Ubuntu для шлюзів Інтернету речей пропонує надійну, гнучку та безпечну платформу, яка може ефективно впоратися зі складнощами комунікації Інтернету речей. Завдяки відкритому коду, багатій екосистемі та сильній підтримці спільноти, Ubuntu є чудовим вибором для розробників, які прагнуть створювати інтелектуальні рішення Інтернету речей. Оскільки ландшафт Інтернету речей продовжує розвиватися, використання можливостей Ubuntu, безсумнівно, покращить підключення, ефективність та інновації в численних додатках.

Впроваджуючи та розгортаючи шлюзи Інтернету речей за допомогою Ubuntu, компанії та розробники можуть відкрити нові можливості та стимулювати майбутнє інтелектуальних технологій.

Системи контролю Інтернет шлюзів на базі ОС Ubuntu – це за фактом міжмережевий екран (брандмауер), який працює під керуванням відповідної ОС. Брандмауери – це не щось привабливе. Вони рідко потрапляють у заголовки газет, а коли працюють добре, ви їх майже не помічаєте. Однак у 2025 році, коли ваш бізнес залежить від хмарних додатків, віддалених користувачів та постійно активних сервісів, скромний брандмауер все ще має велику вагу. Уявіть собі свою мережу як будівлю. У вас є двері, коридори, ліфти та постійний потік відвідувачів. Брандмауер – це стійка реєстрації та служба безпеки. Він впускає потрібних людей, не пускає не потрібних і виявляє дивну поведінку, перш ніж вона стане проблемою.

Що таке брандмауер?

По суті, брандмауер перевіряє трафік, який намагається увійти або вийти з вашого середовища, і застосовує встановлені вами правила. Ці правила можуть бути простими, наприклад, «дозволити цьому офісу доступ до цієї служби», або дуже специфічними, наприклад, «дозволити цьому користувачеві доступ до цієї програми лише в робочий час». Сучасні брандмауери йдуть далі. Вони розуміють програми та користувачів, а не лише IP-адреси та порти. Вони можуть переглядати трафік, щоб виявляти відомі загрози, підозрілі закономірності або ризикований контент. Вони ведуть детальні журнали, щоб ви могли довести, хто до чого мав доступ і коли.

Шифрування є ключовою частиною цієї історії. Більшість бізнес-трафіку зараз передається через TLS. Це чудово для конфіденційності, але також може приховувати атаки. За умови правильного проектування та політик брандмауер може розшифрувати трафік на периферії, застосовувати перевірки безпеки, а потім повторно зашифрувати його для подальшого передавання. Якщо все зроблено добре, користувач не помічає різниці, але ви усуваєте основну сліпу зону. Результатом є точка контролю, яка поєднує видимість із можливістю діяти в режимі реального часу.

Реальні виклики 2025 року

Зловмисники швидкі, терплячі та організовані. Один фішинг може дати їм плацдарм. Звідти вони намагаються переміщатися по вашій мережі, знаходити цінні дані та непомітно викрадати їх, перш ніж з'явиться будь-яке повідомлення з вимогою викупу. Водночас ваші

активи зростають. Співробітники підключаються до мережі як з дому, так і в дорозі. Партнери та постачальники інтегруються з вашими системами. Ви використовуєте поєднання хмарних та локальних сервісів. Кожне підключення – це ще один шлях, який може спробувати зловмисник.

Операції також перебувають під тиском. Команди зайняті, інструментів безпеки багато, а зміни накопичуються. Зі зміщенням акценту на безпеку до сучасніших рішень, таких як XDR, SSE, CNAPP та CTEM, брандмауери часто страждають від проблеми «встановив і забув». Правила швидко додаються для вирішення бізнес-проблеми, а потім ніколи не очищаються. З часом ви отримуєте захаращені політики, тіньові правила та широкі «тимчасові» дозволи. Це послаблює безпеку та може уповільнити продуктивність. Якщо сам брандмауер вийде з ладу, наслідки можуть бути негайними. Персонал не може отримати доступ до потрібних програм. Клієнти не можуть зв'язатися з вами. Для багатьох організацій збій брандмауера є збоєм у роботі бізнесу.

Відповідність додає ще один рівень. Вам може знадобитися продемонструвати відповідність вимогам CIS Controls, ISO 27001, PCI DSS або контрактним вимогам. Аудитори очікують побачити чіткі граничні засоби контролю, історію змін та докази того, що зашифрований трафік не є неконтрольованою прогалиною. Ніщо з цього не є складним окремо, але вимагає регулярної уваги та турботи.

Основна функція брандмауера

Основна функція брандмауера – охороняти вашу безпечну внутрішню мережу та публічний Інтернет. Ця роль є вирішальною для пояснення функції брандмауера в захисті системи та інформаційних активів, оскільки вона гарантує, що проходить лише авторизований трафік. Брандмауери захищають цінні цифрові активи, зосереджуючись на трьох основах інформаційної безпеки:

- Конфіденційність: Запобігання несанкціонованому доступу для збереження конфіденційності даних.
- Цілісність: Блокування шкідливого програмного забезпечення, яке може змінити або пошкодити дані.
- Доступність: Захист від атак, таких як відмова в обслуговуванні (DoS), метою яких є зробити системи недоступними.

Невпинно моніторячи мережевий трафік, брандмауери запобігають проникненню хакерів, вірусів і черв'яків у вашу мережу або викраданню конфіденційних даних.

Основні переваги впровадження брандмауера

Впровадження надійного брандмауера надає численні переваги, які пояснюють функцію брандмауера в захисті системи та інформаційних активів:

- Захист від загроз: Брандмауери діють як щит, запобігаючи несанкціонованому доступу, шкідливим програмам та кібератакам, що потрапляють у вашу приватну мережу.
- Фільтрація трафіку: Вони ретельно перевіряють усі пакети даних, регулюючи вхідний та вихідний трафік, щоб забезпечити потік лише легітимних даних, захищаючи від вірусів та спроб фішингу.
- Контроль доступу: Забезпечуючи дотримання правил безпеки, брандмауери визначають, хто може отримувати доступ до мережевих ресурсів, запобігаючи несанкціонованому доступу.
- Безпечний віддалений доступ: Брандмауери мають вирішальне значення для захисту підключень до віртуальної приватної мережі (VPN), що дозволяє віддаленим співробітникам безпечно отримувати доступ до корпоративних мереж.
- Сегментація мережі: Вони можуть розділити мережу на ізольовані сегменти, тому, якщо одна частина порушена, пошкодження локалізується і не може поширюватися.
- Відповідність нормативним вимогам: Багато нормативних актів (таких як HIPAA або PCI-DSS) вимагають використання брандмауерів для захисту конфіденційних даних, допомагаючи підприємствам уникати штрафів та шкоди репутації.

Як працюють брандмауери: огляд основних механізмів інспекції

Щоб пояснити функцію брандмауера в захисті системи та інформаційних активів, ми повинні зрозуміти, як вони перевіряють дані. Брандмауери – це інтелектуальні контролери трафіку, які постійно, за частки секунди, приймають рішення про те, що дозволяти або блокувати, на основі детального набору правил безпеки.

Ця фільтрація на основі правил діє як контрольний список для відхилення, визначаючи, що потрапляє, а що відхиляється. Для кожного пакета даних брандмауер приймає рішення про дозвіл або блокування, контролюючи як вхідний, так і вихідний трафік. Це запобігає проникненню загроз і запобігає виходу конфіденційних даних без дозволу.

Крім того, брандмауери надають можливості ведення журналу та аудиту, зберігаючи детальний облік мережевого трафіку. Ці журнали безцінні для розслідування підозрілої активності, підтвердження відповідності нормативним вимогам та вдосконалення політик безпеки.

Основні механізми: фільтрація пакетів, перевірка стану та проксі-сервери

Сучасні брандмауери використовують три основні методи перевірки, кожен з яких пропонує різний рівень захисту. Розуміння цих методів допомагає пояснити функцію брандмауера у захисті системи та інформаційних активів.

Фільтрація пакетів – це найбазовіша технологія брандмауера. Вона швидка та ефективна, перевіряючи заголовки пакетів на наявність такої інформації, як IP-адреси, номери портів та протоколи. Це як швидка перевірка ідентифікатора біля дверей, але їй бракує усвідомлення ширшого контексту з'єднання.

Перевірка стану є більш інтелектуальною. Вона використовує відстеження стану з'єднання, щоб запам'ятовувати активні, легітимні з'єднання. Розуміючи контекст потоку трафіку, вона знає, коли дозволити відповідь на запит, зроблений вашою мережею, що робить її набагато ефективнішою у блокуванні спроб несанкціонованого доступу.

Проксі-сервіси пропонують найретельнішу перевірку, працюючи на рівні додатків. Вони діють як посередники, отримуючи та повторно передаючи дані від імені вашої мережі. Ця перевірка на рівні додатків дозволяє їм перевіряти фактичний вміст комунікацій, забезпечуючи найвищий рівень безпеки для критично важливих додатків.

Запобігання шкідливому програмному забезпеченню та іншим кіберзагрозам

Коли ми пояснюємо функцію брандмауера для захисту системи та інформаційних активів, це зводиться до запобігання загрозам. Брандмауери працюють цілодобово, щоб зупинити різні кіберзагрози, перш ніж вони завдадуть шкоди.

– Блокування шкідливого коду: Брандмауери розпізнають підозрілі моделі трафіку, пов'язані з вірусами та черв'яками, зупиняючи їх на периметрі мережі до того, як може статися зараження.

– Запобігання DoS-атак: Коли зловмисники перевантажують мережу трафіком, брандмауери можуть виявляти ці незвичайні закономірності та блокувати джерело шкідливого програмного забезпечення, дозволяючи при цьому продовжувати легітимний бізнес-трафік.

– Зменшення спроб фішингу: Хоча брандмауери не є повним рішенням для боротьби з фішингом, вони можуть блокувати доступ до відомих шкідливих веб-сайтів, посилання на які містяться у фішингових електронних листах, забезпечуючи важливу систему безпеки.

– Зупинка несанкціонованого витоку даних: моніторячи вихідний трафік, брандмауери можуть виявляти та блокувати спроби шкідливого програмного забезпечення або інсайдерів надсилати конфіденційну інформацію з вашої мережі.

На рисунку 1 зображена структурна схема системи. На який розглянута розроблена система в цілому.



Рисунок 1 – Структурна схема системи

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів контролю Інтернет шлюзів на базі ОС Ubuntu. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем контролю Інтернет шлюзів на базі ОС Ubuntu.
- Досліджена система контролю Інтернет шлюзів на базі ОС Ubuntu.
- На основі отриманих результатів досліджень створена програмна реалізація системи контролю Інтернет шлюзів на базі ОС Ubuntu.

Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання контролю Інтернет шлюзів на базі ОС Ubuntu. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Kuznetsov, O., Smirnov, O., Kuznetsova, T., Shaikhanova, A., Svatowsky, I. «Privacy-utility trade-offs in IoT networks: A comparative analysis of differential privacy mechanisms for sensor data aggregation». Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications, 2025, pp. 589–622.
2. Lakhno, V., Malyukov, V., Smirnov, O., Bebesko, B., Chubaievskiy, V., Zhumadilova, M., Malyukova, I., Smirnov, S. «Multifactorial Model for Targeted Attacks Counteracting Within the Framework of a Multi-Step Quality Game with Fuzzy Information». 8th International Symposium on Intelligent Informatics, ISI 2023, 2025. vol 389. pp 377-389. Springer, Singapore.
3. Kuznetsov O., Frontoni E., Kuznetsova Y., Smirnov O., Moskovchenko I. «Trust-Based Security Architecture for Edge Computing: A Simulation Study of Dynamic Trust Evolution and Attack Detection». CEUR Workshop Proceedings, 2024, 3909, pp. 227–241.
4. Kuznetsov, O., Frontoni, E., Kryvinska, N., Chevardin, V., Smirnov, O. «Wireless Network Encryption Stream

- Ciphers, Computational Modeling, and Security Analysis». *Computational Modeling and Simulation of Advanced Wireless Communication Systems*, 2024, pp. 379–402.
5. Kuznetsov, O., Frontoni, E., Kryvinska, N., Smirnov, O., Imoize, G.L. «Computational Modeling of Enhanced Spread Spectrum Codes for Asynchronous Wireless Communication». *Computational Modeling and Simulation of Advanced Wireless Communication Systems*, 2024, pp. 403–447.
 6. Ткаченко, О., Ільченко, А., Улічев, О., Мелешко, Є., Смірнов, О. «Правові засади поширення інформаційних впливів в соціальних мережах». Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2024. № 2(26), С. 170–188.
 7. Смірнова Т.В., Коноплицька-Слободенюк О.К., Буравченко К.О., Смірнов С.А., Кравчук О.В., Козірова Н.Л., Смірнов О.А. «Дослідження технологій забезпечення кібербезпеки хмарних сервісів IaaS, PaaS та SaaS». *Кібербезпека: освіта, наука, техніка*. 2024. №4(24), С. 6-27.
 8. Вінтенко, Б., Миронець, І., Смірнов, О., Кравчук, О., Козірова, Н., Савеленко, Г., Коваленко, А. «Дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». *Кібербезпека: освіта, наука, техніка*. 2024. №3(23), С. 111-131.
 9. Батрак О., Смірнова Т., Гнатюк В., Одарченко Р., Смірнов О. «Дослідження показників ефективності функціонування та перспектив розвитку систем IP-телефонії». *Підводні технології*, 2024, № 13, с. 28-35.
 10. Kuznetsov, O., Kryvinska, N., Ilchenko, O., Smirnova, T., Ulianovska, Y. «Comparative Analysis of Cryptocurrency Trading Platforms Using the Analytic Hierarchy Process». *CEUR Workshop Proceedings*, 2023, 3628, pp. 106-115.
 11. Akhalaia, G., Iavich, M., Iashvili, G., Prysiazhnyy, D., Smirnova, T. «Secure Encrypted Connection on Georgian Website». *CEUR Workshop Proceedings*, 2023, 3550, pp. 313-320.
 12. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». *Advanced Information Systems*, 2023, 7(2), pp. 49-56
 13. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchey, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». *CEUR Workshop Proceedings*, Volume 3530, 2023, pp. 256-265.
 14. Kuznetsov, O., Kandy, S., Frontoni, E., Smirnov, O. «Trade-offs in Post-Quantum Cryptography: A Comparative Assessment of BIKE, HQC, and Classic McEliece». *CEUR Workshop Proceedings*, Volume 3504, 2023, pp. 1-11.
 15. Smirnov, O., Lakhno, V., Akhmetov, B., Chubaievskyi, V., Khorolska, K., Bebesko, B. «Selection of a Rational Composition of Information Protection Means Using a Genetic Algorithm». In: Rajakumar, G., Du, K.L., Vuppapapati, C., Beligiannis, G.N. (eds) *Intelligent Communication Technologies and Virtual Mobile Networks. Lecture Notes on Data Engineering and Communications Technologies*, vol 131. 2023. Springer, Singapore. pp. 21-34.
 16. Смірнова Т.В., Гнатюк С.О., Бердибасєв Р.Ш., Сидоренко В.М., Жигаревич О.К., «Система корелювання подій та управління інцидентами кібербезпеки на об'єктах критичної інфраструктури». *Кібербезпека: освіта, наука, техніка*, №3(19), 2023, С. 176-196.
 17. Смірнов О.А. Козлов Я.О., Смірнова Т.В. «Дослідження застосування SIEM-систем для забезпечення кібербезпеки та захисту інформації». II Міжнародна науково-практична Інтернет-конференція «Інновації та перспективні шляхи розвитку інформаційних технологій (ІПШРІТ-2023)» м.Черкаси 6 грудня 2023 року – Черкаси: ЧДТУ. – 2023. – С.251-252.
 18. Козлов Я.О., Смірнова Т.В., Смірнов О.А. «Дослідження SIEM-систем для забезпечення кібербезпеки». VII міжнародна науково-практична конференція «Інформаційна безпека та комп'ютерні технології» до 30-ти річчя кафедри кібербезпеки та програмного забезпечення, м.Кропивницький. 1 листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 26.
 19. Козлов Я.О., Козірова Н.Л., Смірнов О.А. «Дослідження структури та принципу роботи SIEM-системи». VII міжнародна науково-практична конференція «Інформаційна безпека та комп'ютерні технології» до 30-ти річчя кафедри кібербезпеки та програмного забезпечення, м.Кропивницький. 1 листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 59.
 20. Вінтенко Б.Ю., Смірнов О.А., Коваленко О.В., Смірнов С.А., Коваленко А.С. «Дослідження нормативних документів та галузевих стандартів розробки програмного забезпечення комп'ютерних систем управління АЕС, важливих для безпеки». *Системи управління, навігації та зв'язку*, 2023, вип. 2(72), С. 170-178.
 21. Smirnov, O., Neskordieva, T., Fedorov, E., Rudakov, K., Neskordieva, A. «Method Detection Audit Data Anomalies on Basis Restricted Cauchy Machine» *CEUR Workshop Proceedings*, Volume 3187, 2022,
 22. Smirnov O.A., Al-Oraiqat A.M., Ulichev O.S., Meleshko Ye.V., Al-Rawashdeh H.S., Polishchuk L.I. «Modeling strategies for information influence dissemination in social networks». *Journal of Ambient Intelligence and Humanized Computing* Volume 13, Issue 5. Springer, Cham. 2022, pp. 2463-2477.
 23. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». *Проблеми інформатизації та управління*, № 2(70). 2022. С. 28-37.
 24. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» *Системи управління, навігації та зв'язку*, 2023, вип. 2(72), С. 170-178.

зв'язку, 2022, № 3(69). С. 93-98.

25. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Вісник Хмельницького національного університету. Серія: «Технічні науки», № 2 (307). С. 46-52. 2022.
26. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 1(67). С. 84-89.
27. Smirnov O., Kuznetsov A., Zhora V., Onikiychuk A., Pieshkova O. «Hiding Messages in Audio Files Using Direct Spread Spectrum». 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2021, Cracow, Poland, 22-25 September 2021. P. 414-418
28. Smirnov O., Kuznetsov A., Lokotkova I., Kuznetsova T., Florov S., Lebid O. «Using Orthogonal Signals to Hide Information in Images». 4 IEEE International Conference on Advanced Information and Communication Technologies (AICT) - 2021, Lviv, Ukraine, September 21-25, 2021. P. 255-260.
29. Smirnov O., Kuznetsov A., Girzheva O., Kiian A., Nakisko O., Kuznetsova T. «Advanced Code-Based Electronic Digital Signature Scheme». 2020 IEEE International Conference on Problems of Infocommunications Science and Technology, PIC S and T 2020, Kharkiv, 6 October 2020-9 October 2020, P. 358-362.
30. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova K. «Data hiding scheme based on spread sequence addressing». CEUR Workshop Proceedings Volume 2805, 2020, Pages 44-58.
31. Smirnov, O., Kuznetsov, A., Potii, O., Poluyanenko, N., Stelnyk, I., Mialkovsky, D. «Combining and filtering functions in the framework of nonlinear-feedback shift register». International Journal of Computing; 2020, Volume 19, Issue 2 – Research Institute for Intelligent Computer Systems – 2020. – P. 247-256.
32. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.

УДК 004

С.Талмазан, магістр гр. КІ-24М,

Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ПРОТИДІЇ МЕРЕЖЕВИМ DDoS-АТАКАМ

У статті розроблено програмне забезпечення, яке призначено для системи протидії мережевим DDoS-атакам. Метою розробки є дослідження та принципи побудови системи протидії мережевим DDoS-атакам. Об'єктом дослідження є процес протидії мережевим DDoS-атакам. Предметом дослідження є методи протидії мережевим DDoS-атакам. Методи дослідження базуються на методах захисту інформації у комп'ютерних мережах, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи протидії мережевим DDoS-атакам. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

DDoS-атака

Постановка проблеми. Забезпечення захищеності мережі від DDoS-атак вимагає добре структурованої захисної стратегії. Мережа часто містить численні ресурси – веб-сайти, програми та сервіси – не лише для своїх власників, але й для їхніх клієнтів.

Масштабна DDoS-атака, спрямована лише на один із цих ресурсів, може створити величезне навантаження на мережеву інфраструктуру. Різке збільшення незаконного трафіку може перевантажити навіть найпотужніші маршрутизатори, що призведе до перебоїв у роботі та потенційних збоїв.

І це не просто теорія – DDoS-атаки, що досягають сотень гігабіт на секунду, зараз є поширеним явищем. Нещодавно ми навіть зафіксували атаку потужністю 1,5 Тбіт/с.

Зрозуміло, що само по собі обладнання та програмне забезпечення на периферії ледве справляються з такими масованими атаками, що робить хмарні рішення для боротьби з DDoS-атаками необхідністю.

Проблему посилює те, що мережеві оператори зазвичай керують великими пулами IP-адрес, які зловмисники використовують, одночасно запускаючи численні менші DDoS-атаки. Ці атаки низької інтенсивності можуть залишитися непоміченими традиційними засобами захисту, але їхній сукупний вплив на периферійні пристрої може бути серйозним, що призводить до зниження продуктивності, операційної нестабільності або навіть повного виходу з ладу вузла.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи протидії мережевим DDoS-АТАКАМ.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи протидії мережевим DDoS-атакам.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем протидії мережевим DDoS-атакам.
 - Дослідження системи протидії мережевим DDoS-атакам.
 - Програмна реалізація системи протидії мережевим DDoS-атакам.
- Об'єктом дослідження є процес протидії мережевим DDoS-атакам.
Предметом дослідження є методи протидії мережевим DDoS-атакам.

Методи дослідження базуються на методах захисту інформації у комп'ютерних мережах, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Закрийте невикористовувані порти та приховайте невикористовувані IP-адреси

Ваша мережа повинна виглядати якомога більше схожою на «чорну скриньку» з точки зору зловмисника. Хакери часто шукають вразливості, слабкі місця та незахищені ресурси – іноді навіть ті, які ви могли пропустити під час аудиту – щоб розпочати DDoS-атаки.

Щоб мінімізувати цей ризик, створіть детальний список активних та неактивних мережеслужб і ресурсів. Потім закрийте все, що не використовується, щоб запобігти їхньому використанню зловмисниками.

Ви також захочете ускладнити зловмисникам аналіз вашої мережі. Одна з ефективних стратегій – приховати IP-адреси вашого пірингу від Traceroute, як зовні, так і зсередини. Майте на увазі, що загрози можуть виходити не лише від зовнішніх зловмисників, а й від інсайдерів – це включає ваш власний персонал або співробітників компаній-клієнтів, які розміщують свої ресурси у вашій мережі.

Для адрес, які неможливо приховати, захистіть їх за допомогою списків контролю доступу (ACL). Зверніться до свого постачальника послуг захисту від DDoS, щоб налаштувати це.

Забезпечення належної продуктивності периферійних пристроїв

Одна з найпоширеніших причин, чому мережі страждають від DDoS-атак, – це недостатньо потужні периферійні пристрої – маршрутизатори, брандмауери, балансувальники навантаження та інші компоненти інфраструктури. Ці пристрої можуть добре обробляти звичайний трафік, але навіть відносно невелика DDoS-атака може вивести їх з ладу.

Ми часто стикаємося з брандмауерами Cisco ASA (особливо старішими моделями) та маршрутизаторами MikroTik, які виходять з ладу під час атак. Багато мереж також покладаються на апаратне забезпечення для невеликих офісів або застаріле обладнання, яке колись було ефективним, але тепер нездатним впоратися із сучасними DDoS-загрозами.

Навіть найкращі рішення проти DDoS-атак не можуть відфільтрувати 100% атаки. Якщо лише 1% масштабної атаки (наприклад, 50 Гбіт/с) обійде фільтрацію, це може перевантажити периферійні пристрої в десятки або навіть сотні разів.

З увімкненою перевіркою стану пакетів (SPI) продуктивність падає ще швидше. У важких випадках пристрої перевантажуються настільки, що не можуть обробляти легітимний трафік або навіть повідомляти про свій стан, що робить усунення несправностей неможливим.

– Визначте слабкі пристрої за допомогою мережевого аудиту та замініть їх на більш продуктивні альтернативи. Без цього навіть найкращий захист від DDoS-атак не запобіжить збоєм.

– Розширте пропускну здатність – сильна атака може перевантажити не лише пристрої, але й ваші інтернет-канали. Масштабування існуючої пропускну здатності та додавання резервних каналів допоможе підтримувати стабільність.

Модернізуючи периферійну інфраструктуру та забезпечуючи достатню пропускну здатність, ви можете значно покращити стійкість вашої мережі до DDoS-атак та підтримувати її працездатність навіть під час серйозних атак.

Проведіть стрес-тест

Ви можете оцінити стійкість вашої мережі до DDoS-атак, провівши стрес-тести за допомогою загальнодоступних інструментів, таких як hping3, який входить до складу багатьох дистрибутивів Linux. Ця утиліта дозволяє імітувати різні типи атак з регульованими параметрами. Однак важливо використовувати її обережно, поступово збільшуючи навантаження, щоб уникнути ненавмисних збоїв.

Стрес-тестування також слід регулярно проводити після впровадження захисту від DDoS-атак. Це допомагає оцінити, що відбувається, коли навіть невелика кількість

атакуючого трафіку досягає вашої мережі. Крім того, це дозволяє оцінити швидкість реагування вашого постачальника анти-DDoS-захисту – наскільки швидко вони реагують на атаку, чи надають вони підтримку поза робочим часом і наскільки ефективно вони усувають загрозу.

Читайте також: Чому стрес-тести та інші перевірки захисту від DDoS-атак такі важливі.

Захистіть свої DNS-сервери

У першій половині 2025 року DNS-атаки стали другим за поширеністю типом DDoS-атак, одразу після HTTP-флуду. Це робить захист DNS головним пріоритетом – без нього цілеспрямована атака може спричинити нестабільність, що призведе до проблем з доступністю ресурсів для користувачів.

Якщо ваш DNS-сервер розміщено у вашій мережі, ви можете захистити його за допомогою оголошень BGP, але лише якщо ваш постачальник послуг захисту від DDoS-атак підтримує фільтрацію DNS-атак (не всі вони підтримують!). Якщо ваш постачальник пропонує цю функцію, поділіться з ним адресами своїх DNS-серверів і запросіть налаштовану фільтрацію трафіку для забезпечення стабільної роботи.

Інтегруйте захист від DDoS-атак у свою загальну стратегію безпеки

Захист від DDoS-атак має бути безперешкодно інтегрований у стратегію інформаційної безпеки (ІБ) вашої організації та загальні плани управління кіберризиками. Це не окремий захід – він має працювати синхронно з іншими процесами безпеки, щоб забезпечити комплексний захист від загроз, що постійно змінюються.

Для досягнення цієї мети захист від DDoS-атак має бути тісно узгоджений з:

- Управління вразливостями – виявлення та виправлення слабких місць, перш ніж зловмисники їх скористаються.

- Управління конфігурацією – забезпечення оптимізації налаштувань безпеки для протистояння атакам.

- Реагування на інциденти – наявність чіткого плану виявлення та зменшення DDoS-загроз у режимі реального часу.

- Моніторинг та аудит – безперервна оцінка мережевої активності для виявлення ранніх ознак атаки.

З розвитком DDoS-загроз ваша мережа також повинна адаптуватися:

- Регулярно проводити аудити безпеки та оцінки вразливостей.

- Проаналізуйте минулі атаки, щоб зрозуміти закономірності та запобігти майбутнім загрозам.

- Проведіть стрес-тести, щоб оцінити стійкість вашої мережі під навантаженням.

- Зверніться до свого постачальника анти-DDoS-захисту, щоб проактивно усунути вразливості та покращити конфігурації безпеки.

Постійно вдосконалюючи та узгоджуючи свою стратегію захисту від DDoS-атак із ширшими процесами ІБ, ви забезпечите довгострокову стійкість до постійно зростаючої загрози кібератак.

Як запобігти DDoS-атакам у вашій мережі: остаточний контрольний список

1. Проведіть аудит мережі та розробіть стратегію захисту від DDoS-атак.
2. Зберіть ключові мережеві дані для вашого постачальника послуг захисту від DDoS-атак.

3. Закрийте невикористовувані порти та приховуйте невикористовувані IP-адреси.

4. Переконайтеся, що периферійні пристрої можуть обробляти DDoS-трафік.

5. Проведіть стрес-тести для оцінки стійкості мережі.

6. Впровадити надійний захист для DNS-серверів.

7. Інтегруйте захист від DDoS-атак у свою загальну стратегію безпеки.

Дотримуючись цих кроків, ви можете захистити свою мережу від DoS-атак і значно зменшити ризик простою через ці загрози.

DDoS-атаки можуть мати шкідливі наслідки для вашої організації, зокрема:

- Фінансові невдачі: Успішна DDoS-атака може призвести до зниження продуктивності, простоїв, втрати доходів та значних витрат на пом'якшення наслідків атаки та відновлення після неї.

- Збої в роботі: DDoS-атаки можуть паралізувати основні операції вашої організації або перешкодити клієнтам у доступі до послуг.

- Шкода репутації: DDoS-атаки можуть потенційно підірвати довіру та лояльність клієнтів, змушуючи їх обирати конкурентів через неможливість доступу до бажаного веб-сайту або сіючи сумніви щодо його надійності.

- Підвищені ризики для безпеки системи: DDoS-атаки можуть виявити існуючі слабкі місця в корпоративній мережі, які потім можуть бути використані зловмисниками для здійснення додаткових атак або отримання несанкціонованого доступу до системи.

Хоча кінцевою метою DDoS-атаки є зробити онлайн-сервіс недоступним для користувачів, методи, що використовуються для досягнення цієї мети, можуть відрізнятися. Різні типи DDoS-атак спрямовані на різні частини мережі та класифікуються на основі рівнів мережевого з'єднання, які вони використовують. Три основні типи: об'ємна атака, атака протоколу та атака прикладного рівня.

Об'ємні атаки

Найпоширенішим типом DDoS-атаки є волюметрична атака. Цей тип атаки зосереджений на перевантаженні мережі хибними запитами даних та виснаженні пропускної здатності мережі та можливостей обробки, що призводить до відмови в обслуговуванні для законних користувачів. Це часто досягається за допомогою ботнетів. Прикладом волюметричної атаки є посилення системи доменних імен (DNS), яке використовує відкриті DNS-сервери для надсилання багатьох DNS-запитів до цілі, що призводить до перевантаження трафіку. Атака перевантаження протоколу користувацьких дейтаграм (UDP) – це ще один тип волюметричної DDoS-атаки, метою якої є затоплення певного сервера пакетами інтернет-протоколу (IP) за допомогою UDP. Оскільки сервер не може визначити пункт призначення або цільову програму для цих пакетів, він відповідає повідомленнями «пункт призначення недоступний». Цей потік UDP-трафіку може перевантажити сервер, що призведе до перебоїв у обслуговуванні або простоїв.

Атаки на протоколи

Атаки на протоколи – це тип DDoS-атаки, спрямованої на порушення роботи сервісу шляхом використання вразливостей у протоколах, що використовуються для передачі даних. Мета полягає в перевантаженні ресурсів сервера та/або ресурсів мережевого обладнання, такого як брандмауери та балансувальники навантаження. На щастя, цей тип атаки зазвичай має чіткий слід і його легко виявити.

Прикладом протокольної атаки є атака синхронізації (SYN) перевантаженням, коли зловмисник надсилає цілі надмірну кількість запитів на з'єднання протоколу керування передачею (TCP), використовуючи підроблені вихідні IP-адреси. Цільові сервери намагаються виконати ці запити на з'єднання, але замість успішних з'єднань ціль отримує велику кількість запитів на з'єднання. Це перевантаження запитами виснажує ресурси цілі, фактично зв'язуючи систему та перешкоджаючи їй приймати легітимні з'єднання.

Атаки на рівні додатків

Атаки на рівні додатків спрямовані на слабкі місця в додатку. Ці атаки зосереджені переважно на прямому веб-трафіку та їх може бути важко виявити, оскільки машині може бути важко відрізнити їх від звичайного інтернет-трафіку з великим обсягом.

Поширеною формою атаки на рівні додатків є перевантаження через протокол передачі гіпертексту (HTTP), яке нагадує багаторазове оновлення веб-браузера на кількох комп'ютерах одночасно. Ця надмірна кількість HTTP-запитів перевантажує сервер, що призводить до відмови в обслуговуванні.

Прикладом HTTP-флуду є Slowloris, який в першу чергу націлений на веб-сервери. Під час атаки Slowloris зловмисник надсилає HTTP-запити на веб-сервер, але насправді ніколи не завершує їх. Періодично та повільно зловмисник додає додаткові заголовки, щоб продовжувати обробку запиту, так і не завершивши його. Ця стратегія змушує веб-сервер підтримувати відкриті з'єднання для цих частково завершених HTTP-запитів, що зрештою запобігає прийняттю будь-яких нових з'єднань.

Ще одним прикладом атаки на рівні додатків є ін'єкція структурованої мови запитів (SQL). За допомогою цієї форми SQL-ін'єкції зловмисники маніпулюють полями введення на веб-сайті, щоб виконувати шкідливі SQL-запити до бази даних, що споживатиме потужність веб-сервера та бази даних, а також виснажуватиме ресурси сервера.

3 мотивації DDoS-атаки

DDoS-атаки можуть бути ініційовані окремими особами, компаніями та навіть державами, кожна з яких має свої власні мотиви. Ось деякі можливі мотиви DDoS-атак:

1. Хактивізм: Хактивісти використовують DDoS-атаки як метод протесту та привернення уваги до своїх соціальних чи політичних проблем. Їхні цілі можуть включати уряди, політиків та великі бізнес-організації.

2. Вимагання: Вимагання стало популярною мотивацією для DDoS-атак, коли зловмисники вимагають викуп від своїх жертв, щоб зупинити DDoS-атаку.

3. Ідеологічні причини: Деякі зловмисники можуть ініціювати DDoS-атаки, керуючись своїми ідеологічними переконаннями. Це може включати осіб, які прагнуть порушити роботу та завдати шкоди компаніям чи організаціям, які вони вважають неетичними.

4. Кібервійна: Кібервійна зазвичай асоціюється з використанням державами DDoS-атак, що спонсоруються ними, для отримання політичної та військової переваги. Вони спрямовані на руйнування життєво важливих фінансових, медичних та інфраструктурних систем у країнах, на які спрямовані дії. Ці стратегії передбачають залучення добре навчених фахівців з технологій та пов'язані з урядовими військовими або терористичними організаціями. Багато урядів у всьому світі інвестували значні ресурси для здійснення атак, які порушують роботу онлайн- та критично важливої інфраструктури їхніх супротивників.

5. Конкуренція в бізнесі: DDoS-атаки все частіше використовуються як стратегічний інструмент для конкурентних підприємств. Основною метою застосування такої тактики є завдання фінансової та репутаційної шкоди конкуруючим компаніям з метою порушення їхніх послуг для отримання конкурентної переваги на ринку. Ці атаки можуть приймати різні форми, починаючи від запобігання участі конкурента в онлайн-заходах і закінчуючи повним порушенням їхньої онлайн-операцій на тривалий час.

6. Помста: Деякі особи або групи, які відчують розчарування через уявну несправедливість, можуть розпочинати DDoS-атаки як помсту проти особи чи організації.

Як виявити DDoS-атаку?

Виявлення DDoS-атаки передбачає розпізнавання ознак, які можуть свідчити про те, що ваша мережа піддається атаці. Наступні ознаки можуть потенційно вказувати на DDoS-атаку:

- Раптове та неочікуване зростання веб-трафіку з певного місця або IP-адреси
 - У більшості випадків ці запити на підключення неможливо виконати, оскільки справжнє джерело IP-пакетів приховане.
- Повільна або нестабільна робота мережі, наприклад, затримка завантаження веб-сайту
 - Це трапляється, коли зловмисник перевантажує сервер надмірним обсягом запитів, що призводить до помітного уповільнення роботи системи.
- Незрозумілі повідомлення про помилки сервера, тайм-аути або неможливість доступу до вашого веб-сайту

- Це трапляється, коли зловмисник завантажує ваш сервер великою кількістю запитів, що призводить до його перевантаження та виникнення помилки 503 "Служба недоступна", яка зазвичай пов'язана зі збоями в роботі сервісу. Зазвичай це вирішується самостійно, коли вхідний трафік зменшується. Однак, якщо проблема не зникає, це може свідчити про серйознішу проблему, таку як DDoS-атака.

- Працівники скаржаться на повільне з'єднання

- Це особливо актуально, якщо вони використовують те саме мережеве з'єднання, що й ваш вебсайт. У такому випадку це свідчить про те, що продуктивність мережі може бути порушена та пов'язана з DDoS-атакою.

- Зниження продуктивності інших служб, що використовують ту саму мережу

- Часто це відбувається через те, що запити зловмисника перевищують доступну пропускну здатність мережі, що призводить до уповільнення або перебоїв в роботі інших служб.

- Сповідання від постачальника інтернет-послуг (ISP), постачальника хмарних послуг (CSP) або іншого постачальника послуг

5 стратегій пом'якшення наслідків DDoS-атак

Основною проблемою у запобіганні DDoS-атаці є розрізнення легітимного трафіку та шкідливого трафіку. Проблема виникає через безліч різних типів DDoS-атак в Інтернеті. Ці атаки можуть набувати різних форм, починаючи від атак з одного джерела до складних атак з кількох джерел.

Складні DDoS-атаки можуть використовувати кілька шляхів для перевантаження цілі, одночасно використовуючи різні методи для перенаправлення зусиль щодо пом'якшення наслідків між цими різними маршрутами. Прикладом є одночасне націлювання на кілька рівнів стеку протоколів, наприклад, поєднання атаки посилення DNS з HTTP-флудом. Загалом, чим складніша атака, тим важче відрізнити трафік атаки від легітимного трафіку.

Зловмисники прагнуть залишатися непоміченими, щоб перешкоджати зусиллям щодо пом'якшення наслідків. Щоб ефективно протидіяти цим складним DDoS-атакам, слід впровадити багаторівневе захисне рішення для боротьби з різноманітними маршрутами атак. Ваше рішення має бути розроблене з урахуванням масштабованості, інтегрованого резервування, а також мати можливість моніторити трафік і ефективно керувати вразливостями.

Навчайте своїх співробітників

Навчання ваших співробітників є важливою частиною загальної стратегії кібербезпеки. DDoS-ботнет – це тактика, яку використовують зловмисники для компрометації мережі пристроїв шляхом дистанційного маніпулювання ними, щоб затопити ціль величезним обсягом трафіку. Зловмисники можуть використовувати пристрої нічого не підозрюючих співробітників як частину цього ботнету. Вкрай важливо навчити своїх співробітників, щоб вони розуміли, як захистити свої пристрої від такого використання.

Працівники можуть значно зменшити ризик стати учасником ботнету, дотримуючись наступних запобіжних заходів та впроваджуючи рекомендації, описані у відповідних інструкціях, зазначених нижче.

- Забезпечте регулярне оновлення ваших пристроїв та програмного забезпечення.

- Використовуйте багатофакторну автентифікацію для захисту своїх облікових записів.

- Будьте пильними щодо підозрілих електронних листів та їхніх вкладень.

- Використовуйте надійне рішення для захисту своїх пристроїв від шкідливих програм.

- Використовуйте надійну віртуальну приватну мережу (VPN).

- Резервне копіювання ваших пристроїв та інформації.

Реалізація маршрутизації чорних дір

Чорні діри – це контрзахід для пом'якшення DDoS-атаки шляхом відкидання вхідного трафіку, спрямованого на певну IP-адресу. За допомогою вашого інтернет-провайдера ваш мережевий адміністратор може встановити маршрут чорної діри, який спрямовує весь мережевий трафік на нульовий маршрут. Однак, якщо фільтрація чорних дір не має конкретних критеріїв обмеження, вона може направляти як легітимний, так і шкідливий мережевий трафік у чорну діру, назавжди видаляючи його з мережі. Маршрутизація чорних дір DDoS далеко не ідеальна, оскільки вона по суті досягає мети зловмисника, яка полягає в тому, щоб зробити мережу недоступною та потенційно спричинити втрати для бізнесу. Отже, її слід розглядати як крайній засіб, коли альтернативні методи пом'якшення виявляються неефективними. Незважаючи на свій потенціал допомогти зловмиснику досягти своїх цілей, маршрутизація чорних дір все ще може служити цінній меті, коли ціллю атаки є менший сайт у більшій мережі. У таких ситуаціях перенаправлення трафіку з цільового сайту за допомогою чорних дір може ефективно захистити більшу мережу від негативних наслідків атаки.

Впровадження обмеження швидкості

Обмеження швидкості – це ще один метод зменшення DDoS-атак, який передбачає встановлення обмежень на кількість запитів, які сервер може прийняти до певної IP-адреси протягом певного періоду часу. Це обмежить мережевий трафік і допоможе запобігти перевантаженню системних ресурсів з боку зловмисників. Впровадження обмеження швидкості – це хороший спосіб гарантувати, що законні користувачі все ще можуть отримати доступ до системних ресурсів, не перешкоджаючи загальній продуктивності програми. Хоча цей підхід сам по собі може не забезпечити повного захисту від складних DDoS-атак, він може служити цінним компонентом більш комплексної стратегії зменшення DDoS-атак.

Встановлення брандмауера веб-застосунку

Брандмауер веб-застосунків(WAF) – це захисний інструмент, який використовується для зменшення DDoS-атак на рівні додатків. Він служить зворотним проксі-сервером і створює щит між Інтернетом і вашими додатками. Він допомагає експертам з безпеки виявляти будь-який шкідливий трафік, який намагається порушити роботу ваших сервісів. WAF дозволяє вам контролювати вхідний трафік, дозволяючи або забороняючи доступ на основі попередньо визначеного набору правил безпеки. Ви можете почати з базового набору правил і налаштовувати їх у міру виявлення підозрілих закономірностей, пов'язаних з DDoS-атаками.

Забезпечити постійний моніторинг мережевого трафіку

Безперервний моніторинг (CM) та аналіз мережевого трафіку в режимі реального часу пропонують кілька переваг для виявлення та зменшення потенційних DDoS-атак. Впровадження виявлення вторгнень Системи виявлення вторгнень (IDS) та системи запобігання вторгненням (IPS) для постійного моніторингу мережевого трафіку ефективні у розпізнаванні та блокуванні підозрілих моделей трафіку, пов'язаних з DDoS-атаками. Використання цих інструментів аналізу трафіку дозволяє раннє виявлення DDoS-атак, що дозволяє швидко реагувати до ескалації атак. Моніторинг допомагає створити базовий рівень нормальної активності в мережі або комп'ютерних системах. Цей базовий рівень повинен охоплювати як дні із середнім, так і з високим трафіком. Він також допомагає зрозуміти нормальну мережеву активність та моделі трафіку, що полегшує розрізнення легітимного та шкідливого трафіку та виявлення незвичайної або підозрілої активності. Цілодобовий моніторинг також дозволить виявити майбутню атаку навіть у неробочий час та вихідні.

Реалізація розповсюдження мережі anycast

Одноадресна маршрутизація, що широко використовується в мережевому зв'язку завдяки своїй простоті та універсальності, обслуговує різні програми, такі як перегляд веб-сторінок, електронна пошта та передача файлів. В моделі одноадресної розсилки кожен мережевий вузол або пристрою призначається унікальна IP-адреса, що забезпечує прямий та

ефективний зв'язок по мережі. Однак, незважаючи на свою простоту, одноадресний зв'язок не є стійким до DDoS-атак. Оскільки трафік спрямовується безпосередньо до певного центру обробки даних, DDoS-атака може перевантажити це місце або навколишню інфраструктуру надмірним трафіком. Такий сплеск може призвести до відмови в обслуговуванні, що ускладнить виконання законних запитів. На відміну від одноадресної маршрутизації, мережеве поширення Anycast є більш стійким завдяки своїм унікальним характеристикам маршрутизації та адресації. Anycast розподіляє вхідний трафік по мережі серверів, розподілених у різних місцях, використовуючи одну й ту саму IP-адресу. Цей метод розширює покриття мережі, запобігаючи перевантаженню будь-якого місця шкідливими запитами. Коли на адресу надсилається надзвичайно великий обсяг трафіку, наприклад, під час DDoS-атаки, трафік автоматично перенаправляється до найближчого доступного місця в мережі, тим самим мінімізуючи вплив на основну інфраструктуру.

Маршрутизація Anycast підвищує стійкість мережі, роблячи атаки більш керованими та зменшуючи їхній потенціал для збоїв, тим самим забезпечуючи безперебійну доступність послуг. Широко розповсюджена конфігурація мережі ускладнює для зловмисників виконання DDoS-атаки, оскільки це вимагає значних ресурсів для ефективного надсилання шкідливого трафіку через ботнет.

Проведіть оцінку ризиків

Оцінка ризиків дозволить вам оцінити вразливість вашої організації до DDoS-атак. Вам слід регулярно проводити оцінки ризиків та аудити вашої мережевої інфраструктури, щоб виявити вразливості. Хоча повністю запобігти DDoS-атаці неможливо, повне розуміння апаратних та програмних активів вашої організації, включаючи їхні сильні та слабкі сторони, має вирішальне значення для забезпечення належного захисту. Визначення найбільш вразливих зон у вашій мережі є важливим для визначення найефективнішої стратегії пом'якшення впливу DDoS-атаки.

Проводячи оцінку ризиків, ви:

- Визначте критично важливі активи вашої організації та їх важливість для забезпечення безперервної роботи.

- Аналізуйте та оцінюйте потенційні загрози, що стосуються діяльності вашої організації.

- Визначте вразливості мережі вашої організації, включаючи слабкі місця, які можуть використовувати зловмисники, та оцініть вплив і ймовірність DDoS-атаки на основі історичних даних, розвідки загроз та галузевих тенденцій.

- Визначте різні шляхи, які зловмисники можуть використовувати для ініціювання DDoS-атаки, включаючи такі методи, як UDP-флуд, SYN-флуд або HTTP-флуд.

- Розставте пріоритети між виявленими ризиками, враховуючи такі фактори, як ймовірність здійснення атаки, потенційні наслідки атаки та ймовірність як виявлення, так і пом'якшення наслідків атаки.

Розробка плану реагування на DDoS-атаку

Для ефективної підготовки до DDoS-атаки вкрай важливо мати добре структурований план реагування. Цей план повинен містити чіткі кроки, які допоможуть виявити, пом'якшити та відновитися після атаки. Ваш план також має бути спрямований на мінімізацію впливу на вашу організацію та забезпечення безперебійного або мінімального простою у вашій бізнес-операції.

У рамках цього плану слід враховувати такі компоненти:

- Чітко окресліть та задокументуйте ролі та обов'язки всіх членів команди, які реагуватимуть на DDoS-атаку, включаючи внутрішніх зацікавлених сторін, керівників організації та мережевих адміністраторів, а також будь-яких залучених постачальників послуг.

- Розробіть вичерпний контрольний список, який визначає процеси та дії, необхідні під час DDoS-атаки. Вкажіть необхідні інструменти та ресурси, які будуть потрібні, та визначте осіб, з якими потрібно зв'язатися.

- Розробіть надійний план комунікації, який окреслює заздалегідь визначений ланцюжок зв'язку, якого слід дотримуватися у разі DDoS-атаки.

- Регулярно проводите навчання з реагування на інциденти та переконайтеся, що ваш план реагування на DDoS-атаки є невід'ємною частиною загальної стратегії аварійного відновлення та плану забезпечення безперервності бізнесу вашої організації.

Зверніться до постачальника послуг захисту від DDoS-атак

Якщо ваша організація має обмежені ресурси для управління кібербезпекою, ви можете розглянути можливість співпраці зі сторонніми організаціями для посилення захисту від кіберзагроз. Вони можуть пропонувати різні послуги захисту, включаючи очищення DDoS-трафіку, яке може допомогти захистити ваш інтернет-трафік від DDoS-атаки. Очищення DDoS-трафіку передбачає фільтрацію вхідного трафіку для виявлення та видалення шкідливих даних, дозволяючи лише легітимному трафіку потрапляти до цільової мережі. Це дозволить вам підтримувати онлайн-присутність під час атак, не втрачаючи зв'язку.

Більшість інтернет-провайдерів та постачальників послуг зв'язку пропонують певний рівень захисту від DDoS-атак. Вам слід дізнатися про захисні заходи, які вони надають, та переглянути угоду про надання послуг, щоб визначити будь-які потенційні обмеження їхнього покриття.

Використання хмарних рішень для запобігання DDoS-атак також може запропонувати багато переваг. До них належать спеціалізований персонал, який забезпечує швидший час реагування у разі атаки, та висока пропускна здатність мережі, що робить їх більш стійкими до DDoS-атак на основі обсягів. Ці рішення також можуть забезпечувати автоматичні варіанти реплікації або резервного копіювання, що дозволяє вам запускати свої сервіси, не перериваючи роботу користувачів.

Якщо вам потрібне ще надійніше рішення для захисту від DDoS-атак, зверніться до постачальника керованих послуг (MSP), щоб дослідити рішення, адаптовані до потреб вашої організації для захисту від DDoS-атак. Ці служби вміють активно моніторити ваш мережевий трафік, виявляти будь-які ознаки атаки, визначати її походження та вживати заходів для перенаправлення шкідливого трафіку з вашої мережі.

Звернення до постачальника керованих послуг (MSP) для захисту від DDoS-атак пропонує численні переваги. MSP, що спеціалізуються на кібербезпеці, надають досвід, передові технології та цілодобовий моніторинг для раннього виявлення загроз. Вони швидко реагують на атаки та масштабують послуги відповідно до потреб мережі. MSP постійно оновлюють системи, щоб випереджати нові загрози, забезпечуючи стратегічний та ефективний підхід до захисту онлайн-сервісів. Довіряючи захист від DDoS-атак постачальнику керованих послуг (MSP), ваша внутрішня IT-команда може зосередитися на основних бізнес-операціях, а не постійно моніторити та реагувати на потенційні кіберзагрози.

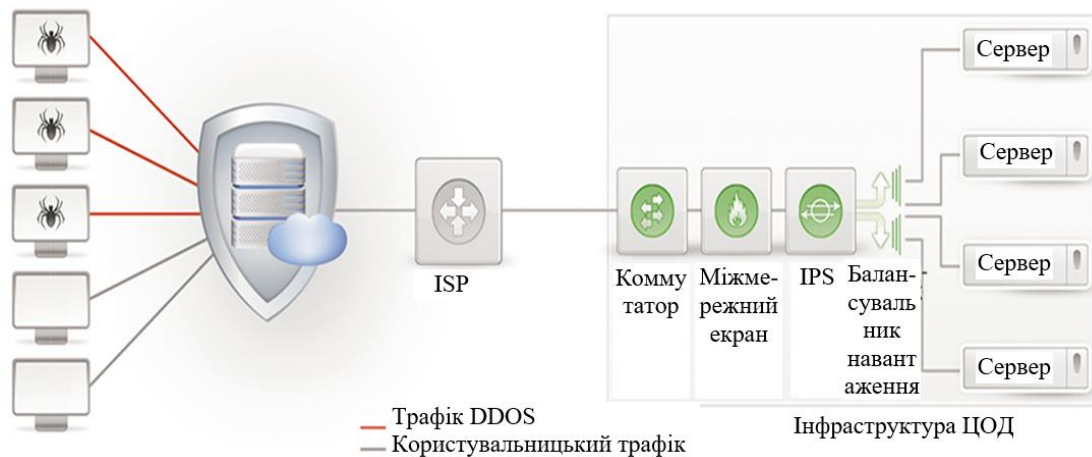


Рисунок 1 – Структурна схема системи

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів протидії мережевим DDoS-атакам. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем протидії мережевим DDoS-атакам.
- Досліджена система протидії мережевим DDoS-атакам.
- На основі отриманих результатів досліджень створена програмна реалізація системи протидії мережевим DDoS-атакам.

Розроблені алгоритми дозволяють успішно вирішувати завдання протидії мережевим DDoS-атакам. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Smirnov, O., Neskorodieva, T., Fedorov, E., Rudakov, K., Neskorodieva, A. «Method Detection Audit Data Anomalies on Basis Restricted Cauchy Machine» CEUR Workshop Proceedings, Volume 3187, 2022,
2. Smirnov O.A., Al-Oraiqat A.M., Ulichev O.S., Meleshko Ye.V., Al-Rawashdeh H.S., Polishchuk L.I. «Modeling strategies for information influence dissemination in social networks». Journal of Ambient Intelligence and Humanized Computing Volume 13, Issue 5. Springer, Cham. 2022, pp. 2463-2477.
3. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». Проблеми інформатизації та управління, № 2(70). 2022. С. 28-37.
4. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 3(69). С. 93-98.
5. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Вісник Хмельницького національного університету. Серія: «Технічні науки», № 2 (307). С. 46-52. 2022.
6. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 1(67). С. 84-89.
7. Smirnov O., Kuznetsov A., Zhora V., Onikiychuk A., Pieshkova O. «Hiding Messages in Audio Files Using Direct Spread Spectrum». 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2021, Cracow, Poland, 22-25 September 2021. P. 414-418
8. Smirnov O., Kuznetsov A., Lokotkova I., Kuznetsova T., Florov S., Lebid O. «Using Orthogonal Signals to Hide Information in Images». 4 IEEE International Conference on Advanced Information and Communication Technologies (AICT) - 2021, Lviv, Ukraine, September 21-25, 2021. P. 255-260.
9. Smirnov O., Kuznetsov A., Girzheva O., Kiian A., Nakisko O., Kuznetsova T. «Advanced Code-Based Electronic Digital Signature Scheme». 2020 IEEE International Conference on Problems of Infocommunications Science and Technology, PIC S and T 2020, Kharkiv, 6 October 2020-9 October 2020, P. 358-362.

10. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova K. «Data hiding scheme based on spread sequence addressing». CEUR Workshop Proceedings Volume 2805, 2020, Pages 44-58.
11. Smirnov, O., Kuznetsov, A., Potii, O., Poluyanenko, N., Stelnyk, I., Mialkovsky, D. «Combining and filtering functions in the framework of nonlinear-feedback shift register». International Journal of Computing; 2020, Volume 19, Issue 2 – Research Institute for Intelligent Computer Systems – 2020. – P. 247-256.
12. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
13. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». Journal of theoretical and applied information technology Vol.98. No 21, 2020, P. 3334-3346.
14. Smirnov O., Kuznetsov A., Arischenko A., Chepurko I., Onikiychuk A., Kuznetsova T. «Pseudorandom sequences for spread spectrum image steganography». CEUR Workshop Proceedings Volume 2654, 2020, Pages 122-131.
15. Smirnov O., Kuznetsov A., Kovalchuk D., Kuznetsova T. «New technique for data hiding in cover images using adaptively generated pseudorandom sequences». CEUR Workshop Proceedings Volume 2654, 2020, Pages 1-14.
16. Smirnov O., Lutsenko M., Kuznetsov A., Kiian A., Kuznetsova T., «Biometric cryptosystems: overview, state-of-the-art and perspective directions». Lecture Notes in Networks and Systems, vol 152. Springer, Cham. 2021, pp 66-84.
17. Smirnov O., Kuznetsov A., Onikiychuk A., Makushenko T., Anisimova O., Arischenko A. «Adaptive pseudorandom sequence generation for spread spectrum image steganography». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 161-165.
18. Smirnov O., Kuznetsov A., Kiian A., Babenko V., Perevozova I., Chepurko I. «New Approach to the Implementation of Post-Quantum Digital Signature Scheme». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 166-171.
19. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177.
20. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587.
21. Smirnov, O., Markovets, O. Vovk, N., Turchyn, Y., «Model of informational support for social network administrators' content creation». CEUR Workshop Proceedings Volume 2616, 2020, Pages 125-136.
22. Smirnov, O., Shekhanin, K., Kuznetsov, A., Krasnobayev, V. «Detecting Hidden Information in FAT». International Journal of Computer Network and Information Security (IJCNIS). Vol. 12, No. 3, 2020. PP.33-43.
23. Smirnov, O., Kuznetsov, A., Gorbacheva, L., Babenko, V., «Hiding data in images using a pseudo-random sequence», CEUR Workshop Proceedings Volume 2608, 2020, Pages 646-660.
24. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.
25. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019 . P.517-522.
26. Smirnov, O., Ulichev, O., Meleshko, Y., Khokh, V., Goncharenko, I. «Method of Choosing Objects for Informational Influence in Social Networks during Information Campaign Based on the Analytic Hierarchy Process». CEUR Workshop Proceedings, Vol 2588, P. 215-227, 2019.
27. Smirnov, O., Krasnobayev, V., Yanko, A., Kuznetsova, T. «Methods of nulling numbers in the system of residual classes». CEUR Workshop Proceedings, Vol 2588, P. 90-106, 2019.
28. Smirnov, O., Kuznetsov, A., Kiian, A., Gorbenko, Y., Cherep, O., Bexhter L. «Code-based Pseudorandom Generator for the Post-Quantum Period», 2019 IEEE International Conference on Advanced Trends in Information Theory (IEEE ATIT 2019). 18.12.19-20.12.19 Kyiv Ukraine. P. 204 – 209.
29. Smirnov, O., Kuznetsov, A., Nariezhnii, O., Stelnyk, S., Kokhanovska, T., Kuznetsova T., «Side Channel Attack on a Quantum Random Number Generator», 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2019; Metz; France; 18 -21 September 2019. P.713-718.
30. Smirnov, O., Kuznetsov, A., Kiian, A., Pushkar'ov, A., Mialkovskyi, D., Kuznetsova, T., «Code-Based Schemes for Post-Quantum Digital Signatures», 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2019; Metz; France; 18-21 September 2019. P. 707-712.
31. Smirnov, O., Kuznetsov, A., Stefanovych, O., Gorbenko, Y., Krasnobaev, V., Kuznetsova K. «Information Hiding Using 3D-Printing Technology», 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2019; Metz; France; 18-21 September 2019. P.701-706.

УДК 004

Д.Татаров, магістр гр. КН-24М,

Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ВИЗНАЧЕННЯ КОНТЕКСТУ КОРИСТУВАЧА НА ОСНОВІ АРХІТЕКТУРИ CODA

У статті розроблено програмне забезпечення, яке призначено для системи визначення контексту користувача на основі архітектури CoDA. Метою розробки є дослідження та принципи побудови системи визначення контексту користувача на основі архітектури CoDA. Об'єктом дослідження є процес визначення контексту користувача на основі архітектури CoDA. Предметом дослідження є методи визначення контексту користувача на основі архітектури CoDA. Методи дослідження базуються на методах теорії комп'ютерних мереж, теорії захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи визначення контексту користувача на основі архітектури CoDA. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

визначення контексту користувача, CoDA

Постановка проблеми. Gartner визначає CoDA. (Context delivery architecture, Архітектура доставки контексту) як архітектурний стиль, який спирається на стилі взаємодії та розбиття сервіс-орієнтовані архітектури (SOA) та архітектури, керованої подіями (EDA), і додає формальні механізми елементів програмного забезпечення, які відкривають та застосовують контекст користувача в реальному часі. CoDA. надає структуру архітекторам рішень, що дозволяє їм визначати та реалізовувати компоненти технології, інформації та процесів, які дозволяють службам використовувати контекстну інформацію для підвищення якості взаємодії з користувачем. Технології можуть включати контекстних брокерів, моніторів стану, датчиків, аналітичних движків та хмарних двигунів обробки транзакцій.

До того, як з'явився CoDA, існувала SOA (Service-Oriented Architecture), яка являє собою набір принципів та методологій для проектування та розробки програмного забезпечення у формі сумісних служб.

Реалізація SOA покладається на сітці неузгодженого програмного забезпечення, що є вільно пов'язаними одиницями функціональності, які не мають прямого зв'язку один з одним. Кожна служба керує конкретним та незалежним фрагментом функціональності та використовує визначені протоколи, які описують, як передавати інформацію між собою.

SOA покладається на сервісну орієнтацію як на основний принцип проектування. Якщо служба представляє собою простий інтерфейс, який вичерпує його основну складність, користувачі можуть отримати доступ до незалежних служб без знання реалізації платформи служби, включаючи основну операційну систему, мову програмування або апаратне забезпечення.

SOA допомагає підприємствам реагувати швидше та економічно ефективніше на мінливі ринкові умови шляхом заохочення повторного використання на рівні сервісу, а не на мікро (кодовому) рівні.

CoDA або Архітектура доставки контексту забезпечує контекстні послуги, які з'єднуються в рамках SOA. В результаті постачальники послуг, постачальники послуг мережі та інтегратори програмного забезпечення можуть розвивати контекст.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи визначення контексту користувача на основі архітектури CoDA.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи визначення контексту користувача на основі архітектури CoDA.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем визначення контексту користувача на основі архітектури CoDA.
- Дослідження системи визначення контексту користувача на основі архітектури CoDA.
- Програмна реалізація системи визначення контексту користувача на основі архітектури CoDA.

Об'єктом дослідження є процес визначення контексту користувача на основі архітектури CoDA.

Предметом дослідження є методи визначення контексту користувача на основі архітектури CoDA.

Методи дослідження базуються на методах теорії комп'ютерних мереж, теорії захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу.

Архітектура доставки контексту (CoDA) забезпечує індивідуальний цифровий досвід у режимі реального часу, узгоджуючи дані, наміри та доставку по каналах. По суті, CoDA узгоджує те, чого хоче користувач – прямо зараз – з тим, як цей досвід доставляється через цифрові точки контакту. Замість того, щоб покладатися на статичний контент або заздалегідь визначені шляхи, ця архітектура динамічно адаптує відповіді на основі контексту користувача – місцезнаходження, пристрою, поведінки, уподобань – та передбачуваного наміру кожної взаємодії.

У сучасній гіперперсоналізованій екосистемі користувачі очікують більшого, ніж просто доступності. Вони вимагають актуальності, негайності та інтуїтивно оптимізованого досвіду в веб-, мобільних, Інтернеті речей та підключених середовищах. Від електронної комерції до платформ цифрової охорони здоров'я, здатність надавати персоналізований контент на основі намірів, контексту та стану мережі виділяє лідерів галузі.

У даній роботі розглядаються фундаментальні концепції, що формують CoDA, починаючи з визначення контексту та наміру користувача, переходячи до інтелектуальних механізмів доставки та завершуючи роллю якості обслуговування (QoS) у забезпеченні безперебійного виконання. Попутно розглядаються основні технології, такі як периферійні обчислення, оркестрація на основі штучного інтелекту, адаптивні механізми рендерингу, мережі доставки досвіду та брокери контексту. Готові побачити, як інфраструктура поєднується з інтелектом? Давайте зазирнемо всередину механізму.

Стратегічне значення контексту в сучасних цифрових застосунках

Аналіз контексту: що це насправді означає в дизайні застосунків

Контекст стосується ситуативних факторів, які формують взаємодію користувача з цифровим продуктом. До них належать місцезнаходження користувача, характеристики пристрою (такі як розмір екрана, операційна система або обчислювальна потужність), часові сигнали, такі як час доби або день тижня, та моделі поведінки, такі як історія переглядів, попередні покупки або навігаційні шляхи в додатку. Додайте визначені користувачем налаштування, такі як мовні налаштування або налаштування сповіщень, і цифрове середовище отримує рівні значення та наміру.

Кожна змінна створює сигнал, який, будучи зареєстрованим у режимі реального часу та точно інтерпретованим, перетворює статичний цифровий досвід на адаптивне середовище. Користувач, який переглядає роздрібний додаток на телефоні під час поїздки на роботу та з

роботи, демонструє інші моделі взаємодії, ніж користувач, який використовує комп'ютер у робочий час. Контекст визначає різницю між наданням загального інтерфейсу та пропонуванням конкретної відповіді, побудованої на спостережуваній потребі.

Від статичного до динамічного: чому контекст визначає релевантність

Релевантність не виникає випадково. Системи повинні реагувати на зміну вхідних даних, щоб відповідати динамічним очікуванням. Цифрові додатки, оснащені контекстною усвідомленістю, коригують контент, функціональність та робочі процеси у відповідь на мінливе середовище.

- Push-сповіщення плануються на основі місцевого часу та вікон сприйняття поведінки.

- Рекомендації щодо контенту розвиваються синхронно з послідовностями перегляду та станами виконання завдань.

- Потоки автентифікації змінюються залежно від цілісності мережі або стану пристрою.

Кожен контекстний вхідний сигнал змінює ймовірність того, що користувач взаємодітиме, здійснить конверсію або повернеться. Замість того, щоб покладатися на статичні правила, додатки, що враховують контекст, використовують ці сигнали для прийняття рішень у режимі реального часу, що безпосередньо призводить до підвищення операційної ефективності та більш інтуїтивного взаємодії з користувачем.

Контекст як основа персоналізації

Ефективна персоналізація залежить від глибокого контексту. Хоча більшість систем покладаються на дані про ідентичність та вподобання, вони часто недостатньо використовують ефемерні сигнали – той вид миттєвих вхідних даних, які забезпечують ситуативну релевантність. Співвідносячи довгострокові профілі з поточними спостереженнями, сучасні архітектури забезпечують точний досвід.

Розглянемо різницю між пропозицією знижки всім користувачам та орієнтацією на користувачів у холоднішому кліматі за допомогою акцій на зимове спорядження. Пристрої можуть бути однаковими, але середовища хостингу відрізняються. Контекстно-залежна система розпізнає це та діє. Цей прямий зв'язок між екологічною обізнаністю та адаптацією досвіду переводить персоналізацію з реактивної на проактивну.

На практиці, персоналізація, що відповідає контексту, змінює правила гри для всього: від цифрових вітрин та медіаплатформ до інтерфейсів телемедицини та корпоративних панелей керування. Йдеться вже не про надання контенту, а про забезпечення правильної взаємодії, через правильний канал, за правильних умов.

Розкриття основних принципів архітектури доставки контексту

Контекстна усвідомленість: сприйняття та адаптація в режимі реального часу

В основі доставки контексту лежить здатність систем активно сприймати дані про навколишнє середовище та реагувати відповідно. Цей принцип перетворює статичні програми на динамічні, адаптивні до потреб користувачів. Використовуючи сигнали від пристроїв, поведінки користувача, місцезнаходження, часу доби та станів системи, контекстно-залежні архітектури ініціюють відповідні дії. Ці зміни відбуваються не через жорстке кодування, а через вивід під час виконання – системи навчаються на операційних даних та миттєво коригують свою поведінку.

Наприклад, навігаційний додаток, виявляючи раптові збільшення заторів, змінює маршрут користувача на основі поточних даних про дорожній рух, моделей водіння користувача та історичних тенденцій заторів. Це не просто реакція; це превентивна адаптація, що стала можливою завдяки інтегрованим даним датчиків та механізмам прогнозування.

Модульність: багаторівневі компоненти з чіткою відповідальністю

Системи доставки контексту працюють безперебійно, коли побудовані на модульній архітектурі. Кожен рівень – прийом даних, логічний висновок та доставка – функціонує незалежно, але взаємодіє через чітко визначені інтерфейси. Така модульність сприяє

швидшій ітерації, ефективнішому усуненню несправностей та безперешкодному оновленню окремих компонентів.

- Рівень захоплення: збирає дані з датчиків, взаємодії з користувачами та зовнішніх систем, таких як API або журнали бази даних.

- Рівень логічного висновку: обробляє необроблені дані, застосовує моделі машинного навчання або механізми правил для отримання корисних висновків.

- Рівень доставки: перетворює аналітичні дані на зміни інтерфейсу користувача, зміни поведінки системи або відповіді API у режимі реального часу.

Розв'язка також підтримує співпрацю між командами: фахівці з обробки даних покращують моделі логічного висновку, не торкаючись інтерфейсу користувача, тоді як фронтенд-інженери налаштовують механізми доставки зі стабільними вхідними даними.

Масштабованість та мінімізація затримки

Контекстно-залежні системи взаємодіють з величезними потоками даних. Щоб надійно обробляти це, вони повинні масштабуватися горизонтально. Це означає, що архітектури повинні враховувати зростаючу кількість користувачів, пристроїв і точок даних без погіршення продуктивності.

Мінімізація затримки під час цього процесу масштабування не є обов'язковою – вона сприяє утриманню користувачів. Дослідження, проведене Google, показало, що мобільні користувачі залишають сторінки, які завантажуються довше 3 секунд. У контекстній доставці вікно допуску ще вужче. Для прогнозних систем, таких як системи рекомендацій, затримка, що перевищує 200 мілісекунд, може перервати потік користувачів і зменшити залученість.

Щоб відповідати цим вимогам, архітектури доставки контексту включають периферійні обчислення, сітки даних в пам'яті, асинхронні шаблони обміну повідомленнями та паралельні конвеєри обробки.

Безшовна інтеграція між пристроями та платформами

Контекст не знаходиться в одному додатку чи пристрої. Він рухається разом з користувачем – від смартфонів до планшетів, від пристроїв Інтернету речей до носимих пристроїв. Архітектура повинна підтримувати безперервність між сесіями, місцями розташування та апаратними екосистемами. Це включає підтримку обізнаності про стан та уніфікованих моделей користувачів через розподілене управління ідентифікацією та рівні збереження контексту.

Уявіть собі роздрібного покупця, який починає переглядати товари на планшеті, додає товари до кошика через мобільний пристрій, а потім завершує покупку на комп'ютері. Щоб цей досвід був цілісним, архітектура серверної частини розпізнає контекст як потік першокласних даних, а не як розрізнені вхідні дані. Цей уніфікований дизайн дозволяє системам виявляти правильний контент, підтримувати релевантність і синхронізувати дії протягом усього шляху користувача.

Технології, що забезпечують архітектуру доставки контексту

Обробка даних у реальному часі

Системи доставки контексту вимагають швидкої реакції. Обробка даних у режимі реального часу усуває затримки, постійно надаючи додаткам актуальну інформацію. Рішення, що залежать від навколишніх ситуаційних даних – поведінки користувача, місцезнаходження, стану пристрою – отримують точність і оперативність завдяки цій можливості.

Фреймворки для обробки потоків формують основу систем реального часу. Apache Kafka обробляє високопродуктивні конвеєри даних у розподілених системах, діючи як надійна основа для публікації та підписки на контекстні події. Apache Flink, з іншого боку, оптимізує аналітику з низькою затримкою для необмежених потоків, що робить її ідеальною для оцінки та оновлення контексту в режимі реального часу в міру надходження вхідних сигналів.

Механізми перетворення та збагачення переплітають необроблені сигнали із семантикою. Наприклад, перетворені телеметричні дані часових рядів можуть включати виведені типи активності – ходьба, водіння, сидіння – отримані з шаблонів акселерометра. Таке збагачення надає контекстним наборам даних їхню інтерпретованість, дозволяючи системам ефективніше реагувати на сигнальні тригери.

Периферійні обчислення для швидкої оцінки контексту

Зміщення обчислень контексту ближче до джерела даних скорочує затримку та підвищує ситуаційну обізнаність. Саме тут вступають у гру периферійні обчислення. Обробка контекстних подій поблизу периферії зменшує час передачі даних до централізованих серверних частин, що дозволяє приймати рішення на міросекундному рівні. Такі програми, як автономна навігація, промислова робототехніка та персоналізовані дисплеї для роздрібно́ї торгівлі, залежать від цих надшвидких реакцій.

Периферійні пристрої – телефони, смарт-хаби, камери – стають не просто збирачами, а й інтерпретаторами контексту. Їхня вбудована логіка визначає шаблони локально. Наприклад, роздрібний дисплей може використовувати розпізнавання обличчя для адаптації рекламного контенту на основі вікової групи покупця або тривалості концентрації уваги, і все це обробляється на пристрої без залежності від хмари.

Інтернет речей та дані датчиків

Датчики роблять фізичний світ контекстуально доступним. Вхідні дані з різних модальностей – руху, світла, звуку, температури чи біометрії – створюють навколишній інтелект. Пристрої збирають ці дані пасивно, дозволяючи цифровим системам «відчувати» своє оточення.

Носимі пристрої, такі як розумні годинники, безперервно подають фізіологічні сигнали, які можуть інформувати про рівень стресу або тип активності. Смартфони постійно відстежують місцезнаходження користувача та моделі взаємодії. Розумні будинки та підключені транспортні засоби – за допомогою вбудованих датчиків – генерують дані про навколишнє середовище, які безпосередньо надходять до контекстного механізму.

Разом ці розподілені джерела даних з реального світу утворюють динамічну карту поведінки користувачів та середовища. Цей фізичний контекст забезпечує різні варіанти використання – від моніторингу здоров'я до адаптивної міської інфраструктури.

Семантична інтеграція даних

Інтеграція контексту означає стандартизацію того, як різні дані взаємодіють один з одним. Це вимагає семантичного рівня, який узгоджує різноманітні джерела. Онтології визначають поняття та зв'язки між ними – що становить «намір користувача» або значення «дім» проти «офіс» – тоді як метадані анують ці сигнали машинозчитуваним значенням.

Такі технології, як RDF (Resource Description Framework), структурують цей граф даних. SPARQL надає мову запитів для його проходження та вилучення з нього значення. У поєднанні з принципами пов'язаних даних системи можуть виявляти нові контекстні шляхи між доменами, навіть коли базові джерела є різноманітними та розподіленими.

Машинне навчання для контекстного виведення

Необроблені дані рідко розповідають повну картину. Моделі логічного висновку перетворюють комбінації сигналів на прогнозне розуміння. Моделі з учителем навчаються на основі позначеної поведінки, щоб розпізнавати заздалегідь визначені контексти, такі як виявлення того, коли клієнт активно робить покупки, а коли просто переглядає веб-сторінки. Моделі без учителя групують та виявляють нові стани, наприклад, виявлення аномалій у робочих процесах користувачів.

Навчання з підкріпленням динамічно адаптує послуги. Спостерігаючи за зворотним зв'язком попередніх взаємодій, ці системи оптимізують результати, що залежать від контексту. Вони можуть вибирати, який діалог використовувати у віртуальному помічнику, або точно налаштовувати рейтинг рекомендацій на основі передбачуваних змін намірів.

Вилучення ознак перетворює необроблені вхідні дані, такі як аудіошаблони або кластери датчиків, на контекстні вбудовування. Ці конденсовані, високовимірні вектори

представляють ситуаційні нюанси у формі, придатній для сприйняття машиною. Контекстно-залежні системи, що використовують такі вбудовування, отримують здатність моделювати не лише те, що відбувається, але й чому, і що, ймовірно, буде далі.

Архітектура фундаменту: Будівельні блоки системи доставки контексту

Рівень збору даних

Відправною точкою будь-якої контекстно-залежної архітектури є надійний та різноманітний надходження даних. Добре функціонуючий рівень збору даних інтегрує кілька джерел інформації для фіксації динамічного середовища, що оточує користувача, у режимі реального часу.

- Датчики: Захоплюють сигнали низького рівня – GPS для визначення місцезнаходження, акселерометри для руху, датчики навколишнього освітлення для визначення умов навколишнього середовища.

- Трекери подій: відстежують взаємодію користувачів на різних платформах і пристроях, збираючи детальні дані про поведінку.

- Налаштування користувача: Включають як явно зазначені опції, так і виведені з часом шаблони, що пропонують важливі дані для персоналізації.

- Зовнішні API: надсилає дані зі сторонніх сервісів, таких як метеорологічні служби, агрегатори трафіку, фінансові ринки тощо.

Разом ці канали створюють багатовимірний профіль контексту реального часу. Вони слугують вихідними даними для наступного операційного рівня – обробки та міркування.

Рівень обробки контексту та міркування

На цьому етапі необроблені дані перетворюються на практичну інформацію. Цей рівень інтерпретує непересічні метадані та перетворює їх на структурований контекст за допомогою передових обчислювальних інструментів.

- Контекстні механізми: центральні процесори, які узгоджують вхідні дані з моделями користувачів та контекстними фреймворками.

- Системи логічного висновку: інтерпретація на основі логіки керування. Наприклад, розпізнавання того, що користувач, який рухається, підключений до системи Bluetooth автомобіля, ймовірно, керує автомобілем.

- Графи знань: забезпечують структуровані семантичні зв'язки між контекстними сутностями, що дозволяє системам з більшою точністю міркувати про наміри користувача.

Співпраця між логічними механізмами та моделями навчання призводить до розуміння змін стану користувача та умов навколишнього середовища в режимі реального часу, що дозволяє проактивно реагувати на доставку.

Адаптація та рівень надання послуг

Після того, як контекст користувача інтерпретовано, система повинна відповідно адаптувати свої послуги. Саме тут аналітичні дані перетворюються на персоналізований досвід.

- Логіка на основі правил та прогнозування: визначає, як і коли коригувати послуги. Логіка на основі правил працює на детермінованих умовах, тоді як прогнозування використовує ймовірності, отримані з моделей машинного навчання.

- Логіка програми: Змінює поведінку функцій залежно від контексту, наприклад, вимикає сповіщення в соціальних програмах під час зустрічей, запланованих у календарі.

- Коригування інтерфейсу користувача: Включає зміни інтерфейсу в режимі реального часу, такі як збільшення розміру шрифту на сонці або спрощення інтерфейсу користувача під час керування автомобілем.

Цей рівень визначає, наскільки інтелектуально та витончено застосунок реагує на зміни контексту, забезпечуючи адаптивність без перебоїв.

Цикл зворотного зв'язку

Жодна система доставки контексту не працює у вакуумі, і жодна конфігурація не залишається оптимальною вічно. Увійдіть у цикл зворотного зв'язку – безперервний механізм удосконалення.

Дії користувача після адаптації сервісу відображаються в системі, допомагаючи перекалібрувати моделі, налаштувати правила та переглянути припущення. З часом цей цикл підвищує точність реагування, виявляє нові закономірності та відкриває можливості для глибшої персоналізації. Чим більше система слухає, тим розумнішою вона стає.

Проектування для користувача: адаптивні та інтелектуальні інтерфейси

Адаптивні інтерфейси користувача (AUI)

Інтерфейси більше не функціонують у вакуумі. Адаптивні користувацькі інтерфейси (AUI) динамічно реагують на середовище, наміри, пристрій та історичні моделі взаємодії кожного користувача. Ця адаптивність виходить за рамки простих налаштувань чи вибору тем. AUI змінюють ієрархію макета, елементи навігації, зворотний зв'язок про взаємодію та навіть доступність функцій у відповідь на контекстні тригери.

Наприклад, додаток для продуктивності може надавати пріоритет інструментам для співпраці під час робочого часу на комп'ютері, але відображати швидкі нотатки та віджети календаря під час поїздки користувача на роботу через мобільний пристрій. Така поведінка не є жорстко запрограмованою – вона походить від контекстного механізму, який інтерпретує такі сигнали, як час, місцезнаходження, рух та тип пристрою.

Елементи інтерфейсу користувача, які переналаштовуються в режимі реального часу

Динамічні елементи інтерфейсу значною мірою спираються на контекстні сигнали. Вхідні дані в режимі реального часу, такі як рівень навколишнього шуму, пропускну здатність інтернету, виявлення руху або спосіб введення, активують правила конфігурації, які за потреби реструктуризують компоненти інтерфейсу. Картки інтерфейсу можуть згортатися або розгортатися, панелі інструментів можуть змінювати порядок, а переходи адаптуються за інтенсивністю або швидкістю анімації.

- Панель навігації може перемикатися з значків + підписів на значки лише у сценаріях низької пропускну здатності або обмеженого простору.
- Голосові підказки можуть з'являтися в середовищах, де використання hands-free передбачається.
- Підказки та мікровзаємодії можуть подовжити видимість, коли дані вказують на те, що користувач новачок у наборі функцій.

Стратегії персоналізації

Універсальний досвід створює тертя. Персоналізовані інтерфейси уникають цього, використовуючи моделі контекстних шарів, які відстежують сегменти користувачів, уподобання, мікроповедінку та історію подій. Послідовність контенту, модифікація тонів повідомлень та рекомендації функцій адаптуються до намірів та архетипів персонажів.

Розглянемо освітній додаток: студент першого курсу інженерного факультету отримує більше візуальних матеріалів та спрощену термінологію, тоді як студент старших курсів отримує глибшу аналітику та посилання на дослідження. Базова модель персоналізації використовує дерева рішень або класифікатори машинного навчання, навчені на когортах та мітках використання, для запуску варіацій інтерфейсу.

Послідовність контенту, тон повідомлень та рекомендації щодо функцій:

- Послідовність контенту: статті, модулі чи ресурси відображаються на основі попередньої споживчої поведінки та контекстуального часу, наприклад, з'являються навчальні матеріали ближче до екзаменаційних сесій.
- Тон повідомлення: Мова сповіщень пом'якшується або загострюється відповідно до моделювання стану користувача (наприклад, користувачі, що перебувають у стані стресу, отримують заспокоїливі, інформативні оновлення, а не термінові пінги).
- Рекомендації щодо функцій: функції програми відображаються контекстуально, залежно від ймовірності релевантності, передбачуваних цілей або нещодавно випущених функцій, що відповідають історичним потребам.

Аналіз поведінки користувачів

Успішне виконання контекстних інтерфейсів вимагає безперервної поведінкової телеметрії. Одних лише сирих даних недостатньо для оптимізації – системи доставки контексту аналізують їх на корисні шаблони за допомогою сегментації та відображення взаємодії.

Відстеження включає шляхи дотику, глибину прокручування, час виконання завдання, рівень перерв та вагання під час введення. Ці показники, коли вони агреговані та проаналізовані, впливають як на адаптацію інтерфейсу користувача, так і на пріоритезацію контенту.

Теплові карти, повтори сеансів та поведінкові сегменти:

- Теплові карти візуалізують місця концентрації уваги та взаємодії. Інтенсивні зони можуть свідчити про перенаселеність, тоді як ігноровані елементи сигналізують про неактуальність.

- Повтори сесій сприяють якісному аналізу, виявляючи вагання, помилки кліків або перешкоди під час адаптації, які не завжди очевидні в сукупних показниках.

- Поведінкові сегменти класифікують користувачів за такими параметрами, як орієнтація на ціль, цифрова грамотність або контекст сеансу, що дозволяє точніше налаштовувати інтерфейс.

Фіксуєючи мікровзаємодії в режимі реального часу та поєднуючи їх із шарами інтерпретації з високим контекстом, сучасні інтерфейси переходять від реактивних до справді випереджальних.

Сервісні шини та мікросервіси для модульної доставки

Архітектури корпоративного рівня дотримуються модульності завдяки сервісним шинам та мікросервісам. Легка корпоративна сервісна шина (ESB) координує незалежні мікросервіси, призначені для аналізу рівнів контексту, таких як місцезнаходження, активність, ідентифікація та поведінка. Кожен мікросервіс розвивається незалежно, що дозволяє системі вибірково масштабуватися та підтримувати стримування відмов. Такі інструменти, як Istio та Linkerd, підтримують реалізацію сервісної мережі, забезпечуючи спостережуваність та стійкість в екосистемі доставки контексту.

Обробка рівня контекстного API Внутрішня та зовнішня інтеграція

В основі лежить рівень контекстного API. Цей трансверсальний рівень приймає, обробляє та надає контекст як внутрішнім модулям, так і зовнішнім партнерам. Він використовує поєднання кінцевих точок RESTful та GraphQL, що дозволяє точно фільтрувати, змінювати та запитувати контекст у режимі реального часу. Зовнішні системи – будь то CRM, платформи Інтернету речей чи мобільні додатки – споживають контекст через токеновані канали доступу з керованими дозволами, забезпечуючи гнучкість та безпеку інтеграції.

Метрики якості досвіду (QoE)

Надання контексту не обмежується технічною точністю – воно досягає кульмінації у сприйнятті користувацького досвіду. Три показники якості обслуговування (QoE) оцінюють продуктивність:

- Затримка: Мілісекунди визначають релевантність. Системи, оптимізовані для периферійних обчислень та попередньої вибірки на основі CDN, досягають часу доставки менше 50 мс для критичного контексту, такого як обробка переривань в автомобільних системах.

- Точність персоналізації: Вимірювана за показниками релевантності протягом сеансів користувачів, точність вище 85% у рекомендаціях або адаптації інтерфейсу користувача свідчить про надійне моделювання контексту.

- Рівень залученості користувачів: Очевидний вплив надання контексту надалі. Платформи зі зрілими контекстними фреймворками повідомляють про в 3–6 разів більшу тривалість сеансу та до 4-кратне збільшення щільності взаємодії порівняно із системами статичного контенту.

Збільшення бізнес-цінності за допомогою архітектури доставки контексту**Посилення залученості завдяки точному визначенню часу**

Загальне спілкування не привертає уваги. Архітектура доставки контексту усуває цю проблему, синхронізуючи контент з намірами, поведінкою та середовищем користувача. Аналізуючи сигнали в режимі реального часу, такі як місцезнаходження, тип пристрою, історичні взаємодії та навіть умови навколишнього середовища, система вибирає найрелевантніше повідомлення щомиті.

Цей підхід є основою для персоналізації кампаній у режимі реального часу. Користувач, який отримує push-сповіщення під час активного перегляду пов'язаного контенту, реагує набагато швидше, ніж той, кого переривають під час простою. Компанії, які використовують цю точність часу, повідомляють про покращення показників залученості. Наприклад, Gartner зазначив, що високоцільовий контекстний маркетинг може підвищити рівень відповідей до 20% порівняно зі статичними кампаніями.

Оптимізація рентабельності інвестицій за допомогою інтелектуального розподілу ресурсів

Контекстно-залежні системи доставки автоматизують значну частину процесу прийняття рішень, який раніше вимагав ручного налаштування та контролю. Замість впровадження універсальних стратегій, компанії можуть налаштовувати інтелектуальні потоки, які автоматично коригують контент, час та канал доставки на основі даних у реальному часі.

Це зменшує зайві зусилля, знижує вартість взаємодії з кожним клієнтом та покращує використання ресурсів. Наприклад:

- Маркетингові команди виграють від меншої кількості ітерацій контенту, водночас досягаючи вищих конверсій.
- Відділи продажів отримують ліди, сегментовані за намірами, що зменшує зусилля на холодний контакт.
- Інженерні команди уникають жорстко запрограмованої логіки персоналізації, зосереджуючись натомість на основних завданнях розробки.

За даними McKinsey, компанії, які застосовують передові стратегії персоналізації, що підтримуються контекстними технологіями, спостерігають зростання доходів на 5–15% та підвищення ефективності маркетингових витрат на 10–30%.

Збільшення утримання клієнтів завдяки гіперперсоналізованому досвіду

Коли інтерфейси відповідають контексту користувача – передбачаючи потреби, адаптуючи потік контенту та відображаючи поведінку користувача – залученість застосунку зростає. Клієнти залишаються довше, частіше взаємодіють та демонструють вищий рівень задоволеності.

Персоналізація на основі контекстної доставки також зменшує відтік користувачів. Стрімінгові платформи, що адаптують рекомендації до певних настроїв та умов перегляду, або фітнес-додатки, що змінюють пропозиції залежно від часу доби та нещодавньої активності, змушують користувачів повертатися.

На практиці це безпосередньо впливає на кінцевий результат. Adobe повідомляє, що компанії, які використовують розширену персоналізацію на основі контексту, спостерігають збільшення цінності життя клієнта (CLV) у 1,7 раза.

Варіанти використання, розкриті завдяки наданню контексту

Контекстна архітектура не обмежується теорією. Вона проявляється у відчутних бізнес-функціях у різних відділах:

- Маркетингова автоматизація: тригерні електронні листи та повідомлення реагують на поведінку користувачів у режимі реального часу – залишення кошика, паузи в перегляді або сплески інтересу. Контент розвивається з кожною взаємодією, щоб відображати, на якому етапі своєї подорожі знаходиться користувач.
- Оптимізація підтримки клієнтів: Чат-боти підтримки, наповнені контекстними сигналами, можуть випереджати запитання, посилаючись на нещодавні дії, характеристики

пристроїв або моделі використання послуг. Це скорочує час вирішення проблем і підвищує показники задоволеності клієнтів.

Реальні впровадження демонструють стабільні результати. Компанії, які використовують контекст для керування взаємодією зі службою підтримки, скоротили середній час обробки на 30–40% та покращили показники вирішення проблем з першого контакту більш ніж на 20%.

Балансування точності та захисту: безпека, конфіденційність та управління етичним контекстом

Конфіденційність за проектом у контекстній наданні

Кожен рівень архітектури доставки контексту – збір даних, обробка, виведення та доставка – повинен вбудовувати засоби контролю конфіденційності з самого початку. Конфіденційність за принципом проектування (PbD) виходить за рамки дотримання вимог; вона інтегрує механізми конфіденційності в операційну логіку систем. Це означає, що конфіденційні вхідні дані ніколи не торкаються незахищеного сховища, контекстні висновки залишаються в межах визначених меж, а всі процеси за замовчуванням дотримуються принципу мінімального розкриття.

Підхід PbD вимагає проактивної, а не реактивної інженерії. Наприклад, моделі персоналізації на основі контексту повинні анонімізувати точки даних під час їх отримання, а не після нього. Вони також повинні створювати системні бар'єри, що запобігають надмірному контекстуалізму, коли системи роблять висновки, що виходять за рамки очікувань або корисності користувача.

Згода користувачів, мінімізація даних та прозорість політики

В архітектурі контекстної доставки дані не просто чекають на запит – вони динамічно передаються, узгоджуючи їх із шаблонами використання, просторовими умовами та поведінкою користувачів у режимі реального часу. Цей потік має ґрунтуватися на чіткій та відкличній згоді користувача.

- Явні дозволи замінюють приховані прапорці; користувачі повинні розуміти, що вони дозволяють.

- Мінімізація даних означає збір лише інформації, що відповідає конкретному випадку використання. Якщо сервіс не потребує детальної геолокації, він не повинен мати до неї доступу.

- Чітко опубліковані політики, структуровані доступною мовою та підкріплені машинозчитуваними форматами, гарантують, що як люди, так і агенти штучного інтелекту дотримуються умов договорів використання.

Ця модель створює цифровий контракт, який є дієвим, відстежуваним та таким, що може бути виконаний, що є ключовим для масштабування контекстно-залежних послуг у різних юрисдикціях та екосистемах.

Забезпечення контексту на кожній точці взаємодії

Контекстні дані не є статичними. Вони швидко передаються між рівнями – датчиками, посередниками, сервісами, механізмами прийняття рішень. Це робить їх захист на кожному етапі невід'ємним.

Шифрування на периферії має застосовуватися якомога ближче до джерела. Дані датчиків та сигнали користувача повинні бути зашифровані перед тим, як залишити пристрій, за допомогою стандартизованих бібліотек та захищених ключів. Це запобігає атакам типу «людина посередині» та не дозволяє платформам перехоплювати необроблений контекст.

Далі, моделі безпечного федеративного навчання дозволяють системам покращувати свої можливості контекстного виведення без агрегації персональних даних у централізовані бази даних. Замість надсилання даних до моделі, модель безпечно передається до даних, навчається локально та повертає лише зашифровані статистичні оновлення.

Автентифікація та довіра в екосистемах багатьох пристроїв

Один користувач може взаємодіяти з десятком пристроїв протягом 24 годин – телефонами, годинниками, терміналами, розумними колонками, транспортними засобами. Ці кінцеві точки повинні координувати свою роботу, не порушуючи меж довіри.

– Безперервна автентифікація особи за допомогою мультимодальної біометрії гарантує, що контекст відповідає фактичному користувачеві, а не лише пристрою.

– Оцінка довіри між пристроями визначає, чи може вторинний пристрій отримувати доступ до контексту з первинного вузла, запобігаючи перевантаженню з менш захищених кінцевих точок.

– Принципи архітектури нульової довіри вимагають, щоб кожен запит або обмін даними був автентифікований, перевірений та зареєстрований, незалежно від зв'язку джерела з мережею.

Разом ці механізми створюють стійку структуру довіри, гарантуючи, що доставка контексту залишається узгодженою з ідентифікатором користувача, правами доступу та рівнем безпеки, незалежно від того, наскільки гнучкою стає екосистема.

Об'єднання інтелекту, досвіду та інфраструктури

Архітектура доставки контексту (CoDA) – це не теоретична основа, що збирає цифровий пил, а операційна парадигма, яка диктує, як поведуться чутливі, релевантні та прогнозні цифрові системи. Кожен компонент, від датчиків, розгорнутих на периферії, до хмарних аналітичних механізмів, відповідає одній директиві: надавати точну, персоналізовану інформацію потрібному користувачеві за правильних умов.

Цей фреймворк процвітає завдяки поєднанню технологій, які вже вплетені в цифрову тканину – машинного навчання, обробки даних у реальному часі, CDN, адаптивних фреймворків інтерфейсу користувача та платформ оркестрації. Зі зближенням цих рівнів вони генерують більше, ніж просто підвищення продуктивності. Вони відкривають можливості, орієнтовані на аудиторію, де програми не чекають дій користувачів; вони передбачають та реагують динамічно, формуючись часом, місцем розташування, поведінкою та уподобаннями.

Подивіться, як адаптивний UX-дизайн сьогодні не спирається виключно на естетику інтерфейсу – він зчитує сигнали. Маршрутизація контекстних сигналів, таргетування збагаченого контенту та ідіоматичне моделювання поведінки стали міркуваннями дизайну, а не лише механізмами бекенду. Цей зсув відображає суть CoDA: об'єднання архітектури, інтерфейсу та обчислень у безшовний, інтелектуальний досвід.

Розгортання плану

– Виберіть одну сферу – охорона здоров'я, роздрібна торгівля, фінанси. Зробіть карту, як контекст може покращити шляхи доставки або переосмислити точки дотику.

– Проведіть опитування зацікавлених сторін щодо прогалин у точках контакту та неефективності. Де сьогодні ігнорується контекст?

– Визначте, де поточні конвеєри (від оркестрації API до пристрою користувача) розривають ланцюг між станом користувача та поведінкою програми.

– Прототипні сценарії, де система реагує на виведений контекст, а не на статичні вхідні дані чи підказки користувача.

Ви вже бачили функцію, яка змінювалася залежно від вашого місцезнаходження або нещодавнього шаблону використання? Це була взаємодія дизайну, архітектури та даних. Розбийте це – які системи це забезпечили? Кому належать ці контекстні моделі?

Вивчення реальних архітектур – не лише кодових баз, а й потоків доступу, карт затримки та ієрархій сигналів – пропонує більше розуміння, ніж статичні офіційні документи. CoDA переживає шаблони розгортання та спостережувані зміни у поведінці використання. Затримайтеся в цьому просторі, і системи, готові до майбутнього, не залишаться абстрактними ідеями, а операційними активами, готовими до впливу у великих масштабах.

Безпека продукту

CoDA пропонує функції безпеки продуктів корпоративного рівня для більшого контролю, прозорості та гнучкості:

- Автентифікація: CoDA пропонує широкий спектр методів автентифікації, таких як SSO з SAML 2.0, вхід за допомогою Google, Microsoft, Apple, Magic Links та базова автентифікація з 2-факторною автентифікацією. Корпоративні клієнти можуть встановлювати політики автентифікації та керувати користувачами за допомогою SCIM.

- Шифрування: Дані клієнтів шифруються під час передачі та зберігання за замовчуванням.

- Авторизація: керування доступом до документів, папок, пакетів та робочих просторів. Спільний доступ із групами Google. Корпоративні клієнти також можуть ділитися файлами з групами SCIM та встановлювати розширені правила спільного доступу для форм, документів та пакетів.

- Аудит: Ми надаємо API аудиту для корпоративних клієнтів, щоб отримувати журнали аудиту за останні 12 місяців. CoDA також надає пакет адміністратора для перегляду подій аудиту.

- Політики підприємства: підприємства можуть встановлювати політики для керування користувачами, документами та пакетами. До них належать політики для автентифікації користувачів, зовнішнього та вхідного спільного доступу, публікації, створення спільних папок, експорту даних, завантаження файлів та тривалості сеансу.

- Панелі керування Enterprise: CoDA пропонує корпоративним клієнтам розширені адміністративні панелі керування для легкого керування їхніми робочими процесами в CoDA. До них належать панелі керування для перегляду та керування ліцензіями, загальнодоступними документами, активністю користувачів та документами, що належать користувачам з деініціалізацією.

- Конфігурації та схвалення пакетів: CoDA пропонує високорозвинені засоби контролю безпеки для інтеграцій сторонніх розробників. Підприємства мають повний контроль над тим, які дані можна вносити до CoDA, хто може їх вносити та хто може до них отримувати доступ.

Безпека застосунків

Зобов'язання CoDA щодо безпеки починаються з процесів, інструментів та практик для безперервного проектування та розробки безпечного програмного забезпечення:

- Життєвий цикл розробки безпеки: Наша програма життєвого циклу розробки безпеки інтегрована в кожен етап процесу розробки програмного забезпечення для безперервного створення безпечного програмного забезпечення. Прикладами є щорічні тренінги з безпеки для всіх співробітників, моделювання загроз як частина процесу проектування та інструменти статичного аналізу коду.

- Щорічне тестування на проникнення: CoDA проводить щорічне тестування на проникнення, яке проводять авторитетні дослідницькі фірми з безпеки. Сфера цього тестування включає: веб-застосунки, інфраструктуру пакетів CoDA, хмарну інфраструктуру та мобільні застосунки.

- Програма публічної винагороди за виявлені помилки: CoDA запускає публічну програму винагороди за виявлені помилки через HackerOne.

Безпека інфраструктури

CoDA створена з нуля з використанням найкращих практик безпеки AWS:

- Хмарна інфраструктура: CoDA побудована з використанням усталених принципів безпеки, включаючи глибоко ешелонований захист, мінімальні привілеї та зменшення площі поверхні атаки. CoDA дотримується найкращих практик AWS щодо мережевої безпеки, використовуючи такі сервіси, як AWS CloudFront, AWS WAF, групи безпеки AWS та VPC.

- Безпека операцій: Ми використовуємо багатофакторну автентифікацію, контроль доступу на основі ролей (RBAC) та гранти доступу «точно вчасно» для безпечного

керування нашим сервісом. Крім того, ми реєструємо події аудиту та інформацію про безпеку на кожному рівні нашої інфраструктури та відстежуємо їх на наявність підозрілої активності.

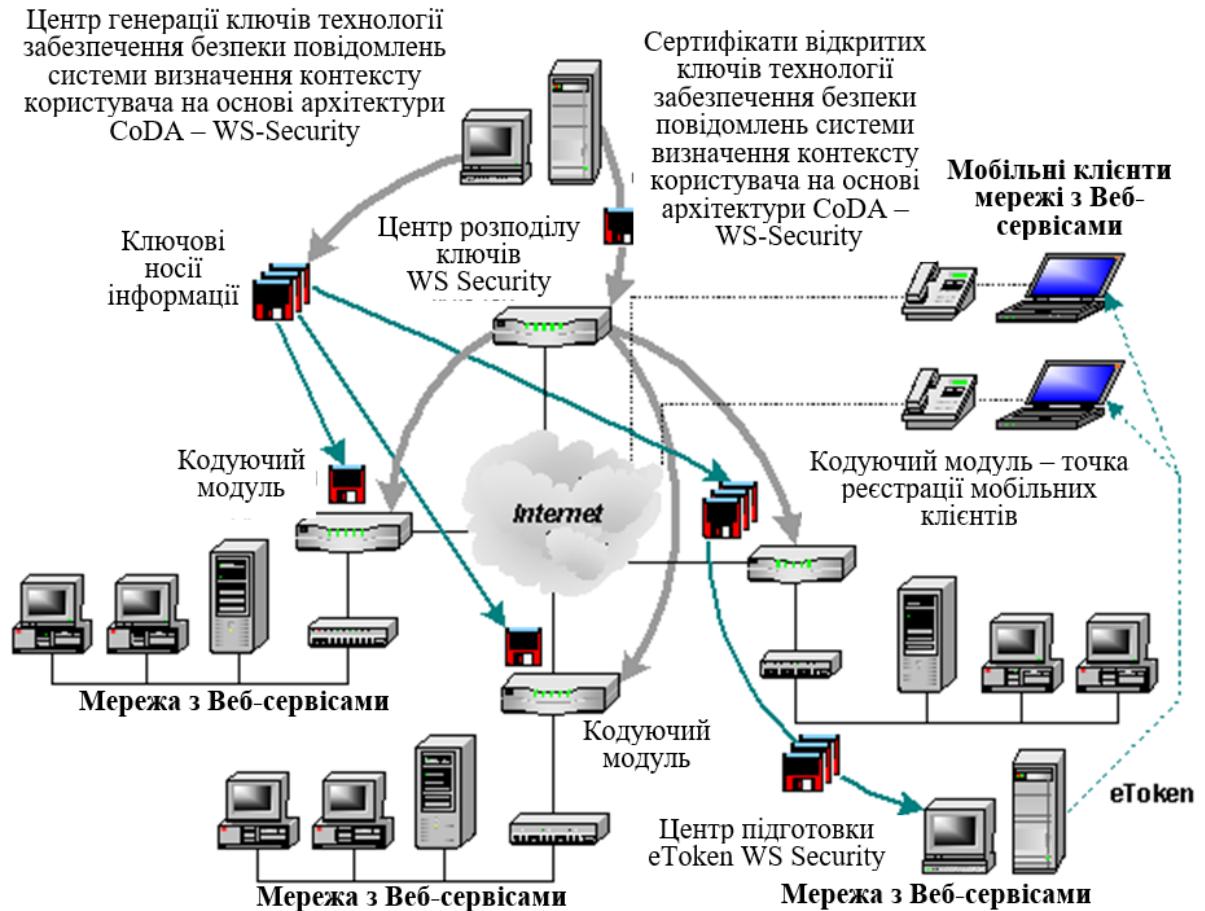


Рисунок 1 – Структурна схема системи

– Резервні копії: CoDA щодня створює резервні копії баз даних для всіх даних, що зберігаються в AWS. Резервні копії зазвичай зберігаються щонайменше 35 днів. Ми також проводимо регулярні перевірки цілісності резервних копій та проводимо навчання з аварійного відновлення на робочому столі щонайменше раз на рік.

– Синхронізація годинника: інформаційні ресурси CoDA використовують протокол NTP для синхронізації із затвердженими джерелами NTP.

– Безпека пакетів: пакети виконуються в ізольованих захищених пісочницях. Розробник пакетів ніколи не торкається облікових даних авторизації, які використовуються користувачами в пакетах. Ми гарантуємо, що пакети обмінюються даними лише з тими веб-сайтами, про які вони заявляють.

– Шифрування: CoDA використовує службу керування ключами Amazon (KMS) для створення, обслуговування та ротації ключів шифрування. CoDA також використовує протокол Transport Layer Security (TLS 1.2) для шифрування даних користувачів під час передачі та симетричний алгоритм шифрування AES-256 для шифрування даних клієнтів у стані спокою.

Склад Комплексу

Комплекс складається з наступних компонентів:

1. Набір шлюзів кодування.
2. Центр генерації ключів.
3. Центр розподілу ключів.
4. Центр реєстрації мобільних клієнтів.

5. Центр підготовки електронних ключів мобільних клієнтів.
6. Мобільний клієнт.
7. Центр моніторингу.
8. Програма контролю цілісності.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів визначення контексту користувача на основі архітектури CoDA. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем визначення контексту користувача на основі архітектури CoDA.
- Досліджена система визначення контексту користувача на основі архітектури CoDA.
- На основі отриманих результатів досліджень створена програмна реалізація системи визначення контексту користувача на основі архітектури CoDA.

Розроблені алгоритми дозволяють успішно вирішувати завдання визначення контексту користувача на основі архітектури CoDA. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Kuznetsov, O., Smirnov, O., Akhmetov, B., Alimseitova, Z., Imoize, A.L. «Deep Learning Frontiers in Copy-Move Forgery Detection: Advances, Challenges, and Future Directions». *Advancements in Cybersecurity Next Generation Systems and Applications*, 2025. 202-229.
2. Вінтенко Б., Смірнов О., Миронець І., Смірнова Т., Смірнов С. «Імітаційна модель шляхів вхідних даних комп'ютерної інтелектуальної системи підтримки оператора енергоблоку АЕС». Комбінаторні конфігурації та їхні застосування: Матеріали XXVII Міжнародного науково-практичного семінару, присвяченого 125-річчю Національного університету «Запорізька політехніка» (Запоріжжя-Кропивницький-Київ, 4-6 червня 2025 р.). Запоріжжя: НУ «Запорізька політехніка», 2025. С.82-91.
3. Al-Azzeh, J., Ayyoub, B., Mesleh, A., Smirnova, T., Gnatyuk, S., Drieiev, O., Smirnov, O., Dorenskyi, O. «Cloud-Based Information System for Evaluating Caverns in the Process of Blasting Metal Surfaces of Details». *International Review on Modelling and Simulations* 18 (1), 2025. pp. 32-42.
4. Вінтенко Б.Ю., Смірнов О.А., Миронець І.В., Смірнова Т.В., Коваленко О.В., Мацуй А.М. «Модель шляхів отримання вхідних даних комп'ютерної інтелектуальної системи підтримки оперативного персоналу АЕС». *Центральноукраїнський науковий вісник. Технічні науки*. 2025. Вип. 11(42), ч. II. С.52-62.
5. Вінтенко Б.Ю., Смірнов О.А., Миронець І.В., Смірнова Т.В. «Методи забезпечення відмовостійкості інтелектуальних систем підтримки оператора». VIII міжнародна науково-практична конференція «Інформаційна безпека та комп'ютерні технології», м. Кропивницький. 24-25 квітня 2025 р. – Кропивницький: ЦНТУ. – 2025. – С. 44-46.
6. Смірнов, О.А., Константинова, Л.В., Коноплицька-Слободенюк, О.К., Козірова, Н.В., Якименко, Н.М., Доренський, О.П., Буравченко, К.О. «Дослідження інструментів штучного інтелекту для роботи з базами даних та аналізу даних». *Кібербезпека: освіта, наука, техніка*. 2025. №3(27), С. 429–448.
7. Lakhno, V., Malyukov, V., Smirnov, O., Bebesko, B., Chubaievskiy, V., Zhumadilova, M., Malyukova, I., Smirnov, S. «Multifactorial Model for Targeted Attacks Counteracting Within the Framework of a Multi-Step Quality Game with Fuzzy Information». *8th International Symposium on Intelligent Informatics, ISI 2023*, 2025. vol 389. pp 377-389. Springer, Singapore.
8. Smirnov O., Fedorov E., Neskrodieva A., Neskrodieva T. «Intellectual Classification method of Gymnastic Elements Based on Combinations of Descriptive and Generative Approache». *CEUR Workshop Proceedings Volume 3664*, 2024, Pages 11-23.
9. Kuznetsov, O., Kryvinska, N., Ilchenko, O., Smirnova, T., Ulianovska, Y. «Comparative Analysis of Cryptocurrency Trading Platforms Using the Analytic Hierarchy Process». *CEUR Workshop Proceedings*, 2023, 3628, pp. 106-115.
10. Malyukov V., Bebesko B., Lakhno V., Smirnov O., Malyukova I., Mohylnyi H. «Managing the Purchase-Sale Process of Digital Currencies Under Fuzzy Conditions». *Lecture Notes in Networks and Systems*, 2023, 729 LNNS, pp. 104–112.
11. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». *Advanced Information Systems*, 2023, 7(2), pp. 49-56.
12. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchey, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». *CEUR Workshop Proceedings, Volume 3530*, 2023, pp. 256-265.

13. Аль-Мудхафар Акіл Абдулхуссейн М., Смірнова Т.В., Буравченко К.О., Смірнов О.А. «Метод оцінки та підвищення користувальницького досвіду абонентів в програмно-конфігурованих мережах на основі використання машинного навчання». Сучасні інформаційні системи, 2023, том 7, № 2, С. 49-56.
14. Smirnov, O., Karapetyan, A., Fedorov, E., «Creating Neural Network and Single Solution Human-Based Metaheuristic Methods of Solving the Traveling Salesman Problem». CEUR Workshop Proceedings, Volume 3312, 2022, pp. 47-58.
15. Smirnov, O., Neskrodieva, T., Fedorov, E., Rudakov, K., Neskrodieva, A. «Method Detection Audit Data Anomalies on Basis Restricted Cauchy Machine» CEUR Workshop Proceedings, Volume 3187, 2022, pp. 1-12.
16. Smirnov O., Smirnova T., Anas M. Al-Oraiqat, Drieiev O., Polishchuk L., Sheraz Khan, Yassin M. Y. Hasan, Aladdein M. Amro, Hazim S. AlRawashdeh «Method for Determining Treated Metal Surface Quality Using Computer Vision Technology». Sensors (Basel, Switzerland) Volume 22, Issue 16, 6223, 2022.
17. Smirnov, O., Lakhno, V., Akhmetov, B., Chubaievskiy, V., Khorolska, K., Bebesko, B. «Selection of a Rational Composition of Information Protection Means Using a Genetic Algorithm». In: Rajakumar, G., Du, K.L., Vuppapapati, C., Beligiannis, G.N. (eds) Intelligent Communication Technologies and Virtual Mobile Networks. Lecture Notes on Data Engineering and Communications Technologies, vol 131. 2023. Springer, Singapore. pp. 21-34.
18. Kuznetsov, A., Oleshko, I., Chernov, K., Bagmut, M., Smirnova, T. «Biometric authentication using convolutional neural networks». Lecture Notes in Networks and Systems. Volume 152, 2021, Pages 85-98.
19. Smirnov O., Kuznetsov A., Kryvinska N., Kiian A., Kuznetsova K. «Full Non-Binary Constant-Weight Codes». SN Computer Science, Vol 2, 337, 2021. <https://doi.org/10.1007/s42979-021-00739-w>.
20. Smirnov O., Neskrodieva T., Fedorov E., Rymar P. «Neural Network Modeling Method of Transformations Data of Audit Production with Returnable Waste». CEUR Workshop Proceedings Volume 3101, 2021, Pages 192-207.
21. Smirnov, O., Kuznetsov, A., Potii, O., Poluyanenko, N., Stelnyk, I., Mialkovsky, D. «Combining and filtering functions in the framework of nonlinear-feedback shift register». International Journal of Computing; 2020, Volume 19, Issue 2 – Research Institute for Intelligent Computer Systems – 2020. – P. 247-256.
22. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
23. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177.
24. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587.
25. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». CEUR Workshop Proceedings Volume 2616, 2020, Pages 366-379.
26. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645.
27. Smirnov O. Kuznetsov A., Zaichenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019; Odessa; Ukraine; 9-13 September 2019. P.22-28.
28. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.
29. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019 . P.517-522.
30. Smirnov, O., Ulichev, O., Meleshko, Y., Khokh, V., Goncharenko, I. «Method of Choosing Objects for Informational Influence in Social Networks during Information Campaign Based on the Analytic Hierarchy Process». CEUR Workshop Proceedings, Vol 2588, P. 215-227, 2019.
31. Smirnov, O., Krasnobayev, V., Yanko, A., Kuznetsova, T. «Methods of nulling numbers in the system of residual classes». CEUR Workshop Proceedings, Vol 2588, P. 90-106, 2019.
32. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Averchev, A., Pastukhov, M., Kuznetsova, K., «Formation of Pseudorandom Sequences with Special Correlation Properties», 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT -2019/ Lviv, Ukraine, 2-6 July, 2019, P. 395-399.
33. Smirnov, O., Kuznetsov, A., Kiian, A., Zamula, A., Rudenko, S., Hryhorenko, V., «Variance Analysis of Networks Traffic for Intrusion Detection in Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 353-358.
34. Smirnov, O., Kuznetsov, A., Kavun, S., Babenko, B., Nakisko, O., Kuznetsova, K., «Malware Correlation Monitoring in Computer Networks of Promising Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 347-352.

УДК 004

Б.Турик, магістр гр. КІ-24М,*Центральноукраїнський національний технічний університет*

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ВІРТУАЛІЗАЦІЇ МЕРЕЖІ NUAGE NETWORKS

У статті розроблено програмне забезпечення, яке призначено для системи віртуалізації мережі Nuage Networks. Метою розробки є дослідження та принципи побудови системи віртуалізації мережі Nuage Networks. Об'єктом дослідження є процес віртуалізації мережі Nuage Networks. Предметом дослідження є методи віртуалізації мережі Nuage Networks. Методи дослідження базуються на методах теорії побудови комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи віртуалізації мережі Nuage Networks. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

віртуалізація мережі, Nuage Networks

Постановка проблеми. Віртуалізація мережі – це процес створення віртуальної версії мережі, включаючи апаратні та програмні компоненти. Вона дозволяє користувачам створювати, розгортати та керувати мережами у віртуальному середовищі.

Віртуалізацію мережі можна використовувати для різних цілей, включаючи тестування нових мережевих проєктів, моделювання різних мережевих середовищ та навчання співробітників новим мережевим технологіям.

Це також дозволяє мережевим адміністраторам ефективніше керувати кількома мережами, зменшуючи витрати та підвищуючи ефективність. Крім того, віртуалізацію можна використовувати для покращення масштабованості, доступності та безпеки мережі.

Віртуалізація – це технологія, яка дозволяє кільком віртуальним серверам працювати на одному фізичному сервері, що максимізує використання ресурсів та гнучкість, дозволяючи створювати ізольовані віртуальні середовища, що підвищує безпеку та спрощує розгортання та управління програмами.

Хмарні обчислення – це технологія, яка дозволяє користувачам отримувати доступ до даних, програм та обчислювальних ресурсів через Інтернет. Замість того, щоб покладатися на фізичні сервери чи обладнання, хмарні обчислення спираються на мережу віддалених серверів, розміщених в Інтернеті.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи віртуалізації мережі Nuage Networks.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи віртуалізації мережі Nuage Networks.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем віртуалізації мережі Nuage Networks.
- Дослідження системи віртуалізації мережі Nuage Networks.
- Програмна реалізація системи віртуалізації мережі Nuage Networks.

Об'єктом дослідження є процес віртуалізації мережі Nuage Networks.

Предметом дослідження є методи віртуалізації мережі Nuage Networks.

Методи дослідження базуються на методах теорії побудови комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Віртуалізація – це ключова технологія хмарних обчислень, яка дозволяє запускати кілька віртуальних машин (ВМ) на одній фізичній машині, що дозволяє краще використовувати доступні ресурси. Це дає організаціям змогу знизити витрати, підвищити ефективність та покращити гнучкість. Крім того, це забезпечує кращу масштабованість та можливість швидко видавати нові ресурси за потреби.

Огляд технологій віртуалізації та їх ключових компонентів

Існує кілька типів технологій віртуалізації, включаючи віртуалізацію серверів, віртуалізацію робочих столів, віртуалізацію сховищ даних, віртуалізацію програм та віртуалізацію мережі. Ключові компоненти віртуалізації включають гіпервізор, який відповідає за керування та розподіл апаратних ресурсів між віртуальними машинами, віртуальну машину, яка є програмним представленням фізичної машини, та програмне забезпечення для керування віртуалізацією, яке надає інструменти для керування віртуальними машинами та моніторингу їх.

Переваги віртуалізації в традиційних обчислювальних середовищах

Однією з найважливіших переваг віртуалізації є можливість максимального використання апаратних ресурсів. Запускаючи кілька віртуальних машин (ВМ) на одному фізичному сервері, організації можуть зменшити витрати на обладнання та підвищити свою ефективність. Крім того, віртуалізація спрощує управління ресурсами, включаючи можливість розподіляти та перерозподіляти ресурси за потреби. Це може призвести до швидшого впровадження нових послуг і програм, а також до ефективнішого використання існуючої інфраструктури.

Роль віртуалізації в хмарних обчисленнях

Віртуалізація – це основна технологія, яка забезпечує роботу хмарної інфраструктури. Вона дозволяє кільком віртуальним машинам працювати на одному фізичному сервері, що максимізує використання обладнання та знижує витрати. Крім того, віртуалізація забезпечує ізоляцію між віртуальними машинами, гарантуючи, що одна віртуальна машина не заважатиме іншій. Це підвищує безпеку та дозволяє робочим навантаженням з різними вимогами співіснувати на одному фізичному сервері.

Як віртуалізація забезпечує ефективне використання ресурсів у хмарі?

Кожна віртуальна машина працює незалежно, з власною операційною системою та програмами, і ізольована від інших віртуальних машин. Це забезпечує гнучкість, масштабованість та економічну ефективність для хмарних обчислень. Крім того, віртуалізація дозволяє легко мігрувати віртуальні машини між фізичними серверами, що дозволяє динамічно розподіляти ресурси та балансувати навантаження.

Масштабованість та еластичність, досягнуті завдяки віртуалізації в хмарі

Еластичність забезпечує автоматичне масштабування ресурсів відповідно до робочого навантаження, оптимізуючи ефективність та знижуючи витрати. Ці переваги дозволяють створювати кілька віртуальних машин на одному фізичному сервері. Це дозволяє компаніям адаптуватися до змінних потреб та максимізувати рентабельність інвестицій.

Віртуальні машини в хмарних середовищах

У хмарних обчисленнях віртуальні машини є важливими, оскільки вони забезпечують гнучку та масштабовану інфраструктуру для економічно ефективного запуску програм. Віртуальні машини також дозволяють легко мігрувати програми між різними хмарними постачальниками в багатохмарних середовищах, що полегшує для компаній вибір найкращого хмарного рішення для їхніх потреб. Загалом, виділення ресурсів та керовані хмари революціонізують обчислювальний підхід.

Віртуальні машини стали популярною технологією, що дозволяє легко масштабувати віртуальні машини завдяки швидкому розгортанню та налаштуванню змінних вимог. Вони забезпечують високий рівень ізоляції між різними програмами та користувачами на одному фізичному сервері, підвищуючи безпеку та зменшуючи ризик витоку даних.

Віртуальні машини дозволяють користувачам запускати кілька операційних систем на одному фізичному сервері, що підвищує гнучкість та ефективність. Крім того, віртуальні машини сприяють аварійному відновленню та забезпеченню безперервності бізнесу, дозволяючи легко створювати резервні копії та відновлювати віртуальні машини. Загалом, використання віртуальних машин у хмарних обчисленнях може сприяти економії коштів, підвищенню продуктивності та підвищенню безпеки.

Гіпервізори: ключові фактори віртуалізації в хмарі

Гіпервізори – це програмне забезпечення, яке дозволяє створювати та керувати віртуальними машинами у віртуалізаційних та хмарних середовищах. Основне призначення гіпервізорів – дозволити кільком віртуальним машинам працювати на одній фізичній машині, кожна з яких має власну операційну систему та програми. Центри обробки даних та хмарні обчислення використовують гіпервізори для оптимізації використання ресурсів та спрощення управління та масштабування ІТ-інфраструктури.

Існує два основних типи гіпервізорів: Тип 1 та Тип 2. Гіпервізори *Типу 1* працюють безпосередньо на обладнанні хоста, а віртуальні машини працюють поверх них. Вони також відомі як гіпервізори без вбудованого обладнання. Гіпервізори *Типу 2*, навпаки, працюють поверх операційної системи, а віртуальні машини працюють поверх них. Вони також відомі як розміщені гіпервізори.

Тип 1 зазвичай використовується в корпоративних середовищах для віртуалізації серверів. Прикладами гіпервізорів типу 1 є VMware ESXi, Microsoft Hyper-V та Citrix Hypervisor.

Гіпервізори типу 2 зазвичай використовуються для віртуалізації робочих столів. Прикладами гіпервізорів типу 2 є Oracle VirtualBox, VMware Workstation та Parallels Desktop.

Як гіпервізори забезпечують ефективне управління та розподіл ресурсів у хмарі?

Гіпервізори забезпечують ефективне керування ресурсами та розподіл ресурсів у хмарі. Це означає, що кілька користувачів або програм можуть працювати на одному фізичному сервері, не заважаючи один одному, що призводить до кращого використання ресурсів та економії коштів. Загалом, гіпервізори є важливим компонентом хмарної інфраструктури, що дозволяє ефективно керувати ресурсами та розподіляти їх для задоволення потреб різних користувачів та робочих навантажень.

Вплив віртуалізації на гнучкість та спритність хмарних технологій

Віртуалізація в хмарі забезпечує кілька переваг гнучкості:

- Це дозволяє швидко виділяти ресурси, дозволяючи організаціям швидко реагувати на змінні потреби бізнесу.
- Це спрощує створення та розгортання нових програм, оскільки розробники можуть легко створювати нові середовища для тестування та ітерації свого коду.
- Це забезпечує мобільність робочого навантаження, переміщуючи програми між різними хмарними провайдерами або навіть між локальними та хмарними середовищами.

Гнучкість у розгортанні та міграції робочих навантажень завдяки віртуалізації

Технологія віртуалізації забезпечує гнучкість у розгортанні та міграції робочих навантажень, легко переміщуючи робочі навантаження між фізичними серверами або навіть між центрами обробки даних, щоб збалансувати робочі навантаження та оптимізувати використання ресурсів. Крім того, віртуалізація дозволяє створювати віртуальні машини, які можуть запускати різні операційні системи та програми на одному фізичному сервері, підвищуючи гнучкість та зменшуючи витрати.

Віртуалізація дозволяє платформам електронної комерції масштабувати ресурси на вимогу, гарантуючи, що вони зможуть обробляти збільшений трафік і робоче навантаження. Це означає, що платформа може швидко виділяти додаткові ресурси, такі як процесор, пам'ять і сховище, без необхідності оновлення фізичного обладнання. В результаті платформа може обробляти більший обсяг транзакцій, покращуючи взаємодію з користувачем і зменшуючи ризик простоїв або збоїв.

Міркування безпеки у віртуалізованих хмарних середовищах

Віртуалізовані хмарні середовища стають дедалі популярнішими завдяки своїм численним перевагам, таким як масштабованість та економічна ефективність. Однак із цим зростанням використання виникають нові проблеми та вразливості. Однією з проблем є потенційна конкуренція за ресурси, коли кілька віртуальних машин конкурують за одні й ті ж ресурси, що призводить до проблем із продуктивністю.

Ще однією проблемою є підвищена складність середовища, що може ускладнити його керування та захист. Вразливості також можуть виникати через спільну інфраструктуру та потенційну можливість зловмисних атак на віртуальні машини. Організаціям необхідно впроваджувати політики розподілу ресурсів та застосовувати заходи безпеки.

Найкращі практики та заходи безпеки для забезпечення цілісності віртуалізованих ресурсів:

- Зрозумійте використання ресурсів.
- Автоматизуйте розподіл та оптимізацію ресурсів, щоб зменшити кількість людських помилок, підвищити ефективність та заощадити час і кошти.
- Впроваджуйте управління ресурсами та дотримання вимог, щоб забезпечити безпеку, цілісність та доступність ваших даних і програм.
- Моніторинг продуктивності та доступності ресурсів
- Вирішення проблем та інцидентів з вашими ресурсами
- Оптимізуйте свою стратегію управління та моніторингу ресурсів.

Майбутні тенденції та інновації у віртуалізації для хмарних обчислень

Інноваційні технології, такі як периферійні обчислення, контейнери, штучний інтелект (ШІ), машинне навчання (МН) та безсерверні обчислення, кардинально трансформують хмарні технології. Це значно покращило функціонування бізнесу, особливо завдяки тому, що підприємства навчилися тактовно та стратегічно використовувати хмарні можливості.

Поєднання віртуалізації, контейнерів та безсерверних обчислень може створити потужну екосистему для створення та запуску сучасних програм. Наприклад, контейнери можна використовувати для пакування та розгортання програм, тоді як віртуалізацію можна використовувати для керування базовою інфраструктурою та забезпечення ефективного використання ресурсів. Безсерверні обчислення можна використовувати для автоматичного забезпечення високогнучкого та економічно ефективного рішення.

Збільшення використання контейнерів, покращені функції безпеки, збільшення використання периферійних обчислень. Загалом, віртуалізація, ймовірно, залишатиметься фундаментальною технологією для хмарних обчислень у майбутньому, але її роль може змінюватися з появою нових технологій та варіантів використання.

Висновок

Віртуалізація – це ключова технологія хмарних обчислень, яка дозволяє запускати кілька віртуальних машин (ВМ) на одній фізичній машині, що дозволяє краще використовувати доступні ресурси. Це дає організаціям змогу знизити витрати, підвищити ефективність та покращити гнучкість. Віртуалізація також забезпечує ізоляцію між ВМ, гарантуючи, що одна ВМ не заважатиме іншій. Це підвищує безпеку та дозволяє робочим навантаженням з різними вимогами співіснувати на одному фізичному сервері.

З розвитком хмарних обчислень віртуалізація продовжуватиме відігравати важливу роль. Нові технології, такі як контейнери та безсерверні обчислення, поєднуються з віртуалізацією для створення потужної екосистеми для створення та запуску сучасних програм.

Продукти SDN та SD-WAN від Nuage Networks допомагають підприємствам та постачальникам послуг підвищити ефективність та знизити витрати, автоматизуючи хмарні операції та мережеві завдання.

Хмара обіцяє підвищити ефективність використання ІТ-ресурсів та гнучкість бізнесу, забезпечуючи більший ступінь автоматизації всіх ІТ-задач. Ця автоматизація дозволить гнучко налаштовувати мережеві та обчислювальні ресурси для оптимізації. Ви також зможете розгортати та масштабувати нові програми та послуги на вимогу.

Значна частина цієї автоматизації походить від нової програмно-визначеної інфраструктури, де програмне забезпечення для хмарної оркестрації пришвидшує процеси та зменшує вартість завдань, схильних до помилок у великих масштабах. Програмно-визначена інфраструктура спирається на віртуалізацію серверів і мереж, щоб усунути складність і допомогти досягти мобільності хмарного робочого навантаження та незалежності від розташування.

Nuage Networks допомагає створити програмно-визначені мережі (SDN) як основу для хмарних мереж та автоматизації на основі політик. Але на відміну від інших постачальників, вона використовує відкритий та нейтральний підхід до хмарної інфраструктури.

Nuage Networks об'єднує хмарні мережі, що працюють на будь-якій платформі, мережевому обладнанні, системі управління хмарию та хмарному провайдеру. Сумісність з платформами з відкритим кодом.

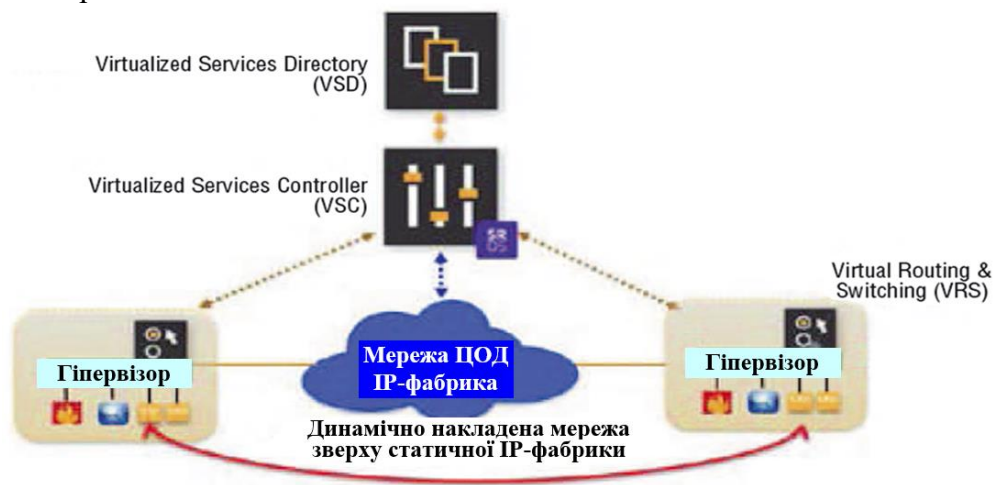


Рисунок 1 – Структурна схема системи

Nuage Networks – єдиний постачальник, який пропонує цю концепцію автоматизації на основі політик у центрі обробки даних, хмарі та глобальній мережі на одній платформі. Не потрібно кілька постачальників чи продуктів для управління хмарною автоматизацією. Продукти SDN дозволяють зменшити витрати на інфраструктуру та криві навчання, щоб ви могли реалізувати всі обіцянки хмари.

Платформа віртуалізованих сервісів

Платформа віртуалізованих сервісів (VSP) Nuage Networks – це комплексне рішення для автоматизації на основі політик. Це мережеве рішення включає компоненти, які можуть допомогти оптимізувати операції WAN, визначені центром обробки даних, хмарию або програмним забезпеченням, або автоматизувати політики безпеки та виправлення.

Рішення Nuage Networks Virtualized Services Platform (VSP) складається із трьох основних елементів:

- каталогу віртуалізованих сервісів (Virtualized Services Directory, VSD);
- агентів віртуальної маршрутизації/комутації (Virtual Routing & Switching, VRS);
- контролерів віртуалізованих сервісів (Virtualized Services Controller, VSC).

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів віртуалізації мережі Nuage Networks. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем віртуалізації мережі Nuage Networks.
- Досліджена система віртуалізації мережі Nuage Networks.

– На основі отриманих результатів досліджень створена програмна реалізація системи віртуалізації мережі Nuage Networks.

Розроблені алгоритми дозволяють успішно вирішувати завдання віртуалізації мережі Nuage Networks. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Smirnova, T., Gnatyuk, S., Yudin, O., Sydorenko, V., Polozhentsev, A., «The Model for Calculating the Quantitative Criteria for Assessing the Security Level of Information and Telecommunication Systems». CEUR Workshop Proceedings Volume 3156, 2022, Pages 390-399.
2. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». Проблеми інформатизації та управління, № 2(70). 2022. С. 28-37.
3. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 3(69). С. 93-98.
4. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Вісник Хмельницького національного університету. Серія: «Технічні науки», № 2 (307). С. 46-52. 2022.
5. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 1(67). С. 84-89.
6. Smirnova T., Gnatyuk S., Berdibayev R., Avkurova Zh., Iavich M. «Cloud-Based Cyber Incidents Response System and Software Tools». Communications in Computer and Information Science, 2021, vol 1486. Springer, Cham. pp 169-184.
7. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
8. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». Journal of theoretical and applied information technology Vol.98. No 21, 2020, P. 3334-3346.
9. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177.
10. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587.
11. Smirnov, O., Markovets, O. Vovk, N., Turchyn, Y., «Model of informational support for social network administrators' content creation». CEUR Workshop Proceedings Volume 2616, 2020, Pages 125-136.
12. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». CEUR Workshop Proceedings Volume 2616, 2020, Pages 366-379.
13. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645.
14. Smirnov O. Kuznetsov A., Zaichenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019; Odessa; Ukraine; 9-13 September 2019. P.22-28.
15. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.
16. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019 . P.517-522.
17. Smirnov, O., Odarchenko, R., Abakumova, A., Usik, P., Kundyzy, M., «QoE optimization technique for media

- delivery in 5G networks». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019. P.597-601.
18. Smirnov, O., Krasnobayev, V., Yanko, A., Kuznetsova, T. «Methods of nulling numbers in the system of residual classes». CEUR Workshop Proceedings, Vol 2588, P. 90-106, 2019.
19. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Averchev, A., Pastukhov, M., Kuznetsova, K., «Formation of Pseudorandom Sequences with Special Correlation Properties», 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT -2019/ Lviv, Ukraine, 2-6 July, 2019, P. 395-399.
20. Smirnov, O., Kuznetsov, A., Kiian, A., Zamula, A., Rudenko, S., Hryhorenko, V., «Variance Analysis of Networks Traffic for Intrusion Detection in Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 353-358.
21. Smirnov, O., Kuznetsov, A., Kavun, S., Babenko, B., Nakisko, O., Kuznetsova, K., «Malware Correlation Monitoring in Computer Networks of Promising Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 347-352.
22. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Pastukhov, M., Kuznetsova, K., Prokopovych-Tkachenko, D., «Discrete Signals with Special Correlation Properties», CEUR Workshop Proceedings Volume 2353, CEUR Workshop Proceedings 2019, Pages 618-629.
23. Smirnov A.A., Kuznetsov A.A., Danilenko D.A., Berezovsky A., «The statistical analysis of a network traffic for the intrusion detection and prevention systems», Telecommunications and Radio Engineering. – Volume 74, Issue 1. – Begel House Inc. – 2015. – P. 61-78.
24. Смірнов О.А., Смірнова Т.В., Буравченко К.О., Кравченко С.С., Горбов В.О., «Хмарна система підтримки прийняття рішень технологічного процесу відновлення поверхонь конструкцій і деталей машин». Сучасні інформаційні системи. 2021. Т. 5, № 4. С. 79-95
25. Смірнов О.А., Усік П.С., Миронець І.В., Буравченко К.О., Якименко Н.М. «Метод підвищення ефективності розподіленої обробки даних у комп'ютерних системах операторів стільникового зв'язку» Вісник Черкаського державного технологічного університету. Технічні науки. №4. С. 103-110. 2020.
26. О.А.Смірнов, Т.В.Смірнова, Л.І. Поліщук, К.О. Буравченко, А.О.Макевнін, «Дослідження хмарних технологій як сервісів», Кібербезпека: освіта, наука, техніка. № 3(7). С. 43-62. 2020.
27. Смірнов О.А., Коноплицька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Поліщук Л.І. Інформаційна безпека в комп'ютерних мережах. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2020. – 294 с.
28. О.А. Смірнов, П.С. Усік, «дослідження перспектив використання технологічних рішень в мережах 5g» у Кібербезпека та інформаційні технології: монографія. – Х. : ТОВ «ДІСА ПЛЮС», 2020.С. 122-135.
29. Смірнов О.А., Дреєва Г.М., Дреєв О.М., Смірнова Т.В. «Фрактальний аналіз генератора самоподібного трафіку на основі ланцюга Маркова». Центральнотрапійський науковий вісник. Технічні науки. № 2(33). с. 161-172, 2019.
30. Смірнов О.А., Коноплицька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В. Поліщук Л.І. Проектування комп'ютерних систем та мереж. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2019. – 264 с.
31. Smirnov, O., Kuznetsov, A., Kuznetsova, K. Synthesis of Discrete Signals with Improved Correlation Properties. Монографія: In.: ISCI'2019: Information Security in Critical Infrastructures. Collective monograph. Edited by Ivan D. Gorbenko and Alexandr A. Kuznetsov, ASC Academic Publishing, USA, 2019, pp. 281-299. – ISBN: 978-0-9989826-8-7 (Hardback), ISBN: 978-0-9989826-9-4 (Ebook).

УДК 004

С.Фоменко, магістр гр. КН-24М,

Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ПРОТИДІЇ ЗЛОВМИСНИМ ПРОГРАМАМ З ВИКОРИСТАННЯМ МЕТОДІВ МАШИННОГО НАВЧАННЯ

У статті розроблено програмне забезпечення, яке призначено для системи протидії зловмисним програмам з використанням методів машинного навчання. Метою розробки є дослідження та принципи побудови системи протидії зловмисним програмам з використанням методів машинного навчання. Об'єктом дослідження є процес протидії зловмисним програмам з використанням методів машинного навчання. Предметом дослідження є методи протидії зловмисним програмам з використанням методів машинного навчання. Методи дослідження базуються на методах машинного навчання, методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи протидії зловмисним програмам з використанням методів машинного навчання. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

протидія зловмисним програмам, машинне навчання

Постановка проблеми. Антивірусний бізнес зараз на підйомі. Тільки в 2025 році, за даними компанії Gartner, по усьому світі було продано програм безпеки на суму в 22 мільярда доларів. Однак скільки б засобів не витрачали підприємства й частки користувачі, стовідсоткового захисту не існує.

Особливо «улюбленим» у розроблювачів антивірусів підвидом шкідливого ПЗ є програми-здирилки. Усього за третій квартал минулого року було заблоковано 821 865 подібних атак на користувачів продуктів.

Жахає при цьому те, наскільки зловмисники успішні у своїй справі: за інформацією цієї компанії, через відсутність мер протидії кожна третя жертва перераховує хакерам викуп – однак 20 відсотків таких користувачів ніколи не одержать від здириликів код для дешифрування своїх даних. На кожному потерпілому злочинці заробляють у середньому близько 17 000 грн. – досить вигідний бізнес.

Щодня з'являються 300 000 нових видів шкідливого ПЗ – безперервна гра в кішки-мишки для антивірусів. Стандартними базами сигнатур з небезпекою впоратися практично неможливо. Тому сучасні захисні рішення роблять ставку на аналіз поведінки. У цьому випадку захисне ПЗ в реальному часі перевіряє, як поводить себе передбачуваний вірус на комп'ютері. При підозрілих зверненнях сканер блокує програму й повідомляє про це користувача.

Проблема: зловмисники розробляють методи для обходу евристики, наприклад, укриваючи своїх шантажистів у серйозних продуктах. Покласти кінець такому принципу дії здатні тільки зовсім нові техніки.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи протидії зловмисним програмам з використанням методів машинного навчання.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи протидії зловмисним програмам з використанням методів машинного навчання.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем протидії зловмисним програмам з використанням методів машинного навчання.
- Дослідження системи протидії зловмисним програмам з використанням методів машинного навчання.
- Програмна реалізація системи протидії зловмисним програмам з використанням методів машинного навчання.

Об'єктом дослідження є процес протидії зловмисним програмам з використанням методів машинного навчання.

Предметом дослідження є методи протидії зловмисним програмам з використанням методів машинного навчання.

Методи дослідження базуються на методах машинного навчання, методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Опишемо які технології повинна реалізовувати сучасна система протидії зловмисним програмам з використанням методів машинного навчання.

Система протидії зловмисним програмам з використанням методів машинного навчання є платформою безпеки, призначення якої – виявлення й відбиття різних погроз, включаючи погрози нульового дня, як на робочих станціях, так і в мережі за допомогою міжмережних екранів (Firepower) або ж засобами захисту контенту. Вона дозволяє безпосередньо виявляти шкідливі програми, проводити історичний аналіз файлових подій на робочій станції або ж у мережі, взаємодіяти з «пісочницею». Функціонал ретроспективного аналізу допомагає виявити шкідливе ПЗ, що змогло обійти традиційні механізми безпеки. Наприклад, система протидії зловмисним програмам з використанням методів машинного навчання ідеально підійшла для виявлення й блокування на крапці входу недавніх WannaCry і Petya.

Безперервна аналітика

Використання хмарної аналітики (Talos) більших обсягів даних для визначення, чи є файл безпечним або шкідливим, що підвищує точність виявлення схованих атак на вході в систему й для закриття шляхів проникнення, а також мінімізації уразливостей.

Швидке виявлення погроз

За допомогою технології безагентового виявлення (аналіз і тестування поведінки підозрілих файлів) здійснюється реєстрація всієї файлової активності й, як наслідок, швидке виявлення вірусів.

Ретроспективний аналіз

Автоматичний аналіз історії дій файлів (звідки проникнув, де виконувався, що робив) не тільки знижує до мінімуму ризик глобального поширення зловмисного ПЗ, але й дозволяє виявити точну локалізацію атаки.

Захист від атак

Забезпечення повсюдного захисту від погроз із використанням ретроспективної безпеки до традиційного виявлення, що значно підвищує ефективність, продуктивність мережі й охоплення потенційно шкідливих файлів.

Контроль ланцюжка атаки

Новий рівень аналітики в режимі реального часу для виявлення погроз, що зіставляє шаблони шкідливого поведінки на окремому кінцевому пристрої й на всіх кінцевих пристроях мережі.

Розширена аналітика

Автоматизоване виявлення підозрілого поведінки, що забезпечують розподілене подання всіх областей, які найбільш піддані ризику атаки.

Поведінковий аналіз

Цілеспрямований пошук порушень на підставі реальних подій.

Відстеження подій

Можливість спрощеної й швидкої розбивки ланцюжка атак для своєчасного виявлення основних причин зараження (окремі додатки, файли, документи, віруси й т.д.)

Моніторинг мережі

Звіти не обмежені збором і підрахунком подій. Звітність у системі протидії зловмисним програмам з використанням методів машинного навчання для прикінцевих пристроїв включає панелі, що дають можливість діяти, моніторингу й визначення тенденцій, що показує доречність із погляду бізнесу й вплив з погляду ризику.

Інтеграція з іншими рішеннями

Система протидії зловмисним програмам з використанням методів машинного навчання виконує передачу й кореляцію інформації про погрози по всій архітектурі, включаючи як екосистему система протидії зловмисним програмам з використанням методів машинного навчання, так і інші платформи безпеки, таких як Email і Web Security.

Джерелами найбільшої в галузі бази даних, сформованої на основі моніторингу погроз і аналізу більших даних, є системи колективної інформаційної безпеки, група по інформаційній безпеці й дослідженням і канали системи протидії зловмисним програмам з використанням методів машинного навчання.

Система протидії зловмисним програмам з використанням методів машинного навчання працює в такий спосіб:

- До початку атаки система протидії зловмисним програмам з використанням методів машинного навчання використовує глобальні аналітичні дані по погрозах, які надходять із відділу колективної інформаційної безпеки компанії, групи по інформаційній безпеці й дослідженням, а також по каналах дані системи протидії зловмисним програмам з використанням методів машинного навчання. Це допомагає підсилити захист від відомих і невідомих погроз.

- Під час атаки система протидії зловмисним програмам з використанням методів машинного навчання використовує аналітичні дані, відомі сигнатури файлів і динамічний аналіз на основі технології система протидії зловмисним програмам з використанням методів машинного навчання, щоб виявити й блокувати файли, що порушують політику безпеки, експлуатувати й шкідливе ПЗ, що намагається проникнути в мережу.

- Після завершення атаки або після первісної перевірки файлу система безупинно контролює й аналізує всю активність і трафік файлу, незалежно від його статусу, відслідковуючи будь-які ознаки шкідливого поведіння. Якщо файл, що одержав раніше статус «невідомий» або «безпечний», діє підозріло, система протидії зловмисним програмам з використанням методів машинного навчання фіксує це й відправляє повідомлення в службу інформаційної безпеки із вказівкою потенційної погрози. система протидії зловмисним програмам з використанням методів машинного навчання забезпечує своєчасне одержання даних про те, звідки з'явилася шкідлива програма, які системи вона торкнулася й що робить у цей момент. Система надає інструменти, які дозволяють швидко реагувати на проникнення й усунути його за допомогою декількох клацань миші. Такі інструменти дозволяють службам інформаційної безпеки вчасно одержувати дані, допомагаючи швидко виявити атаку, оцінити масштаб вторгнення й знешкодити шкідливий код до того, як він завдасть шкоди

Машинне навчання складається із двох великих розділів: фази навчання й розпізнавання.

- **Фаза навчання.** На початку фахівці повинні пояснити комп'ютеру, що характеризує вірус. На наступних етапах комп'ютер буде стає усе розумніше до того ж почне вчитися.

- **Розпізнавання.** Потім натренований алгоритм на підставі поведінки виконуваної програми здатний вирішити, чи йде мова про легітимний додаток або про схований у файлі вірус.

У сучасні комерційні продукти безпеки інтегрований захист від програм-зидників. Вона в реальному часі постійно сканує систему на наявність дивних звертань до файлів. Одночасно із цим перевіряються показники системи, з'ясовується, чи не підвищується

раптово навантаження на процесор і чи не зростає стрімко число звертань до дисків (перші індикатори атаки).

В офіційних заявах затверджується, що розроблювачі антивірусів знають свою справу й гарантують ефективний захист від нападів. Однак інсайдери пошепки розповідають, що й у цієї технології є слабкі місця: кібергангстери послідовно встановлюють на ізольовану систему всі розповсюджені антивірусні рішення, а потім спокійно розробляють ідеальний вірус, що не буде замічений сканером і зможе обдурити навіть найсучаснішу евристику.

Проти таких, розроблених з більшими зусиллями, варіантів практично будь-який антивірусний продукт неспроможний. Незважаючи на те що розроблювачі протягом декількох годин після поширення вірусу підготовляють захист, до перших потерпілих протиотрута попадає занадто пізно.

Винуватий у цьому людський фактор: фахівцям зі шкідливого ПЗ необхідно вручну розібрати новий вірус, проаналізувати його й підготувати опис, що потрапить на систему клієнта при відновленні. У випадку зі складними «шкідниками» процес може зайняти кілька днів. На аналіз особливо вишуканого утвору злочинців можуть піти навіть місяці.

Деякі розроблювачі бачать майбутнє вірусного аналізу у відмові від людського фактора: у центрі будуть перебувати машини, що розпізнають шкідливе ПЗ й запускають відповідне відновлення.

Аналіз через машинне навчання

Усілякі компанії, від Symantec до Malwarebytes, сьогодні займаються розробкою методів, при яких роботу з аналізу вірусів візьмуть на себе ІТ-системи. У випадку з машинним навчанням дослідники «зкормлюють» суперкомп'ютеру кілька мільйонів файлів – як шкідливих, так і безпечних.

Програми з машинним навчанням. Malwarebytes починаючи із третьої версії робить ставку на автоматизоване навчання.

За допомогою так званих ознакових описів потім комп'ютеру пояснюється, як виглядає вірус, якими характеристиками він володіє і як звичайно поводить себе на комп'ютері своєї жертви – абсолютно так само, як і при розвитку й вихованні дитини.

Таким чином, поступово машина знайде самостійність і буде усе надійніше розрізняти вірус і легітимну програму. І нехай частота помилок залишається ще досить високої, поступово вона буде знижуватися, а алгоритм удосконалюватися.

Компанія Symantec для машинного навчання звела навіть окремий обчислювальний центр у Великобританії

Однак такий розвиток вимагає часу й ресурсів. В Symantec є свій окремий обчислювальний центр для машинного навчання, де займаються оптимізацією методики.

У сучасних антивірусних продуктах цей алгоритм уже є елементом стратегії розпізнавання. Незважаючи на це на заднім тлі однаково присутні люди-дослідники, оскільки нова технологія ще страждає від дитячих хвороб.

Проблеми з панацеєю

Як би не була гарна ідея машинного навчання, до цих спостерігаються ключові недоліки, що затримують тріумфальний хід. У першу чергу, усе впирається в гроші.

Крім того, незважаючи на перехід до машинного навчання, на місці завжди повинна бути присутнім команда експертів. Вона контролює алгоритм і в неоднозначних випадках сама приймає рішення, вірус це чи ні, вносячи відповідні коректування.

Фірми, що скорочують витрати на персонал і стовідсотково належні на алгоритм, ризикують допустити в навчальний процес помилкові результати. Таким чином, їхня безпека стрімко знижується.

Одного лише машинного навчання недостатньо

Проблема машинного навчання впирається насамперед у мову. Якщо представити нинішній сценарій погрози у вигляді англомовної країни, такий алгоритм був би успішний лише в боротьбі зі шкідливим ПЗ англійською мовою.

Однак оскільки ландшафт погрози постійно змінюється, і відповідно постійно з'являється нова мова, доводиться увесь час із чистого аркуша адаптувати алгоритм під ситуацію, що змінилася. А це складно. Приміром, сімейство Trojan-Ransom.Win32.Shade складається з 30 000 підтипів. Одним лише розпізнаванням такого сімейства алгоритм не здатний забезпечити захист від всіх його підвидів. Для цього знадобилися б сотні прикладів на кожний вірус – лише так алгоритм навчається автоматично.

Утиліта машинного навчання також не здатна захистити від спеціалізованих атак. Просто відсутня база даних. На одній методиці машинного навчання далеко не виїхати. Вона може бути винятково шестірнею в складній антивірусній машині. Але навіть із машинним навчанням і іншими засобами антивірусні системи катастрофічно відстають від розроблювачів шкідливого ПЗ.

Всі захисні продукти роблять помилки

Навіть якщо в системі використовуються «пісочниці», карантин, евристичні методи й машинне навчання, зловмисники умудряються неї обманювати. Як уже було сказано вище, досить протестувати антивірусне рішення на ізольованій системі до релізу «шкідника» і знайти в такий спосіб пробіли в розпізнаванні.

Сучасні антивіруси повинні розпізнавати й зупиняти програми-зидники завчасно

Іншу небезпеку представляють самі антивіруси. Хакери, користуючись уразливостями, за допомогою перепрограмування можуть одержати за ними контроль так само, як над звичайним ПЗ. Так, у червні 2016 року постраждала компанія Symantec. Фахівці виявили сім критичних лазівок практично у всіх антивірусних продуктах цього розроблювача.

Приклавши мінімальні зусилля, зловмисники інфікують не тільки комп'ютери, але й цілі корпоративні мережі. Для використання уразливостей вони повинні примусити свою жертву до виклику модифікованої веб-сторінки. Оскільки антивірусним продуктам на комп'ютері видаються максимально розширені права, подібні уразливості стають фатальними. Гра в кішки-мишки між атакуючими й що обороняються, таким чином, триває. Однак машинне навчання в кожному разі ускладнить життя розроблювачам вірусів.

Напрямки розпізнавання

У сучасних антивірусних системах для розпізнавання використовується цілий ряд методів. Нові файли проходять через різні стадії за пару митей.

– **Аналіз поведінки.** При виникненні підозр сканер запускає файл передбачуваного вірусу в пісочниці – захищеної області. Там рудиментарний алгоритм перевіряє, чи не заражена програма.

– **Швидка оцінка.** У майбутньому після впровадження машинного навчання нинішня модель буде пропонувати більше швидкий і надійний захист, а також відрізнитися підвищеною продуктивністю. Однак і в цьому випадку остаточне рішення, чи довіряти файлу або перемістити його в карантин, приймає користувач за комп'ютером.

Структурна схема розробленої, у результаті виконання магістерської роботи, системи зображена на рисунку 1.

З нього ми бачимо, що система складається з наступних структурних блоків:

– Модуль машинного навчання системи протидії зловмисним программам (антивірусної системи (АС)).

– Джерела погроз.

– Антивірусне програмне забезпечення на персональному комп'ютері.

– Загрози безпеці.

Розглянемо ці структурні блоки більш детально.

До джерел загроз відносяться наступні:

– Загрози з інтернету.

– Загрози при роботі зі змінними носіями інформації.

До антивірусного програмного забезпечення на персональному комп'ютері, відносяться наступні підсистеми:

- Підсистема контролю цілісності.
- Підсистема контролю процесів.
- Підсистема самозахисту антивірусу.
- Підсистема виявлення атак.
- Підсистема аналізу захищеності.
- Підсистема антивірусного захисту.
- Підсистема захисту від спаму.
- Підсистема мережного екранування.

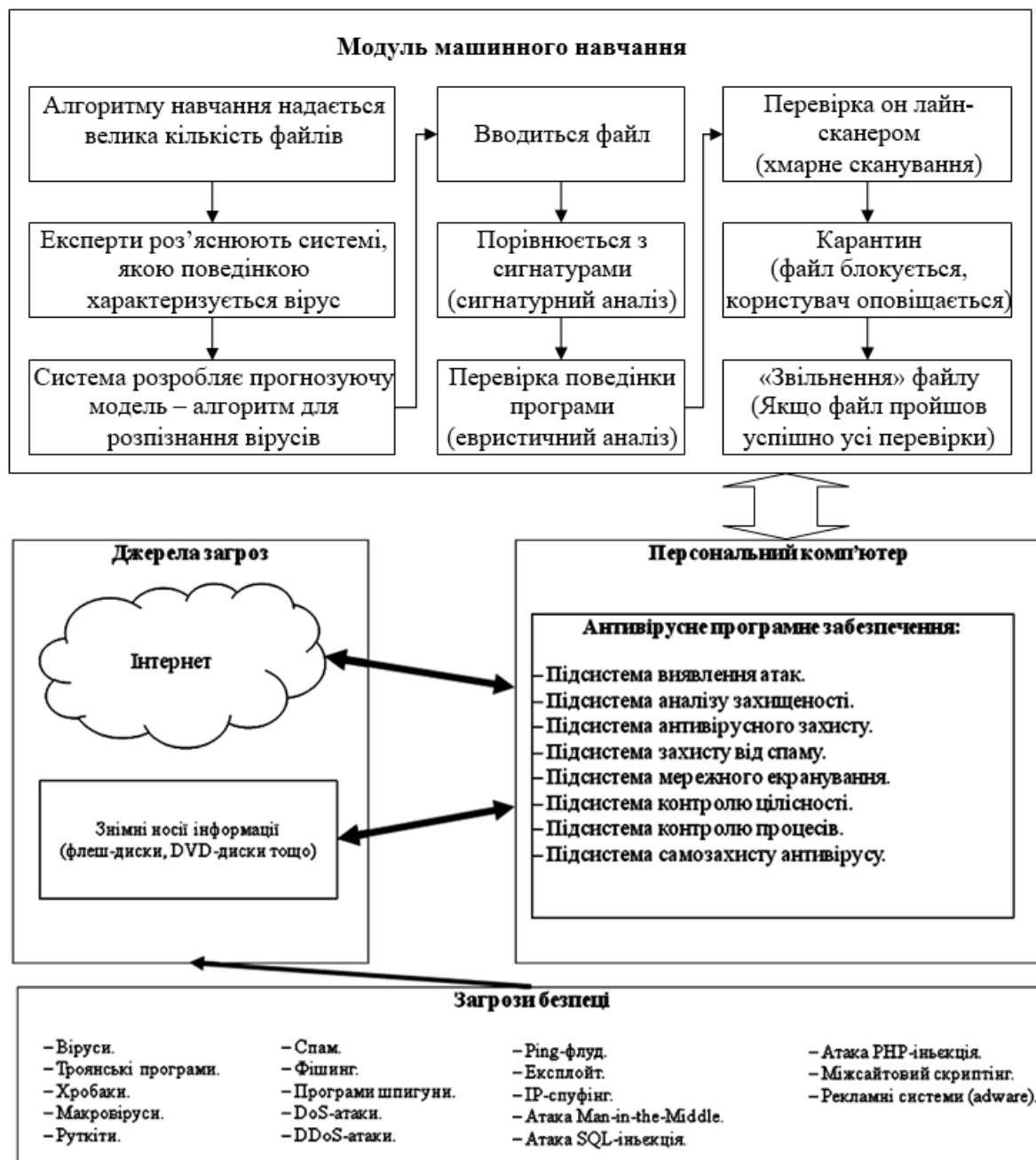


Рисунок 1 – Структурна схема системи

Розглянемо їх більш детально.

Підсистема виявлення атак призначена для виявлення несанкціонованої вірусної активності за допомогою аналізу пакетів даних, циркулюючих в антивірусній системі, а також подій, що реєструються на серверах і робочих станціях користувачів.

Підсистема аналізу захищеності забезпечувати можливість виявлення технологічних і експлуатаційних уразливостей АС за допомогою проведення мережевого сканування.

Підсистема антивірусного захисту призначена для виконання наступних функцій: видаленої установки і деінсталяції антивірусних засобів на серверах і робочих станціях користувачів; видаленого управління параметрами роботи підсистем захисту, що входять до складу комплексної системи антивірусного захисту; централізованого збору і аналізу інформації, що поступає від інших підсистем.

Підсистема захисту від спаму. Антиспам дозволяє відслідковувати, фільтрувати та видаляти спам, що пересилається в вашу поштову скриньку. Система не видаляє повідомлення, які здадуться їй спамом. Вона лише робить відповідну позначку на них і доставляє їх, як завжди. Саме тому ці повідомлення також включаються до вашого трафіка. Рівень перевірки спаму – Spam check level – визначає, наскільки жорсткою буде фільтрація спаму. Антиспамові фільтри аналізують кожне електронне повідомлення, яке проходить крізь поштовий шлюз і оцінюють його за шкалою від 1 до 14. Чим більший номер, тим більша ймовірність того, що повідомлення буде віднесено до розряду спаму: Дуже жорстка фільтрація: гарантує, що до вашої поштової скриньки спам практично не буде надходити. Тим не менше, ви ризикуєте втратити і потрібні повідомлення (не пропускає повідомлення, що оцінені вище 2). Жорстка: практично всі спамові повідомлення будуть видалені, є ймовірність видалення потрібних повідомлень (не пропускає повідомлення, що оцінені вище 4). Нормальна: може заблокувати деякі розсилки (не пропускає повідомлення, що оцінені вище 7). Нежорстка: пропускає "другосортну" пошту (не пропускає повідомлення, що оцінені вище 10). М'яка: пропускає майже всю пошту (не пропускає повідомлення, що оцінені вище 14). Рівень оцінки за замовчуванням зазвичай дорівнює 5, проте адміністратор хостингової системи може його змінити. Обробка спаму: Mark as spam: – присвоєння позначки "спам" – до теми електронного повідомлення буде додане слово СПАМ, і потім це повідомлення буде переслане клієнту як вкладення із зазначенням деталей. Remove: видалення спамового повідомлення. Коли клієнт запустить команду надіслати/отримати, повідомлення зі спамом до нього не надійде. Move To: дозволяє вказати поштову скриньку, куди буде відправлено спам. Клієнти не отримають спам у свою поштову скриньку, проте зможуть переглянути його у вказаній скриньці.

Підсистема мережного екранування призначена для захисту робочих станцій користувачів від можливих мережевих вірусних атак за допомогою фільтрації потенційно небезпечних пакетів даних.

Підсистема контролю цілісності. Контролює все програмне забезпечення на брандмауері і присилає звіти про всі віддалені файли, що щойно з'явилися і змінилися.

Підсистема контролю процесів призначена для визначення які процеси відбуваються у системі, та чи є вони дозволеними операційною системою, чи ні.

Підсистема самозахисту антивірусу. Ефективна система самозахисту захищає його від зупинки або відключення навіть при проведенні цільових атак. Антивірус здатний створювати диск аварійної регенерації системи. Будь-які посилання на шкідливі або фішингові сайти програмою блокуються автоматично. У разі поразок антивірус після ліквідації загроз самостійно здатний відновити систему, повернувши її в стан, який був до виникнення проблем з руйнівним кодом або вірусом. Програма виконує діагностику системи, виявляючи існуючі пробіли та визначаючи відповідність її оновлень за допомогою бази даних. Але програмою, на жаль, не передбачено надання інформації про те, яка версія програми, яка має прогалини, встановлювалася. Дану інформацію доведеться виявляти самостійно. Крім того, повна інформація про сам процес усунення вразливих місць недоступна.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів протидії зловмисним програмам з використанням методів машинного навчання. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем протидії зловмисним програмам з використанням методів машинного навчання.
- Досліджена система протидії зловмисним програмам з використанням методів машинного навчання.
- На основі отриманих результатів досліджень створена програмна реалізація системи протидії зловмисним програмам з використанням методів машинного навчання.

Розроблені алгоритми дозволяють успішно вирішувати завдання протидії зловмисним програмам з використанням методів машинного навчання. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Kuznetsov O., Frontoni E., Kuznetsova Y., Chevardin V., Smirnov O. «Architectural foundations for adaptive security in edge computing systems». *Cybersecurity Defensive Walls in Edge Computing*, 2025. pp. 21-61.
2. Вінтенко, Б.Ю., Миронець, І.В., Смірнов, О.А., Коваленко, О.В., Усік, П.С., Буравченко, К.О., Лисенко, І.А. «Логіко-структурна модель комп'ютерно-орієнтованої процедури системи підтримки оперативного персоналу АЕС». *Кібербезпека: освіта, наука, техніка*. 2025. Том 2 № 30. С. 413-427, 2025.
3. Смірнова, Т.В. «Дослідження методів, моделей та сучасних ІТ-рішень для підтримки технологічних процесів у критичній інфраструктурі держави». *Кібербезпека: освіта, наука, техніка*. 2025. Том 2 № 30. С.195-208, 2025.
4. Усік, П.С., Смірнова, Т.В., Буравченко, К.О., Смірнов, О.А., Улічев, О.С., Смірнов, С.А. «Дослідження технологій забезпечення кібербезпеки банківських систем з використанням штучного інтелекту». *Кібербезпека: освіта, наука, техніка*. 2025. Том 1 № 29. С.704-716, 2025
5. Kuznetsov, O., Frontoni, E., Kuznetsova, K., Arnesano, M., Smirnov, O. «A secure biometric authentication architecture for blockchain-driven cyber-physical systems». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 193-224.
6. Kuznetsov, O., Smirnov, O., Akhmetov, B., Alimseitova, Z., Imoize, A.L. «Deep Learning Frontiers in Copy-Move Forgery Detection: Advances, Challenges, and Future Directions». *Advancements in Cybersecurity Next Generation Systems and Applications*, 2025. 202-229.
7. Вінтенко Б., Смірнов О., Миронець І., Смірнова Т., Смірнов С. «Імітаційна модель шляхів вхідних даних комп'ютерної інтелектуальної системи підтримки оператора енергоблоку АЕС». *Комбінаторні конфігурації та їхні застосування: Матеріали XXVII Міжнародного науково-практичного семінару, присвяченого 125-річчю Національного університету «Запорізька політехніка» (Запоріжжя-Кропивницький-Київ, 4-6 червня 2025 р.)*. Запоріжжя: НУ «Запорізька політехніка», 2025. С.82-91.
8. Al-Azzeh, J., Ayyoub, B., Mesleh, A., Smirnova, T., Gnatyuk, S., Drieiev, O., Smirnov, O., Dorenskyi, O. «Cloud-Based Information System for Evaluating Caverns in the Process of Blasting Metal Surfaces of Details». *International Review on Modelling and Simulations* 18 (1), 2025. pp. 32-42.
9. Вінтенко Б.Ю., Смірнов О.А., Миронець І.В., Смірнова Т.В., Коваленко О.В., Мацуй А.М. «Модель шляхів отримання вхідних даних комп'ютерної інтелектуальної системи підтримки оперативного персоналу АЕС». *Центральноукраїнський науковий вісник. Технічні науки*. 2025. Вип. 11(42), ч. II. С.52-62.
10. Вінтенко Б.Ю., Смірнов О.А., Миронець І.В., Смірнова Т.В. «Методи забезпечення відмовостійкості інтелектуальних систем підтримки оператора». *VIII міжнародна науково-практична конференція «Інформаційна безпека та комп'ютерні технології»*, м. Кропивницький. 24-25 квітня 2025 р. – Кропивницький: ЦНТУ. – 2025. – С. 44-46.
11. Смірнов, О.А., Константинова, Л.В., Коноплицька-Слободенюк, О.К., Козірова, Н.В., Якименко, Н.М., Доренський, О.П., Буравченко, К.О. «Дослідження інструментів штучного інтелекту для роботи з базами даних та аналізу даних». *Кібербезпека: освіта, наука, техніка*. 2025. №3(27), С. 429-448.
12. Lakhno, V., Malyukov, V., Smirnov, O., Bebashko, B., Chubaievskiy, V., Zhumadilova, M., Malyukova, I., Smirnov, S. «Multifactorial Model for Targeted Attacks Counteracting Within the Framework of a Multi-Step Quality Game with Fuzzy Information». *8th International Symposium on Intelligent Informatics, ISI 2023*, 2025. vol 389. pp 377-389. Springer, Singapore.
13. Smirnov O., Fedorov E., Neskrodieva A., Neskrodieva T. «Intellectual Classification method of Gymnastic Elements Based on Combinations of Descriptive and Generative Approache». *CEUR Workshop Proceedings Volume 3664*, 2024, Pages 11-23.
14. Kuznetsov, O., Kryvinska, N., Ilchenko, O., Smirnova, T., Ulianovska, Y. «Comparative Analysis of Cryptocurrency Trading Platforms Using the Analytic Hierarchy Process». *CEUR Workshop Proceedings*, 2023, 3628, pp. 106-115.
15. Malyukov V., Bebashko B., Lakhno V., Smirnov O., Malyukova I., Mohylnyi H. «Managing the Purchase-Sale

- Process of Digital Currencies Under Fuzzy Conditions». *Lecture Notes in Networks and Systems*, 2023, 729 LNNS, pp. 104–112.
16. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». *Advanced Information Systems*, 2023, 7(2), pp. 49-56.
 17. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchey, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». *CEUR Workshop Proceedings*, Volume 3530, 2023, pp. 256-265.
 18. Аль-Мудхафар Акіл Абдулхуссейн М., Смірнова Т.В., Буравченко К.О., Смірнов О.А. «Метод оцінки та підвищення користувальницького досвіду абонентів в програмно-конфігурованих мережах на основі використання машинного навчання». *Сучасні інформаційні системи*, 2023, том 7, № 2, С. 49-56.
 19. Smirnov, O., Karapetyan, A., Fedorov, E., «Creating Neural Network and Single Solution Human-Based Metaheuristic Methods of Solving the Traveling Salesman Problem». *CEUR Workshop Proceedings*, Volume 3312, 2022, pp. 47-58.
 20. Smirnov, O., Neskoroidea, T., Fedorov, E., Rudakov, K., Neskoroidea, A. «Method Detection Audit Data Anomalies on Basis Restricted Cauchy Machine» *CEUR Workshop Proceedings*, Volume 3187, 2022, pp. 1-12.
 21. Smirnov O., Smirnova T., Anas M. Al-Oraiqat, Drieiev O., Polishchuk L., Sheroz Khan, Yassin M. Y. Hasan, Aladdein M. Amro, Hazim S. AlRawashdeh «Method for Determining Treated Metal Surface Quality Using Computer Vision Technology». *Sensors (Basel, Switzerland)* Volume 22, Issue 16, 6223, 2022.
 22. Smirnov, O., Lakhno, V., Akhmetov, B., Chubaievskiy, V., Khorolska, K., Bebesko, B. «Selection of a Rational Composition of Information Protection Means Using a Genetic Algorithm». In: Rajakumar, G., Du, KL., Vuppapapati, C., Beligiannis, G.N. (eds) *Intelligent Communication Technologies and Virtual Mobile Networks. Lecture Notes on Data Engineering and Communications Technologies*, vol 131. 2023. Springer, Singapore. pp. 21-34.
 23. Kuznetsov, A., Oleshko, I., Chernov, K., Bagmut, M., Smirnova, T. «Biometric authentication using convolutional neural networks». *Lecture Notes in Networks and Systems*. Volume 152, 2021, Pages 85-98.
 24. Smirnov O., Kuznetsov A., Kryvinska N., Kiian A., Kuznetsova K. «Full Non-Binary Constant-Weight Codes». *SN Computer Science*, Vol 2, 337, 2021. <https://doi.org/10.1007/s42979-021-00739-w>.
 25. Smirnov O., Neskoroidea T., Fedorov E., Rymar P. «Neural Network Modeling Method of Transformations Data of Audit Production with Returnable Waste». *CEUR Workshop Proceedings* Volume 3101, 2021, Pages 192-207.
 26. Smirnov, O., Kuznetsov, A., Potii, O., Poluyanenko, N., Stelnyk, I., Mialkovsky, D. «Combining and filtering functions in the framework of nonlinear-feedback shift register». *International Journal of Computing*; 2020, Volume 19, Issue 2 – Research Institute for Intelligent Computer Systems – 2020. – P. 247-256.
 27. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». *CEUR Workshop Proceedings*. Volume 2740, 2020, Pages 102-114.
 28. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177.
 29. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) *Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies*, vol 48. Springer, Cham. 2021. pp 557-587.
 30. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». *CEUR Workshop Proceedings* Volume 2616, 2020, Pages 366-379.
 31. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», *CEUR Workshop Proceedings* Volume 2608, 2020, Pages 633-645.

УДК 004

М.Хромочкін, магістр гр. КІ-24М,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ МЕРЕЖЕВОГО ВІДЕОСПОСТЕРЕЖЕННЯ НА ОСНОВІ ВИКОРИСТАННЯ DIRECTX

У статті розроблено програмне забезпечення, яке призначено для системи мережевого відеоспостереження на основі використання DirectX. Метою розробки є дослідження та принципи побудови системи мережевого відеоспостереження на основі використання DirectX. Об'єктом дослідження є процес мережевого відеоспостереження на основі використання DirectX. Предметом дослідження є методи мережевого відеоспостереження на основі використання DirectX. Методи дослідження базуються на методах теорії кодування та теорії побудови комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи мережевого відеоспостереження на основі використання DirectX. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

мережеве відеоспостереження, DirectX

Постановка проблеми. Система відеоспостереження забезпечує цілодобовий моніторинг, запобігання злочинам та збір доказів. З огляду на те, що світовий ринок, за прогнозами, досягне 147,04 мільярда доларів до 2030 року, ці системи мають вирішальне значення для захисту співробітників, активів та майна.

Основні компоненти системи відеоспостереження:

- Камери: Запис відео високої чіткості.
- Пристрій запису: Зберігає відео локально (NVR/DVR) або в хмарі.
- Монітор/дисплей: Перегляд відео в реальному часі та записаного відео.
- Мережеве підключення: Забезпечує віддалений доступ.
- Рішення для зберігання даних: керує збереженням відео.

Сучасні системи пропонують розширені функції, такі як виявлення на базі штучного інтелекту, розпізнавання облич та розпізнавання номерних знаків, часто інтегруючись із системами контролю доступу для надсилання сповіщень у режимі реального часу. Технологія вийшла за рамки простого запису та використовує аналіз закономірностей та виявлення аномалій, змінюючи безпеку з реактивної на проактивну.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи мережевого відеоспостереження на основі використання directx.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи мережевого відеоспостереження на основі використання DirectX.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем мережевого відеоспостереження на основі використання DirectX.
- Дослідження системи мережевого відеоспостереження на основі використання DirectX.
- Програмна реалізація системи мережевого відеоспостереження на основі використання DirectX.

Об'єктом дослідження є процес мережевого відеоспостереження на основі використання DirectX.

Предметом дослідження є методи мережевого відеоспостереження на основі використання DirectX.

Методи дослідження базуються на методах теорії кодування та теорії побудови комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Системи відеоспостереження важливі для забезпечення безпеки в різних місцях. Вони допомагають, показуючи відео в реальному часі та покращуючи безпеку. Нові технології змінили принципи роботи цих систем, зробивши їх швидшими та розумнішими. Очікується, що ринок відеоспостереження значно зросте. До 2030 року він може коштувати 88,71 мільярда доларів. Такі круті ідеї, як інструменти штучного інтелекту, блокчейн та чітке зображення, перетворюють старі системи на розумніші.

Системи спостереження на базі штучного інтелекту та інтелектуальні технології

Краще виявлення та розпізнавання об'єктів

Швидке виявлення загроз

Системи на базі штучного інтелекту одразу перевіряють відеопотоки. Розумні програми виявляють небезпеки в міру їх виникнення. Швидкі перевірки допомагають у ризикованих місцях. Служби безпеки діють швидше під час надзвичайних ситуацій. Інструменти штучного інтелекту помічають невеликі проблеми, які люди можуть пропустити. Дослідження мереж реального часу показує, що штучний інтелект економить час у складних ситуаціях.

Спостереження за моделями поведінки

Інструменти штучного інтелекту спостерігають за тим, як люди поведуться в певних місцях. Вони вивчають звичайні дії та виявляють дивні. Це допомагає зупинити проблеми, перш ніж вони погіршаться. Журнал «Campus Safety» стверджує, що системи штучного інтелекту чудово справляються з вивченням поведінки. Спостереження за закономірностями означає меншу потребу в нагляді за людьми, що спрощує роботу.

Розумні прогнози для безпечніших місць

Менше хибних тривог

Системи штучного інтелекту зменшують кількість хибних тривог. Вони розрізняють реальні небезпеки від нешкідливих подій. Це робить роботу служби безпеки більш плавною та з меншою кількістю перерв. Дослідження Vokusee показують, що штучний інтелект значно зменшує кількість хибних тривог. Краща точність допомагає командам безпеки використовувати свій час розумно.

Раннє усунення проблем

Інструменти штучного інтелекту прогнозують ризики до того, як вони стануться. Вони вивчають старі дані, щоб побачити майбутні проблеми. Це допомагає виправити слабкі місця до того, як почнуться проблеми. Ринки та дослідження ринків показують, що штучний інтелект дає поради в режимі реального часу, щоб команди не просто реагували. Прогнозування проблем підвищує безпеку загалом.

Хмарне відеоспостереження та гібридні рішення

Переваги хмарного сховища

Легко вирощувати та економити гроші

Хмарні відеосистеми легко розширювати за потреби. Бізнес може додавати більше сховища, не купуючи нове обладнання. Вони можуть змінювати розмір сховища залежно від того, що їм потрібно на даний момент. Це допомагає заощаджувати гроші та розумно використовувати ресурси. VSaaS пропонує доступні варіанти як для малих, так і для великих компаній. Збільшення або зменшення обсягу сховища дозволяє контролювати витрати.

Дивіться та керуйте з будь-якого місця

Хмарні системи дозволяють перевіряти камери з будь-якого місця. Служби безпеки можуть переглядати відео в реальному часі або збережені відео онлайн. Керування багатьма локаціями стало простіше за допомогою однієї системи. Хмарні інструменти швидко надсилають сповіщення, допомагаючи під час надзвичайних ситуацій. Віддалене спостереження спрощує роботу та забезпечує безперебійний режим.

Збереження безпеки та конфіденційності даних

Надійний захист даних

Спеціальні інструменти захищають дані, що зберігаються в хмарі, від хакерів. Зашифровані дані запобігають доступу інших до конфіденційної інформації. Рівні захисту забезпечують безпеку відео під час надсилання або зберігання. Хмарні компанії використовують надійні засоби безпеки, щоб запобігти витоку даних. Шифрування забезпечує безпеку та конфіденційність відеоданих.

Дотримання правил у всьому світі

Хмарні системи допомагають дотримуватися глобальних правил безпеки даних. Такі правила, як GDPR та CCPA, гарантують правильне оброблення даних. Хмарні інструменти допомагають керувати тим, хто може переглядати або зберігати дані. Дотримання правил зміцнює довіру та уникає юридичних проблем. Дотримання цих стандартів робить системи безпечнішими загалом.

Інтеграція Інтернету речей та смарт-пристроїв у системи відеоспостереження

Розумні пристрої та підключення

Роль датчиків Інтернету речей

Датчики Інтернету речей збирають дані з навколишнього середовища та діляться ними. Вони перевіряють такі речі, як рух, звук і температура. Це покращує роботу систем спостереження. Камери та датчики разом швидко виявляють дивну активність. Ці датчики допомагають у небезпечних зонах, надаючи більше деталей. Системи безпеки використовують їх для швидкого реагування під час надзвичайних ситуацій.

Безшовна інтеграція з розумними містами

Розумні міста використовують інструменти Інтернету речей (IoT) для кращого управління. Камери та датчики вивчають дорожній рух, щоб покращити час сигналізації. Вони також стежать за натовпами, щоб запобігти переповненню в людних місцях. IoT підключає сигналізацію, камери та вуличні ліхтарі для забезпечення безпеки. Міські планувальники покладаються на ці системи для забезпечення безпеки території.

Проблеми інтеграції Інтернету речей

Вразливості мережі

Пристрої Інтернету речей можуть бути атаковані через слабкі мережі. Поганий рівень безпеки дозволяє хакерам переглядати приватні відеодані. Хакери знаходять прогалини в незахищених системах Інтернету речей. Брандмауери та сповіщення допомагають блокувати ці ризики. Оновлення пристроїв часто захищає їх від нових загроз.

Проблеми сумісності

Різні бренди виготовляють пристрої Інтернету речей з унікальним дизайном. Це спричиняє проблеми під час їх підключення в одній системі. Пристрої можуть погано працювати разом через різні правила. Розробники створюють інструменти для виправлення цих проблем з'єднання. Стандартні правила спрощують підключення пристроїв для великих проєктів.

Досягнення в технологіях камер відеоспостереження

Відеоспостереження високої роздільної здатності

Камери Ultra-HD та 8K

Камери високої роздільної здатності показують чіткіші та різкіші зображення. Камери Ultra-HD та 8K дозволяють легко бачити деталі. Ці камери охоплюють великі площі без втрати якості зображення. Вони корисні в людних або небезпечних місцях. Чіткий запис допомагає розслідуванням отримати точні візуальні докази.

Можливості роботи в умовах низької освітленості та нічного бачення

Звичайним камерам важко впоратися з темними місцями. Нові системи відеоспостереження використовують технології низької освітленості та нічного бачення. Інфрачервоні датчики дозволяють камерам бачити в повній темряві. Сонячні камери безпеки, такі як Bokysee Solar Security Camera, показують кольори вночі. Діапазон нічного бачення 65 футів краще захищає майно вночі. Ці функції підвищують безпеку в погано освітлених місцях.

**Міркування щодо сховища та пропускної здатності
Технології стиснення**

Високоякісні відео потребують багато місця для зберігання. Інструменти стиснення зменшують розміри файлів, але зберігають хорошу якість. Такі методи, як H.265, економлять місце для зберігання та використовують менше пропускної здатності. Системи периферійного відеоспостереження обробляють дані безпосередньо на камері. Це зменшує потребу надсилати великі файли на сервери. Швидша обробка покращує роботу систем.

Вплив на витрати

Кращі камери потребують більшого сховища та пропускної здатності. Підприємства можуть витрачати більше на оновлення систем. Хмарне сховище пропонує гнучкі варіанти управління цими витратами. Інструменти стиснення допомагають знизити довгострокові витрати. Сучасні системи відеоспостереження покращують безпеку та з часом заощаджують ресурси.

Bokysee та інші тенденції комерційних камер безпеки**Огляд пропозицій Bokysee****Особливі можливості та здібності**

Bokysee виробляє багато типів камер відеоспостереження для різних потреб. Їхня продукція включає IP-камери, розумні Wi-Fi камери та камери на сонячних батареях. Вони також продають повні комплекти відеоспостереження для комплексних систем безпеки. Bokysee зосереджується на забезпеченні хорошої якості за низькими цінами, допомагаючи як бізнесу, так і домовласникам.

Одним з їхніх найкращих продуктів є PTZ-камера на сонячній енергії. Вона може обертатися на 360° та має подвійний об'єктив для моніторингу. Це робить її чудовою для спостереження за великими просторами. Сонячна енергія забезпечує її роботу з мінімальним обслуговуванням. Людям подобається, наскільки легко нею користуватися вдома та на підприємствах. Сильна дослідницька команда Bokysee постійно створює нові та кращі продукти.

Bokysee працює у понад 80 країнах, пропонуючи індивідуальні рішення. Великі клієнти та покупці на основі проектів користуються їхніми послугами OEM та ODM. Їхні камери використовуються в містах та віддалених місцях.

Наприклад, їхні сонячні камери допомагають у районах без електрики. Бізнес заощаджує гроші, оскільки ці камери потребують менше догляду. Ці приклади показують, як Bokysee вирішує реальні проблеми безпеки за допомогою розумних ідей.

Порівняння Bokysee з іншими**Сильні та слабкі сторони**

Компанія Bokysee відома своєю доступною ціною та креативністю. Їхні камери на сонячних батареях виділяють їх. Функція подвійного об'єктива охоплює більше місця, ніж звичайні камери. Їхні продукти прості в налаштуванні та використанні, що робить клієнтів задоволеними.

Але деякі конкуренти мають краще нічне бачення, ніж Bokysee. Тим не менш, Bokysee пропонує надійні та бюджетні варіанти. Вони постійно вдосконалюються, тому майбутні продукти можуть виправити ці проблеми.

Позиція на ринку та плани на майбутнє

Vokusee має сильні позиції на світовому ринку завдяки своїм розумним ідеям. Присутність у понад 80 країнах показує, що вони задовольняють багато потреб у безпеці. Їхні низькі ціни допомагають як малому, так і великому бізнесу.

Зараз більше людей хочуть сонячних батарей та інтелектуальних систем безпеки. Зосередження Vokusee на дослідженнях незабаром призведе до появи кращих камер. Їхнє прагнення до нових ідей робить їх лідером у сфері відеоспостереження.

Кібербезпека та блокчейн у системах відеоспостереження

Боротьба з кіберзагрозами

Слабкі місця систем спостереження

Хакери атакують слабкі місця у відеосистемах. Старе програмне забезпечення дозволяє їм красти конфіденційні дані. Незахищені мережі дозволяють стороннім людям переглядати відеоканали. Погано налаштовані пристрої полегшують атаки. Слабкі паролі дозволяють хакерам швидко проникнути в систему. Відсутність шифрування під час обміну даними ставить під загрозу конфіденційність.

Оновлення систем часто блокує ці слабкі місця. Брандмауери зупиняють небажаний доступ до мереж. Багатофакторний вхід захищає облікові записи від хакерів. Написання безпечного коду зменшує проблеми з програмним забезпеченням. Тестування систем знаходить та виправляє діри в безпеці.

Поради щодо кращої кібербезпеки

Хороша кібербезпека забезпечує безпеку відеосистем. Шифрування приховує дані, щоб інші не могли їх прочитати. Перевірки ідентифікації контролюють, хто бачить конфіденційну інформацію. Перевірки ризиків виявляють небезпеки та швидко їх усувають. Дотримання правил ISO 27001 та NIST робить системи безпечнішими.

Компанії використовують багато рівнів захисту для захисту даних. Регулярні перевірки гарантують дотримання правил, таких як GDPR. Навчання персоналу допомагає виявляти та зупиняти кіберзагрози. Безпечне зберігання запобігає зміні старих відео. Ці кроки знижують ризики та роблять системи сильнішими.

Як блокчейн покращує безпеку

Безпечне зберігання даних

Блокчейн змінює спосіб зберігання відеоданих. Він поширює дані в багатьох місцях, а не лише в одному. Спільні реєстри безпечно зберігають відео на різних комп'ютерах. Кожна дія перевіряється, що запобігає фальшивим змінам. Записи не можна змінити, що забезпечує достовірність та надійність даних.

Блокчейн зберігає копії даних, щоб уникнути втрати файлів. Розумні контракти обробляють завдання та дотримуються правил безпеки. Криптографічні ключі контролюють, хто може отримати доступ до даних. Обмін даними таким чином робить системи сильнішими захищеними від атак.

Захист відеодоказів

Блокчейн забезпечує безпеку та справжність відеодоказів. Спеціальні коди надають кожному відео унікальний відбиток. Якщо хтось змінить відео, код не збігатиметься. Мітки часу показують, коли відео були створені для законного використання. Суди довіряють доказам, захищеним блокчейном.

Незмінні записи запобігають підробці збережених відео. Блокчейн відстежує весь доступ та редагування для прозорості. Безпечне зберігання запобігає видаленню або зміні відео. Компанії використовують блокчейн, щоб залишатися довіреними та сприяти розслідуванням.

Майбутні тенденції у відеоспостереженні та прогнози на 2026 рік

Нові технології

Як квантові обчислення допоможуть

Квантові обчислення кардинально змінять відеоспостереження. Вони використовуватимуть швидкі алгоритми для швидкої обробки даних. Надійне шифрування

захистить відеопотоки від хакерів. Квантові інструменти дозволять швидше приймати рішення в режимі реального часу. Ці системи краще та ефективніше керуватимуть великими обсягами даних.

Покращення в периферійних обчисленнях

Периферійні обчислення зроблять системи спостереження розумнішими. Камери оброблятимуть дані самостійно, а не на серверах. Це допоможе службам безпеки швидше реагувати на проблеми. Використання меншої пропускну здатності заощадить кошти для бізнесу. Конфіденційність покращиться, оскільки дані залишатимуться захищеними під час обробки. Периферійні пристрої створять розумніші та незалежніші системи.

Зростання на ринку

Регіональні зміни

Азіатсько-Тихоокеанський регіон досягне найбільшого зростання у сфері відеоспостереження до 2025 року. Містам, що швидко розвиваються, знадобляться кращі системи безпеки в цій країні. Північна Америка швидше використовуватиме інструменти на базі штучного інтелекту. Європа підключатиме відеоспостереження до проектів розумних міст. Африка купуватиме дешевші та розширювані рішення безпеки.

Прогнози для галузі

Ринок відеоспостереження значно зросте до 2026 року. Штучний інтелект (ШІ) буде рушійною силою змін, і багато компаній планують його використовувати. Бізнесу потрібні системи, які виконують багато завдань і є простими у використанні. Хмарні рішення стануть більш популярними для безпеки та зростання. Розвиток ШІ створить розумніші та потужніші системи спостереження.

Вивчення нових технологій відеоспостереження допомагає покращити безпеку. Нові ідеї, такі як штучний інтелект та блокчейн, роблять системи розумнішими. Екологічні рішення також змінюють те, як сьогодні працює безпека. Бізнес розвивається швидше завдяки таким інструментам, як розумні камери Vokusee. Використання цих інструментів допомагає зупинити проблеми до їх виникнення. Перевірка систем часто забезпечує їх стійкість до нових ризиків. Сучасні інструменти спостереження – це розумний вибір на майбутнє. Співпрацюйте з експертами, щоб знайти найкращі варіанти для ваших потреб. Це гарантує кращу безпеку та успіх у довгостроковій перспективі.

Опис системи відеоспостереження на основі використання DirectX для бездротових мереж починається із загальних відомостей і з опису основних компонентів, з яких складається система:

- Камера – пристрій, що формує зображення. «Ока» і «вуха» системи. Камера знімає, і передає відеосигнал передавачу. Нічим не відрізняється від провідних аналогів.

- Передавач – пристрій, що передає відеосигнал по бездротовому каналі на приймач. Для бездротового відео, як правило, використовують так звані побутові частоти: 2,4 ГГц. Відповідно використання даних передавачів не вимагають ліцензій і дозволів від держорганів.

- Приймач – пристрій, що приймає відеосигнал по бездротовому каналі, і передавальне його на відеореєстратор або монітор.

- Відеореєстратор – пристрій, що записує відеосигнал, що прийшов від приймача. По суті – аналог побутового відеомагнітофона. Пише відео на жорсткий диск або флешку.

- Монітор – пристрій візуального виводу відеоінформації. На ньому ми бачимо, що, що знімає в цей момент камера.

Разом: камера знімає відео, транслює на передавач, передавач транслює відеосигнал в ефір, приймач приймає сигнал і через відеовиходи передає сигнал або на відеореєстратор.

Примітно, що фізично, система відеоспостереження далеко не завжди складається з 5 частин. Кожний виробник намагається вирішити питання компактності й ергономічності системи по-своєму. Приміром, передавач практично завжди інтегрується в камеру. Приймач із відеореєстратором або монітором поєднують в одному корпусі рідше. Але іноді навіть всі три компоненти: приймач, відеореєстратор і монітор розташовують в один корпус. Можливо,

виникне питання: що краще модульні системи, або ж коли всі «в одній коробці»? Відповідь на дане питання немає. Форм фактор не визначає якість, і чи будуть це дешеві системи відеоспостереження чи ні сказати складно. Все залежить від розв'язуваного завдання. Приміром, якщо купуєте камеру з передавачем, то не зможете змінити характеристики камери. Якщо ж окремо купуєте камеру й передавач, то зможете підібрати камеру з потрібними параметрами й здійснити відеоспостереження периметра більш якісно. Або ж, якщо Ви збираєтеся монтувати систему самостійно, то набагато зручніше взяти найбільш інтегрований варіант для того, щоб не возитися із з'єднанням компонентів. Тобто: монітор, об'єднаний з відеореєстратором і приймачем і камеру з убудованим передавачем.

Структурна схема розробленої системи зображена на рисунку 1. На ній показано структуру системи відеоспостереження на основі використання DirectX для бездротових мереж.



Рисунок 1 – Структурна схема системи

Схема складається з наступних компонент:

- Бездротові IP-камери.
- Відеореєстратор.
- Бездротовий маршрутизатор (роутер).
- ПК куди записуються дані, при цьому на ПК реалізована технологія RAID-1, для підвищення надійності зберігання даних.
- UPS – пристрій безперебійного живлення.

Дані передаються за бездротовою технологією nanoNET (802.15.4a).

Крім того реалізований віддалений доступ через Інтернет до відеокамер.

Технологія NanoNET

Nanotron Technologies – берлінська компанія, що досліджує такі питання бездротового зв'язку з малим радіусом дії, як поліпшення показників завадостійкості, питання енергоспоживання й швидкості передачі даних у бездротових мережах малого радіуса дії, а також питання локалізації пристроїв бездротового зв'язку й розробку протоколів для мереж датчиків бездротового зв'язку. Метод, застосовуваний самою природою – лінійно частотна модуляція (кажани, дельфіни користуються даним методом для того, щоб визначити, де вони перебувають) став основою технології за назвою NanoNet.

Де ж актуальне застосування приймачепередатчиків виробництва компанії Nanotron? Такі приймачепередатчики мають діапазон в 2,4 ГГц і використовуються там, де використання мереж Wi-Fi неможливо через їхню властивість споживати багато енергії, а

також там, де продуктивності ZigBee і Bluetooth катастрофічно не вистачає. Більш конкретно – це системи домашньої автоматизації, моніторингу й керування, охоронні системи.

Сигнал лінійно-частотної модуляції форматується (при передачі) і обробляється (при прийманні) при використанні дисперсійної лінії затримки, що виконана на базі фільтра ПАВ. Якщо рівень помилок фіксований, то високі швидкості прийому-передачі даних досягаються за рахунок високого рівня ширини спектра сигналу, що дорівнює 64 МГц. Але є один недолік. Така ширина не дозволяє використовувати в одному приміщенні більше двох мереж.

Приймачепередатчики NanoNet TRX відрізняються високою швидкістю передачі даних (2 Мб у секунду), потужністю діапазоном 1 мВт – 6,3 мВт, більшим радіусом дії, що на відкритому просторі може рівнятися аж до 900 метрів, а також убудованим контролером типу MAC, що одночасно підтримує кілька різних методів доступу до спектра передачі.

При використанні приймачепередатчиків nanoNET TRX і створенні на їхній базі мережних додатків рекомендується використовувати один із двох варіантів ПЗ – "Driver software" або "Portable Protocol Stack (PPS)". Те, який варіант у підсумку буде обраний, залежить від того, наскільки складне бездротове з'єднання маєтись на увазі. Пропоноване програмне забезпечення являє собою вихідні коди, написані мовою C. Перший пакет здатний забезпечити працездатність функцій по прийому-передачі інформації й управляти режимами функціонування приймачепередатчика. Другий пакет призначений для більше складних мереж, і дозволяє набудовувати конфігурацію протоколу залежно від вимог самого додатка. Використання програмного забезпечення PPS і приймачепередатчиків nanoNET TRX дозволяють реалізовувати різні типи мереж, які можуть підтримувати доступ до спектра передачі як прямого, так і випадкового плану. Випадковий доступ може організовуватися методом CSMA / CA (запобігання колізій) або кількарізним доступом з визначенням несучої як апаратними засобами, так і за допомогою ПЗ PPS. При цьому мережа може складатися з однієї або декількох підмереж. У випадку декількох радіус дії мережі може збільшуватися. Реалізація прямого доступу можлива за схемою TDMA (часовий поділ) або за схемою "майстер-ведений". Наприкінці березня цього року був затверджений новий стандарт для фізичного рівня БПД – IEEE 802.15.4a. Він розроблений для систем з високим рівнем перешкод на базі технології CSS розробленою компанією Nanotron і затверджений інститутом інженерів електротехніки й електроніки IEEE.

Методи повторної передачі (ARQ)

Для підвищення завадостійкості системи бездротового відеоспостереження в магістерській роботі пропонується використовувати протокол ARQ – протокол повторної передачі даних.

Багато протоколів канального рівня підтримують надійну передачу даних, виконуючи повторні передачі невдалих передач. Невдалі передачі повідомляються за допомогою повідомлень зворотного зв'язку, таких як повідомлення підтвердження прийому (ACK) і непідтвердження прийому (NACK) відповідно до протоколів автоматичного запиту повторної передачі (ARQ). Механізми ARQ, зокрема, важливі для бездротового середовища передачі, але також застосовуються до провідних ліній зв'язку. Приклади механізмів ARQ, що працюють по бездротових каналах, містять у собі:

- протоколи керування радіоканалом (RLC) для системи пакетного радіозв'язку загального користування (GPRS) і широкополосного множинного доступу з кодовим поділом каналу (WCDMA);

- протокол гібридного ARQ (HARQ) у високошвидкісному керуванні доступом до середовища (MAC-hs) для високошвидкісного пакетного доступу по спадній лінії зв'язку (HSDPA).

Проблема з такими протоколами в тому, що вони не можуть надати швидкий і надійний зворотний зв'язок і ефективно використання радіоресурсів.

Деякі протоколи попереднього рівня техніки використовують просту й швидку концепцію ACK / NACK, що вказує, чи був кадр даних успішно прийнятий. Такі протоколи

не надають порядкових номерів у зворотному зв'язку, а замість цього передавач і приймач неявно встановлюють зворотний зв'язок для окремої передачі, експлуатуючи фіксовану часову залежність. Це часто називається синхронним зворотним зв'язком. Перевагою такого підходу є те, що короткі сигнали можуть посилати часто, тоді як витрата ресурсу передачі є відносно низьким. Ефективність кодування, що досягається, однак, обмежена або неможлива, якщо кожний ACK або NACK є одиночним бітом. Таким чином, існує ризик невірної тлумачення такого одиночного біта в приймачі. Загасаючі провали додатково збільшують імовірність помилки, і досягнення дуже низького коефіцієнта помилок може споживати багато ресурсів, щоб покрити найгірші провали. Таким чином, така передача сигналу також є дорогою, якщо потрібні дуже низькі коефіцієнти помилок, тому що це може бути досягнуто тільки за допомогою збільшення потужності передачі або за допомогою повтору інформації. Відновлення або повторна передача кожного повідомлення зворотного зв'язку, однак, неможлива, тому що необхідно неї синхронізувати за часом з передачею відповідних даних.

Інший клас протоколів використовує блоки зворотного зв'язку, або керування, (іноді іменовані повідомленнями про стан). Такі механізми найчастіше застосовуються для заснованих на вікнах ARQ-протоколів. Блоки зворотного зв'язку можуть явно містити в собі порядкові номери й контрольну суму, а отже, може підтримуватися надійність повідомлень зворотного зв'язку. Неправильно прийнятий зворотний зв'язок не використовується, а відкидається на стороні відправника даних. Повторні передачі або передачі відновлень зворотного зв'язку використовуються, щоб гарантувати те, що зворотний зв'язок коректно прийнятий. Повинне бути відзначене, що такі блоки зворотного зв'язку не вимагають якого-небудь вирівнювання за часом з відповідними блоками даних через порядкову нумерацію блоків даних і посилання на них у блоках зворотного зв'язку. Ці типи механізмів зворотного зв'язку мають перевагу в тому, що є дуже надійними; однак вони типово набагато повільніше в порівнянні із синхронними механізмами ACK / NACK – зворотного зв'язку.

Отже, в області техніки необхідні інтегровані протоколи повторної передачі, які досягають ефективності традиційних ACK / NACK-протоколів при одночасній реалізації надійності явних повідомлень зворотного зв'язку. Переважно, такі інтегровані протоколи повторної передачі можуть бути здійснені в одній категорії протоколів і засновані на тих самих блоках даних протоколу, стані протоколу й логіку.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів мережевого відеоспостереження на основі використання DirectX. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем мережевого відеоспостереження на основі використання DirectX.
- Досліджена система мережевого відеоспостереження на основі використання DirectX.
- На основі отриманих результатів досліджень створена програмна реалізація системи мережевого відеоспостереження на основі використання DirectX.

Розроблені алгоритми дозволяють успішно вирішувати завдання мережевого відеоспостереження на основі використання DirectX. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». Advanced Information Systems, 2023, 7(2), pp. 49-56.
2. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchey, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». CEUR Workshop Proceedings, Volume 3530, 2023, pp. 256-265.

3. Smirnov, O., Odarchenko, R., Smirnova, T., Bondar, S., Volosheniuk, D. «Optimal Structure Construction of Private 5G Network for the Needs of Enterprises». *Lecture Notes on Data Engineering and Communications Technologies*, 2023, 178, pp. 208–223.
4. Аль-Мудхафар Акіл Абдулхуссейн М., Смірнова Т.В., Буравченко К.О., Смірнов О.А. «Метод оцінки та підвищення користувальницького досвіду абонентів в програмно-конфігурованих мережах на основі використання машинного навчання». *Сучасні інформаційні системи*, 2023, том 7, № 2, С. 49-56.
5. Smirnov, O., Neskorodieva, T., Fedorov, E., Rudakov, K., Neskorodieva, A. «Method Detection Audit Data Anomalies on Basis Restricted Cauchy Machine» *CEUR Workshop Proceedings*, Volume 3187, 2022,
6. Smirnov O., Smirnova T., Anas M. Al-Oraiqat, Drieiev O., Polishchuk L., Sheraz Khan, Yassin M. Y. Hasan, Aladdein M. Amro, Hazim S. AlRawashdeh «Method for Determining Treated Metal Surface Quality Using Computer Vision Technology». *Sensors (Basel, Switzerland)* Volume 22, Issue 16, 6223, 2022.
7. Smirnov O., Kuznetsov A., Kryvinska N., Kiian A., Kuznetsova K. «Full Non-Binary Constant-Weight Codes». *SN Computer Science*, Vol 2, 337, 2021. <https://doi.org/10.1007/s42979-021-00739-w>
8. Smirnov O., Kuznetsov A., Zhora V., Onikiychuk A., Pieshkova O. «Hiding Messages in Audio Files Using Direct Spread Spectrum». *11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2021, Cracow, Poland, 22-25 September 2021*. P. 414-418.
9. Smirnov O., Kuznetsov A., Lokotkova I., Kuznetsova T., Florov S., Lebid O. «Using Orthogonal Signals to Hide Information in Images». *4 IEEE International Conference on Advanced Information and Communication Technologies (AICT) - 2021, Lviv, Ukraine, September 21-25, 2021*. P. 255-260.
10. Smirnov, O., Kuznetsov, A., Potii, O., Poluyanenko, N., Stelnyk, I., Mialkovsky, D. «Combining and filtering functions in the framework of nonlinear-feedback shift register». *International Journal of Computing*; 2020, Volume 19, Issue 2 – Research Institute for Intelligent Computer Systems – 2020. – P. 247-256.
11. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». *CEUR Workshop Proceedings*. Volume 2740, 2020, Pages 102-114.
12. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». *Journal of theoretical and applied information technology* Vol.98. No 21, 2020, P. 3334-3346.
13. Smirnov O., Kuznetsov A., Kovalchuk D., Kuznetsova T. «New technique for data hiding in cover images using adaptively generated pseudorandom sequences». *CEUR Workshop Proceedings* Volume 2654, 2020, Pages 1-14.
14. Smirnov O., Kuznetsov A., Onikiychuk A., Makushenko T., Anisimova O., Arischenko A. «Adaptive pseudo-random sequence generation for spread spectrum image steganography». *2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020*. P. 161-165.
15. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». *2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020*. P. 172-177.
16. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) *Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies*, vol 48. Springer, Cham. 2021. pp 557-587.
17. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». *CEUR Workshop Proceedings* Volume 2616, 2020, Pages 366-379.
18. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», *CEUR Workshop Proceedings* Volume 2608, 2020, Pages 633-645.
19. Smirnov, O., Kuznetsov, A., Gorbacheva, L., Babenko, V., «Hiding data in images using a pseudo-random sequence», *CEUR Workshop Proceedings* Volume 2608, 2020, Pages 646-660.
20. Zhurakovskiy, B., Tsopa, N., Batrak, Y., Odarchenko, R., Smirnova, T «Comparative analysis of modern formats of lossy audio compression». *Workshop Proceedings*, 2020, 2654, стр. 315-327.
21. Smirnov O. Kuznetsov A., Zaichenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». *International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019; Odessa; Ukraine; 9-13 September 2019*. P.22-28.
22. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». *International Journal of Computing*; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.
23. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». *2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019* . P.517-522.
24. Smirnov, O., Krasnobayev, V., Yanko, A., Kuznetsova, T. «Methods of nulling numbers in the system of residual classes». *CEUR Workshop Proceedings*, Vol 2588, P. 90-106, 2019.
25. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Averchev, A., Pastukhov, M., Kuznetsova, K., «Formation of

- Pseudorandom Sequences with Special Correlation Properties», 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT -2019/ Lviv, Ukraine, 2-6 July, 2019, P. 395-399.
26. Smirnov, O., Kuznetsov, A., Kavun, S., Babenko, B., Nakisko, O., Kuznetsova, K., «Malware Correlation Monitoring in Computer Networks of Promising Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 347-352.
27. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Pastukhov, M., Kuznetsova, K., Prokopovych-Tkachenko, D., «Discrete Signals with Special Correlation Properties», CEUR Workshop Proceedings Volume 2353, CEUR Workshop Proceedings 2019, Pages 618-629.
28. Smirnov A.A., Kuznetsov A.A., Danilenko D.A., Berezovsky A., «The statistical analysis of a network traffic for the intrusion detection and prevention systems», Telecommunications and Radio Engineering. – Volume 74, Issue 1. – Begel House Inc. – 2015. – P. 61-78.
29. Smirnov O., Kuznetsov A., Kovalchuk D., Kuznetsova T. «New Technique for Hiding Data in Cover Images Using Adaptively Generated Pseudorandom Sequences». CEUR Workshop Proceedings Volume 2732, 2020, Pages 214-227.
30. Т.В. Смірнова, О.М. Дреєв, О.А. Смірнов «Хмарна інформаційна система оцінювання шорсткості з використанням дискретного частотного аналізу макрофотографій». IV міжнародна науково-практична конференція «Інформаційна безпека та комп'ютерні технології», м. Кропивницький. 15-16 квітня 2021р. – Кропивницький: ЦНТУ. – 2021. – С. 30.
31. О.А. Смірнов, П.С. Усік, «дослідження перспектив використання технологічних рішень в мережах 5g» у Кібербезпека та інформаційні технології: монографія. – Х. : ТОВ «ДІСА ПЛЮС», 2020.С. 122-135.
32. О.А.Смірнов, Т.В.Смірнова, Л.І. Поліщук, К.О. Буравченко, А.О.Макевнін, «Дослідження хмарних технологій як сервісів», Кібербезпека: освіта, наука, техніка. № 3(7). С. 43-62. 2020.
33. Смірнов О.А., Дреєва Г.М., Дреєв О.М., Смірнова Т.В. «Фрактальний аналіз генератора самоподібного трафіку на основі ланцюга Маркова». Центральнуукраїнський науковий вісник. Технічні науки. № 2(33). с. 161-172, 2019.

УДК 004

Д.Хуторний, магістр гр. КІ-24М,

Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ПІДВИЩЕННЯ НАДІЙНОСТІ ЗБЕРЕЖЕННЯ ІНФОРМАЦІЇ НА SSD ДИСКАХ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ RAID

У статті розроблено програмне забезпечення, яке призначено для системи підвищення надійності збереження інформації на SSD дисках з використанням технології RAID. Метою розробки є дослідження та принципи побудови системи підвищення надійності збереження інформації на SSD дисках з використанням технології RAID. Об'єктом дослідження є процес підвищення надійності збереження інформації на SSD дисках з використанням технології RAID. Предметом дослідження є методи підвищення надійності збереження інформації на SSD дисках з використанням технології RAID. Методи дослідження базуються на методах теорії зберігання даних, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи підвищення надійності збереження інформації на SSD дисках з використанням технології RAID. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

підвищення надійності, збереження інформації, SSD диски, RAID

Постановка проблеми. Сучасні комп'ютери, ноутбуки та мобільні пристрої використовують твердотільні накопичувачі (SSD), які є енергоефективними та швидкими! Оскільки SSD-накопичувачі не мають рухомих частин, вони також довговічніші, ніж технологія жорстких дисків у мобільних сценаріях.

Але SSD-сховища мають обмеження. Дві основні проблеми:

- Дані можна записати лише обмежену кількість разів.
- Дані не зберігаються надійно протягом тривалого часу, коли живлення вимкнено.

По суті, дані записуються на SSD-накопичувач у вигляді статичних зарядів в окремих комірках. Зазвичай ці комірки утримують заряд дуже довго, але сам процес заряджання комірки є руйнівним. Потрібна висока напруга, щоб послабити бар'єр комірки, перш ніж вона зможе зарядитися. І щоразу, коли записується в комірку, бар'єр постійно послаблюється. Зрештою, комірка не зможе надійно зберігати заряд.

Твердотільні накопичувачі вирішують цю проблему кількома способами. Одна з тактик – вирівнювання зносу, що означає, що дані зазвичай не записуються в одну й ту саму комірку. Накопичувач записує в нові комірки якомога частіше. Це вирівнює знос по всіх комірках. Інша стратегія, яку вони використовують, полягає у збереженні банку додаткових (прихованих) доступних комірок. Коли твердотільний накопичувач бачить, що комірка достатньо «погана», її місце займає одна з «резервних» комірок. Все це відбувається у фоновому режимі.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи підвищення надійності збереження інформації на SSD дисках з використанням технології RAID.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи підвищення надійності збереження інформації на SSD дисках з використанням технології RAID.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем підвищення надійності збереження інформації на SSD дисках з використанням технології RAID.

- Дослідження системи підвищення надійності збереження інформації на SSD дисках з використанням технології RAID.

- Програмна реалізація системи підвищення надійності збереження інформації на SSD дисках з використанням технології RAID.

Об'єктом дослідження є процес підвищення надійності збереження інформації на SSD дисках з використанням технології RAID.

Предметом дослідження є методи підвищення надійності збереження інформації на SSD дисках з використанням технології RAID.

Методи дослідження базуються на методах теорії зберігання даних, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Індустрія SSD-накопичувачів переживає свій найважливіший період. Те, що починалося як дорога розкіш для техноентузіастів, стало основою всього, від ігрових пристроїв до найбільших у світі центрів обробки даних. Оскільки ринок досяг 61,30 мільярда доларів у 2025 році та стрімко зростає до 129,62 мільярда доларів до 2030 року, ми спостерігаємо революцію в сфері зберігання даних, яка змінює наше уявлення про дані.

Почнемо з того, що всі хочуть знати: наскільки великим стає цей ринок? Численні дослідницькі фірми малюють однакову картину – вибухове зростання в кожному секторі. Mordor Intelligence прогнозує темпи зростання на рівні 16,16% на рік, тоді як інші аналітики ще більш оптимістичні, деякі прогнози сягають майже 280 мільярдів доларів до 2030 року.

Але ось що відрізняє цей період від попередніх технологічних бумів: не лише споживачі є рушійною силою зростання. Корпоративні клієнти лідирують, підживлюючись робочими навантаженнями штучного інтелекту, які просто не можуть функціонувати на традиційних жорстких дисках. Коли ви навчаєте наступний ChatGPT або обробляєте дані автономного транспортного засобу в режимі реального часу, кожна мілісекунда має значення.

Зміна настільки разюча, що навіть найбільш економічно свідомі компанії роблять цей стрибок. Чому? Тому що SSD-накопичувачі виходять з ладу лише з 0,5% порівняно з 5% для традиційних жорстких дисків. Коли прості коштують тисячі за хвилину, ця різниця в надійності стає очевидним бізнес-рішенням.

PCIe 5.0

Після років ажіотажу, 2025 рік – це час, коли PCIe 5.0 дійсно став вартим покупки. Ранні користувачі платили високі ціни за накопичувачі, які більшість систем не могли повноцінно використовувати, але масове впровадження знизило витрати, а програмне забезпечення наздогнало.

Ці накопичувачі можуть досягати швидкості 14 000 МБ/с – вдвічі більше, ніж PCIe 4.0 за хороших умов. Для геймерів це означає завантаження величезних відкритих світів за лічені секунди, а не за хвилини. Для професіоналів, які редагують відео 8K, це різниця між плавним відтворенням у реальному часі та постійними заїканнями.

Корпоративні клієнти також звертають на це увагу. Кіюхія постачає диски серії CM9 ємністю до 61,44 ТБ – цифри, які здавалися б неможливими ще кілька років тому. Тим часом, PCIe 6.0 залишається на горизонті до 2030 року, що вселяє компаніям впевненість у тому, що їхні інвестиції в PCIe 5.0 не застаріють за одну ніч.

Місткість стає смішною

Пам'ятаєте, коли диск на 1 ТБ здавався величезним? Корпоративні SSD-накопичувачі зараз зазвичай перевищують 100 ТБ, а деякі виробники досягають 512 ТБ за допомогою передової технології виправлення помилок. Це не просто маркетингові трюки – вони вирішують реальні проблеми для компаній, які тонуть у даних.

Секретний інгредієнт – технологія QLC (Quad-Level Cell), яка упаковує чотири біти в кожен комірку пам'яті. Ранні QLC-накопичувачі мали проблеми з довговічністю, але сучасні реалізації значною мірою вирішили ці проблеми, забезпечуючи потужність, яка вимагала б серверних кімнат, заповнених традиційними накопичувачами.

Продуктивність, яка дійсно має значення

Показники швидкості вражають, але реальні покращення продуктивності говорять краще. Сучасні SSD-накопичувачі забезпечують у 30 разів вищу продуктивність, ніж жорсткі диски, у завданнях, які дійсно важливі – час завантаження, запуск програм і передача файлів.

Збільшення енергоспоживання не менш різке. SSD-накопичувачі використовують 2-5 Вт проти 6-15 Вт для жорстких дисків. Це може здатися небагато для одного диска, але помножите це на тисячі серверів, і ви отримаєте серйозні гроші. Центри обробки даних спостерігають падіння рахунків за електроенергією, тоді як продуктивність стрімко зростає.

Хто що купує і чому

Підприємство лідирує

Корпоративні клієнти становлять 65% ринку SSD, і їхня частка щорічно зростає на 18,2%. Це не імпульсивні покупки – корпоративні покупці мають інші пріоритети, ніж споживачі. Їх цікавлять показники витривалості, гарантійні умови та стабільна продуктивність за високих робочих навантажень.

Значну частину цього попиту забезпечують програми штучного інтелекту. Навчання великих мовних моделей вимагає стабільної пропускної здатності даних, яку традиційні сховища просто не можуть забезпечити. Програмам периферійних обчислень потрібен мілісекундний час відгуку для автономних транспортних засобів та інфраструктури розумного міста.

Споживачі стають витонченими

Споживчий ринок може бути меншим, займаючи лише 35%, але він стає дедалі складнішим. Геймери розуміють різницю між PCIe 3.0 та 4.0. Творці контенту знають, що їм потрібне швидке сховище для безперебійного редагування 4K.

Для тих, хто хоче оновити старі системи з обмеженим бюджетом, традиційні накопичувачі SATA все ще мають сенс. Такі рішення, як 2,5-дюймовий SATA III SSD серії S330, пропонують значні покращення порівняно з жорсткими дисками, працюючи з існуючим обладнанням. Іноді найкращим оновленням є просто повна відмова від обертання дисків.

Регіональні відмінності мають значення

Азіатсько-Тихоокеанський регіон домінує з 45% часткою ринку, слугуючи як виробничим центром, так і зростаючою споживчою базою. Південна Корея, Китай та Японія контролюють виробництво, тоді як ринки, що розвиваються, стимулюють зростання впровадження.

Північна Америка становить 30% попиту, на чолі з постачальниками гіпермасштабних хмарних технологій та дослідницькими установами зі штучного інтелекту. Ці клієнти розширюють межі технологій та стимулюють інновації, які зрештою приносять користь усім.

Європа зосереджується на ефективності та відповідності вимогам, причому особливі переваги демонструє автомобільна та промислова галузі. Різні регіони мають різні пріоритети, але всі рухаються до більш продуктивного зберігання даних.

Реальні застосування, що стимулюють зростання

Центри обробки даних трансформують усе

Постачальники хмарних послуг поспішають замінити жорсткі диски, бо математика переконлива. SSD-накопичувачі забезпечують вищу щільність серверів, знижують витрати на охолодження та забезпечують стабільну продуктивність, з якою жорсткі диски просто не можуть зрівнятися.

Розрахунки рентабельності інвестицій прості: більшість підприємств бачать окупність протягом 18-24 місяців завдяки зниженню витрат на електроенергію, вищим коефіцієнтам

консолідації та покращенню продуктивності додатків. Якщо врахувати зниження рівня відмов та витрат на обслуговування, бізнес-кейс стає переконливим.

Штучний інтелект змінює правила гри

Штучний інтелект – це не просто чергове робоче навантаження, він принципово відрізняється. Навчання великих моделей вимагає постійної пропускну здатності даних, що перевищує 100 ГБ/с. Жорсткі диски розряджаються з набагато меншою швидкістю.

Застосування периферійних обчислень роблять вимоги ще суворішими. Автономні транспортні засоби потребують прийняття рішень у режимі реального часу на основі даних датчиків. Розумні фабрики вимагають миттєвого аналізу виробничих показників. Ці застосунки буквально не можуть функціонувати з традиційними затримками зберігання.

Ігри та створення контенту для дорослих

Технологія DirectStorage від Microsoft є прикладом того, як ігри розвиваються навколо можливостей SSD. Замість того, щоб розробляти ігри з урахуванням обмежень жорсткого диска, нові ігри передбачають швидке сховище та використовують його для реалізації ігрових механік, які раніше були неможливі.

Творцям контенту, які працюють з відео 4K та 8K, потрібен стабільний високошвидкісний доступ до величезних файлів. Сучасні SSD-накопичувачі дозволяють редагувати в режимі реального часу без використання проксі-серверів, що значно підвищує продуктивність творчих професіоналів.

Конкуренція на ринку загострюється

Конкурентне середовище характеризується тим, що відомі гравці борються за частку ринку, тоді як менші компанії знаходять нішеві можливості. Samsung зберігає лідерство завдяки вертикальній інтеграції та передовому виробництву. Western Digital використовує зв'язки з підприємствами та комплексні лінійки продуктів. Micron конкурує завдяки ефективності виробництва та стратегічним партнерствам.

Цікаво, як розвивається конкуренція. Чисто швидкісні війни поступаються місцем інтеграції програмного забезпечення, корпоративним функціям та спеціалізованим рішенням для конкретних застосувань. Компанії створюють комплексні екосистеми, а не просто продають пристрої зберігання даних.

Погляд у майбутнє: що далі до 2030 року

Технологічна дорожня карта

PCIe 5.0 домінуватиме протягом наступних кількох років, а PCIe 6.0 почне впроваджуватися підприємствами приблизно у 2030 році. Інтерфейси SATA залишаться для бюджетних застосувань та оновлення застарілих систем – не всім потрібна передова продуктивність.

Зростання ємності продовжує неупинний рух у бік 1PB SSD для спеціалізованих гіпермасштабованих застосувань. Але справжній акцент зміщується на стабільну продуктивність за різних робочих навантажень, а не лише на пікову пропускну здатність.

Новітні технології

Технології пам'яті наступного покоління, такі як 3D XPoint, можуть доповнювати флеш-пам'ять NAND для застосувань з наднизькою затримкою. Обчислювальні сховища – SSD-накопичувачі з інтегрованими можливостями обробки – можуть зменшити переміщення даних та підвищити ефективність системи.

Міркування щодо сталого розвитку стають дедалі важливішими. Енергоефективність, можливість переробки та екологічно чисті виробничі процеси впливають на рішення щодо проектування, оскільки зростає екологічна свідомість.

Інвестиційна стратегія для бізнесу

Розумні організації надають пріоритет інвестиціям в інфраструктуру PCIe 5.0 у 2025 році. Це забезпечує запас продуктивності в майбутньому, уникаючи при цьому преміальних витрат та обмеженої підтримки програмного забезпечення, характерних для найсучаснішого PCIe 6.0.

Планування потужностей має передбачати щорічне зростання на 20-30%, щоб врахувати зростаючі потреби в даних, особливо для робочих навантажень штучного інтелекту та аналітики. Але ключовим висновком є оцінка загальної вартості володіння, включаючи споживання енергії, обслуговування та переваги в продуктивності, а не лише витрати на придбання.

Підсумок

Ринок SSD-накопичувачів у 2025 році являє собою зрілу технологію, яка досягає нових висот продуктивності, одночасно розширюючись у застосування, які раніше були непомірно дорогими. Організації, які інвестують у сучасну інфраструктуру зберігання даних сьогодні, позиціонують себе для отримання стійких конкурентних переваг.

Ми спостерігаємо конвергенцію робочих навантажень штучного інтелекту, розширення хмарних обчислень та остаточний перехід від механічного зберігання даних. Це створює безпрецедентні можливості для компаній, готових впроваджувати технології зберігання даних наступного покоління.

Фокус змістився з базової заміни жорстких дисків на оптимізацію архітектур сховищ даних для нових робочих навантажень, які вимагають як величезної ємності, так і виняткової продуктивності. Успіх вимагає розуміння не лише поточних технологічних можливостей, але й стратегічних наслідків рішень щодо сховищ даних для довгострокової конкурентоспроможності бізнесу.

Незалежно від того, чи ви оновлюєте ігрову систему, плануєте корпоративну інфраструктуру чи створюєте наступне покоління додатків штучного інтелекту, основа сховища, яку ви оберете сьогодні, визначатиме можливості завтрашнього дня. Революція SSD не настає – вона вже тут, і вона змінює все.

Сьогодні навіть мілісекунди мають значення. Моргнуть, і ваш користувач йде до швидшого та витонченішого конкурента. Ми знаходимося на перетині, де продуктивність веб-сайту – це вже не просто жаргон серверної частини; це життєва сила користувацького досвіду, SEO та коефіцієнта конверсії. Повільні сайти дратують. Швидкі перемагають! Крапка. Якщо ви прагнете швидшої роботи сайту та кращої взаємодії користувача, SSD-хостинг – ваша секретна зброя.

На полі цифрової битви, якщо ви не оптимізуєте, ви просто зникаєте. Саме тут і вступає в гру SSD-накопичувач – розкішна необхідність. Це ваша секретна зброя для швидкого веб-хостингу, скорочення часу завантаження та покращення продуктивності веб-сайту. Користувачі навіть не відчують часу очікування. Погоджуйтеся чи ні, швидкість – це наша валюта. Тепер перейдемо до головного питання.

Що таке SSD-сховище у веб-хостингу?

Пам'ятаєте гудіння та клацання старих комп'ютерів? Це був звук жорстких дисків (HDD) – важких жорстких дисків, що оберталися, як крихітні вінілові платівки, відчайдушно намагаючись отримати ваші дані. Тепер же тиша (спокій)... і швидкість. Це SSD-накопичувачі – твердотільні накопичувачі – сучасне диво без рухомих частин, лише миттєвий доступ до ваших файлів, як перехід з рикші на швидкісний поїзд.

У світі веб-хостингу це не просто оновлення, це революція. SSD-накопичувачі у веб-хостингу означають, що ваш веб-сайт завантажується швидше, обробляє більше користувачів і рідше аварійно завершує роботу. Жорсткі диски були непогані, коли у нас було терпіння (і dial-up). Але в якому ми сьогодні? Користувачі відмовляються від доступу, якщо ваш сайт затримується навіть на 2 секунди. SSD-накопичувачі отримують доступ до даних миттєво, а це означає, що ваші зображення, скрипти та бази даних доставляються блискавично.

Хостинг на SSD – це вже не бонус, а виживання. У світі, залежному від миттєвого задоволення, повільне завантаження – це вірне цифрове самогубство.

SSD проти HDD у хостингу: технічне порівняння

Жорсткі диски (HDD) (накопичувачі вашого дідуся) використовують обертові магнітні диски та механічну ручку для читання/запису даних. Уявіть собі це як програвач

платівок. Механічний, ностальгічний... і болісно повільний. З іншого боку, SSD-накопичувачі – це круті дітища – без рухомих частин, лише чиста електронна магія, яка майже миттєво отримує доступ до даних. Як перемикач світла замість того, щоб чекати, поки закипить чайник.

Цифри? Жорсткі. SSD-накопичувачі можуть бути до 20 разів швидшими, зі значно меншою затримкою, надзвичайно високою кількістю операцій вводу/виводу за секунду (IOPS) та швидшим часом доступу до даних. Крім того, вони міцніші, відсутність рухомих частин означає менше збоїв, і вони енергоємні, на відміну від енергоємних жорстких дисків (знову ж таки, фу!).

У веб-хостингу це означає, що швидкість веб-сайту з SSD не просто помітна, а й змінює правила гри. Швидше завантаження сторінок, швидші виклики бази даних, плавніший користувацький досвід. Тим часом жорсткі диски вагаються, як сонний динозавр.

Досі дивуєтесь, чому SSD кращий за HDD для хостингу? Простіше кажучи: швидший час доступу, менше збоїв та неперевершена стабільність продуктивності в сценаріях з високим трафіком.

Тож так, обидва зберігають дані. Але один проноситься, як Flash, поки інший ще зав'язує шнурки. Вибирайте з розумом, або ризикуєте втратити відвідувачів ще до того, як ваша головна сторінка завантажиться.

Переваги SSD-хостинга для власників веб-сайтів

Перехід на SSD-хостинг – це не просто «приємна річ», це веб-еквівалент відмови від кінного воза на користь ракети. Ось чому власники сайтів усюди обирають цей варіант:

- Швидше завантаження веб-сайту. Якщо ви керуєте інтернет-магазином, переваги SSD-хостингу для веб-сайтів електронної комерції ще більш важливі. Кожна секунда, скорочена під час завантаження, може безпосередньо вплинути на ваші продажі. Швидкість – це головне, а SSD-сховище – головне.

- SSD проти HDD у хостингу. На відміну від старих жорстких дисків (HDD), які бавляться з даними, SSD-накопичувачі доставляють контент миттєво. На практиці? Ваш показник відмов падає, залученість зростає, а клієнти не йдуть, поки не завантажиться ваш логотип. Якщо вам потрібен швидкий веб-хостинг і така швидкість веб-сайту з SSD, що користувачі кажуть «Вау», це ваш шлях. Для електронної комерції, портфоліо або навіть того блогу про котів, який ви думаєте створити, швидкість має значення.

- Підвищена надійність та цілісність даних. Жорсткі диски мають рухомі частини, і знаєте що? Рухомі елементи зрештою виходять з ладу. SSD-накопичувачі, без механічних частин, схожі на цифрові танки: тихі, міцні та набагато рідше ламаються. Це означає кращий час безвідмовної роботи, менше помилок даних та більше спокою для вас. Якщо ваш сайт – це ваш бізнес, ви не можете дозволити собі збоїв. Одного збою забагато, а SSD-накопичувачі допомагають переконатися, що цього не станеться.

- Покращена SEO-продуктивність. У Google є одне правило: пришвидшуйся або відставай. Сайти на SSD завантажуються швидше, що подобається як користувачам, так і володарям пошукових систем. Швидкість завантаження сторінки – це відомий сигнал ранжування, і SSD допомагає вам впевнено поставити цю галочку. Якщо ви серйозно налаштовані піднятися в результатах пошуку, інвестування в SSD – це не просто варіант, це одна з найрозумніших переваг SSD-хостингу, яку ви можете використовувати. Швидке завантаження сторінок на SSD-хостингу також знижує показник відмов, що є ще одним непрямим посиленням SEO, особливо важливим для блогів, що розвиваються, та веб-сайтів малого бізнесу, які прагнуть піднятися в рейтингу:

- Менше споживання ресурсів та ефективність хостингу. SSD-накопичувачі не просто швидкі, вони ефективні. Ви обслуговуєте користувачів з меншим навантаженням на процесор, краще обробляєте трафік та швидше обробляєте дані. Платформи CMS, такі як WordPress, Magento та інші, процвітають у своїх SSD-середовищах. Це означає плавніше

кешування, швидші виклики бази даних та більшу віддачу від витрат на хостинг. Результат? Ви покращуєте продуктивність веб-сайту, не витрачаючи ресурси.

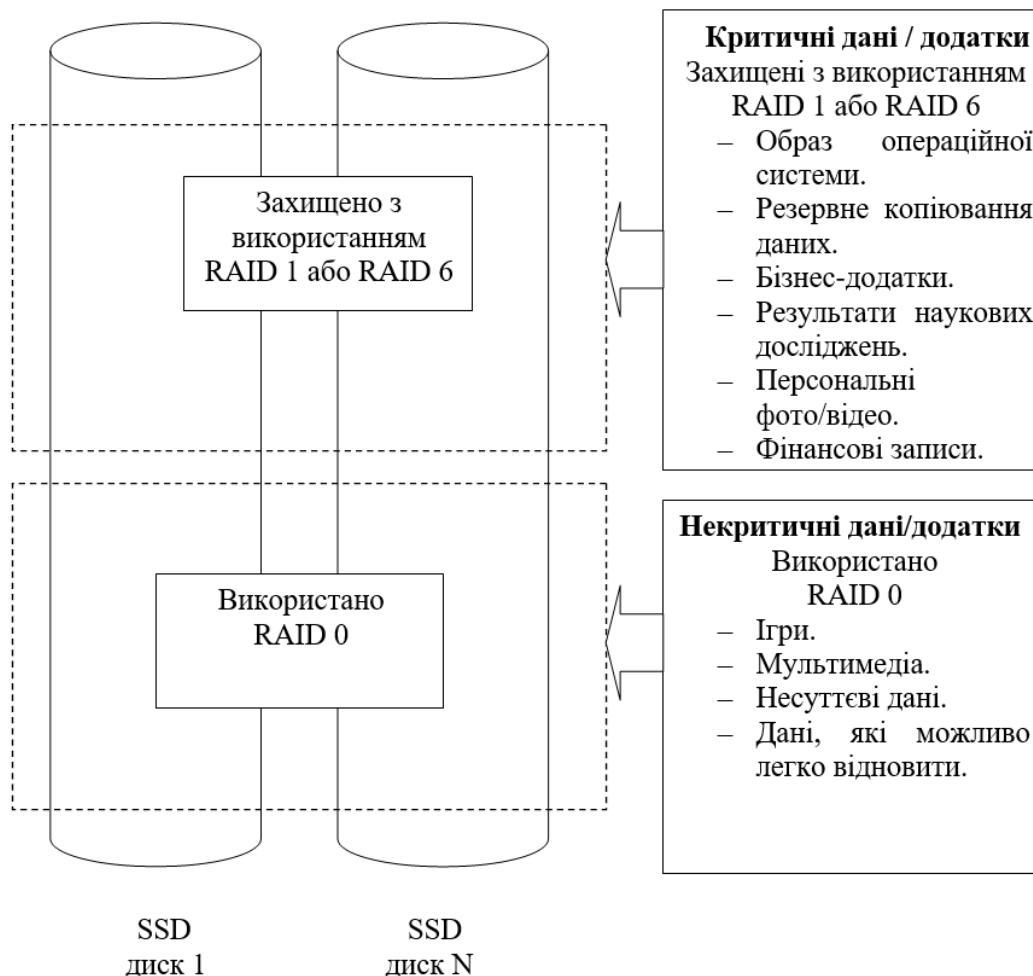


Рисунок 1 – Структурна схема розробленої системи

Структурна схема розробленої системи зображена на рисунку 1.

Реальні переваги продуктивності завдяки хостингу на SSD-дисках

Давайте на секунду відкинемо теорію та поговоримо про холодні, однозначні результати. Коли веб-сайти переходять на SSD-хостинг, різниця не є ледь помітною – вона вражає. Дослідження показують, що веб-сайти, розміщені на SSD-серверах, мають скорочення часу завантаження до 50%. Це вдвічі менше очікування, вдвічі більше задоволення. Уявіть, що ви скорочуєте час завантаження на 3 секунди з 6-секундного – тепер ви граєте у вищій лізі швидкого веб-хостингу.

Візьмемо, наприклад, WordPress. Це потужна CMS, але вона також багато працює з базами даних. На SSD-хостингу швидкість виконання запитів значно вища, що робить адміністративну панель більш адаптивною, а фронтенд – оперативнішим. Те саме стосується таких платформ, як Joomla, Magento або Drupal – SSD спрощує їх усі.

Чи то інтернет-магазин, який завантажує тисячі зображень товарів, чи блог зі стрімким зростанням трафіку, переваги SSD-хостинга очевидні: краща швидкість, кращий досвід та помітна перевага в сучасному інтернеті, де швидкість залежить від сайту.

Чому сайти електронної комерції потребують SSD-хостинга

Не кожному вебсайту потрібна прискорена швидкість, але якщо ви запускаєте щось серйозне, вам це точно потрібно.

– Вебсайти електронної комерції? Вони процвітають за рахунок швидкості, а повільне оформлення замовлення вбиває продажі.

– Сайти з високим навантаженням, завантажені зображеннями, відео або великим трафіком? SSD-накопичувачі з'їдають це навантаження на сніданок!

– SaaS-платформи чи недбалі стартапи? SSD-хостинг забезпечує продуктивність, швидкість та стійкість до збоїв, коли кількість користувачів раптово зростає.

Це ті самі поля битви, де продуктивність має найбільше значення, і SSD-накопичувачі чудово справляються з цим завданням. Якщо ви серйозно ставитеся до масштабування та хочете дійсно покращити продуктивність веб-сайту, переваги SSD-хостинга говорять самі за себе.

Як вибрати правильного постачальника SSD-хостингу

Вибір правильного SSD-сховища для веб-хостингу – це не просто вибір швидшого варіанту. Шукайте постачальника, який пропонує щедрі ліміти сховища, підтримку NVMe SSD (наступне покоління швидкісних SSD), стратегічно розташовані центри обробки даних та надійну гарантію безвідмовної роботи, адже навіть мілісекунда простою може дорого коштувати вашому бізнесу. Ретельно збалансуйте ціну та продуктивність; найдешевший варіант може заощадити копійки, але згодом погіршити продуктивність.

Не менш важливими є підтримка та масштабованість. Переконайтеся, що постачальник пропонує цілодобову технічну підтримку та інфраструктуру для зростання відповідно до потреб вашого бізнесу.

Майбутні тенденції: SSD-хостинг та розвиток Інтернету

Інтернет не сповільнюється, і ваш хостинг теж не повинен. Майбутнє явно схиляється до твердотільних накопичувачів на базі NVMe та PCIe, які пропонують блискавично високу швидкість передачі даних, що набагато перевищує традиційні твердотільні накопичувачі SATA. Зі зростанням хмарного хостингу та периферійних обчислень потреба у високошвидкісному сховищі з низькою затримкою стає критичною, і твердотільні накопичувачі є лідерами в цьому питанні.

У цій ситуації питання SSD проти HDD у хостингу вже навіть не обговорюється: HDD швидко стають пережитком минулого. Переваги SSD-хостингу – швидкість, масштабованість та ефективність – формують наступне покоління Інтернету. Будьте попереду або забудьте.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів підвищення надійності збереження інформації на SSD дисках з використанням технології RAID. Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем підвищення надійності збереження інформації на SSD дисках з використанням технології RAID.

– Досліджена система підвищення надійності збереження інформації на SSD дисках з використанням технології RAID.

– На основі отриманих результатів досліджень створена програмна реалізація системи підвищення надійності збереження інформації на SSD дисках з використанням технології RAID.

Розроблені алгоритми дозволяють успішно вирішувати завдання підвищення надійності збереження інформації на SSD дисках з використанням технології RAID. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Kuznetsov O., Frontoni E., Kuznetsova Y., Chevardin V., Smirnov O. «Architectural foundations for adaptive security in edge computing systems». Cybersecurity Defensive Walls in Edge Computing, 2025. pp. 21-61.
2. Вінтенко, Б.Ю., Миронець, І.В., Смірнов, О.А., Коваленко, О.В., Усік, П.С., Буравченко, К.О., Лисенко, І.А. «Логіко-структурна модель комп'ютерно-орієнтованої процедури системи підтримки оперативного персоналу АЕС». Кібербезпека: освіта, наука, техніка. 2025. Том 2 № 30. С. 413-427, 2025.

3. Смірнова, Т.В. «Дослідження методів, моделей та сучасних ІТ-рішень для підтримки технологічних процесів у критичній інфраструктурі держави». Кібербезпека: освіта, наука, техніка. 2025. Том 2 № 30. С.195-208, 2025.
4. Вінтенко Б., Смірнов О., Миронець І., Смірнова Т., Смірнов С. «Імітаційна модель шляхів вхідних даних комп'ютерної інтелектуальної системи підтримки оператора енергоблоку АЕС». Комбінаторні конфігурації та їхні застосування: Матеріали XXVII Міжнародного науково-практичного семінару, присвяченого 125-річчю Національного університету «Запорізька політехніка» (Запоріжжя-Кропивницький-Київ, 4-6 червня 2025 р.). Запоріжжя: НУ «Запорізька політехніка», 2025. С.82-91.
5. Al-Azzeh, J., Ayyoub, B., Mesleh, A., Smirnova, T., Gnatyuk, S., Drieiev, O., Smirnov, O., Dorenskyi, O. «Cloud-Based Information System for Evaluating Caverns in the Process of Blasting Metal Surfaces of Details». International Review on Modelling and Simulations 18 (1), 2025. pp. 32-42.
6. Вінтенко Б.Ю., Смірнов О.А., Миронець І.В., Смірнова Т.В., Коваленко О.В., Мацуї А.М. «Модель шляхів отримання вхідних даних комп'ютерної інтелектуальної системи підтримки оперативного персоналу АЕС». Центральнотраїнський науковий вісник. Технічні науки. 2025. Вип. 11(42), ч. II. С.52-62.
7. Вінтенко Б.Ю., Смірнов О.А., Миронець І.В., Смірнова Т.В. «Методи забезпечення відмовостійкості інтелектуальних систем підтримки оператора». VIII міжнародна науково-практична конференція «Інформаційна безпека та комп'ютерні технології», м. Кропивницький. 24-25 квітня 2025 р. – Кропивницький: ЦНТУ. – 2025. – С. 44-46.
8. Смірнов, О.А., Константинова, Л.В., Коноплицька-Слободенюк, О.К., Козірова, Н.В, Якименко, Н.М., Доренський, О.П., Буравченко, К.О. «Дослідження інструментів штучного інтелекту для роботи з базами даних та аналізу даних». Кібербезпека: освіта, наука, техніка. 2025. №3(27), С. 429–448.)
9. Smirnov O., Fedorov E., Neskoriadiya A., Neskoriadiya T. «Intellectual Classification method of Gymnastic Elements Based on Combinations of Descriptive and Generative Approache». CEUR Workshop Proceedings Volume 3664, 2024, Pages 11-23.
10. Вінтенко, Б., Миронець, І., Смірнов, О., Коваленко, А., Коноплицька-Слободенюк, О., Смірнова, Т., Константинова, Л. «Дослідження застосування систем підтримки оперативного персоналу об'єкту критичної інфраструктури при керуванні енергоблоком АЕС з реактором типу ВВЕР-1000». Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2024. № 2(26), С. 6-26.
11. Вінтенко, Б., Миронець, І., Смірнов, О., Кравчук, О., Козірова, Н., Савеленко, Г., Коваленко, А. «Дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». Кібербезпека: освіта, наука, техніка. 2024. №3(23), С. 111-131.
12. Kuznetsov O., Ilchenko O., Kryvinska N., Buravchenko K., Smirnov O., Savchenko Iu. «An Empirical Assessment of Leading Blockchain Financial Services». 2023 IEEE 1st Ukrainian Distributed Ledger Technology Forum (UADLTF), Kyiv, Ukraine, 2023, pp. 1-6,
13. Kuznetsov, O., Kryvinska, N., Ilchenko, O., Smirnova, T., Ulianova, Y. «Comparative Analysis of Cryptocurrency Trading Platforms Using the Analytic Hierarchy Process». CEUR Workshop Proceedings, 2023, 3628, pp. 106-115.
14. Malyukov V., Bebesko B., Lakhno V., Smirnov O., Malyukova I., Mohylnyi H. «Managing the Purchase-Sale Process of Digital Currencies Under Fuzzy Conditions». Lecture Notes in Networks and Systems, 2023, 729 LNNS, pp. 104–112.
15. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». Advanced Information Systems, 2023, 7(2), pp. 49-56.
16. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchey, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». CEUR Workshop Proceedings, Volume 3530, 2023, pp. 256-265.
17. Smirnov, O., Odarchenko, R., Smirnova, T., Bondar, S., Volosheniuk, D. «Optimal Structure Construction of Private 5G Network for the Needs of Enterprises». Lecture Notes on Data Engineering and Communications Technologies, 2023, 178, pp. 208–223.
18. Вінтенко Б.Ю., Смірнов О.А., Коваленко А.С., Смірнов С.А., Буравченко К.О. «Дослідження вимог міжнародних стандартів ІЕС60880 та ІЕС62138 з розробки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». Системи управління, навігації та зв'язку, 2023, вип. 3(73), С. 155-166.
19. Вінтенко, Б., Миронець, І., Смірнов, О., Кравчук, О., Козірова, Н., Савеленко, Г., Коваленко, А. «Дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». Кібербезпека: освіта, наука, техніка. 2024. №3(23), С. 111-131.
20. Вінтенко Б.Ю., Смірнов О.А., Коваленко О.В., Смірнов С.А., Коваленко А.С. «Дослідження нормативних документів та галузевих стандартів розробки програмного забезпечення комп'ютерних систем управління АЕС, важливих для безпеки». Системи управління, навігації та зв'язку, 2023, вип. 2(72), С. 170-178.
21. Аль-Мудхафар Акіл Абдулхуссейн М., Смірнова Т.В., Буравченко К.О., Смірнов О.А. «Метод оцінки та підвищення користувацького досвіду абонентів в програмно-конфігурованих мережах на основі використання машинного навчання». Сучасні інформаційні системи, 2023, том 7, № 2, С. 49-56.
22. Вінтенко Б.Ю., Смірнов О.А., Коваленко О.В., Смірнов С.А. «Дослідження нормативної документації та

- стандартів розробки програмного забезпечення комп'ютерних систем управління АЕС, важливих для безпеки». VI міжнародна науково-практична конференція "Інформаційна безпека та комп'ютерні технології", м. Кропивницький. 20-21 квітня 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 35-36.
23. Smirnov, O., Karapetyan, A., Fedorov, E., «Creating Neural Network and Single Solution Human-Based Metaheuristic Methods of Solving the Traveling Salesman Problem». CEUR Workshop Proceedings, Volume 3312, 2022, pp. 47-58.
24. Smirnov O., Kuznetsov A., Kryvinska N., Kiian A., Kuznetsova K. «Full Non-Binary Constant-Weight Codes». SN Computer Science, Vol 2, 337, 2021. <https://doi.org/10.1007/s42979-021-00739-w>.
25. Smirnov O., Kovalenko O., Kovalenko A., Kavun S. «Quantitative Risk Assessment Method Development in the Context of the SDLC-model». 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), 2021, pp. 203-208, doi: 10.1109/PICST54195.2021.9772143
26. Smirnova T., Gnatyuk S., Berdibayev R., Avkurova Zh., Iavich M. «Cloud-Based Cyber Incidents Response System and Software Tools». Communications in Computer and Information Science, 2021, vol 1486. Springer, Cham. pp 169-184.
27. Smirnov, O., Kuznetsov, A., Potii, O., Poluyanenko, N., Stelnyk, I., Mialkovsky, D. «Combining and filtering functions in the framework of nonlinear-feedback shift register». International Journal of Computing; 2020, Volume 19, Issue 2 – Research Institute for Intelligent Computer Systems – 2020. – P. 247-256.
28. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
29. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177.
30. Smirnov, O., Shekhanin, K., Kuznetsov, A., Krasnobayev, V. «Detecting Hidden Information in FAT». International Journal of Computer Network and Information Security (IJCNIS). Vol. 12, No. 3, 2020. PP.33-43.
31. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645.
32. Smirnov O. Kuznetsov A., Zaichenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019; Odessa; Ukraine; 9-13 September 2019. P.22-28.

УДК 004

М.Черкашин, магістр гр. КН-24М,*Центральноукраїнський національний технічний університет*

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ НАДАННЯ ХМАРНИХ ПОСЛУГ НА БАЗІ CISCO HYPERFLEX

У статті розроблено програмне забезпечення, яке призначено для системи надання хмарних послуг на базі Cisco HyperFlex. Метою розробки є дослідження та принципи побудови системи надання хмарних послуг на базі Cisco HyperFlex. Об'єктом дослідження є процес надання хмарних послуг на базі Cisco HyperFlex. Предметом дослідження є методи надання хмарних послуг на базі Cisco HyperFlex. Методи дослідження базуються на методах теорії побудови комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи надання хмарних послуг на базі Cisco HyperFlex. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

хмарні послуги, Cisco HyperFlex

Постановка проблеми. Під конвергентною ІТ-інфраструктурою розуміють системи, у яких обчислювальні потужності, мережні ресурси й сховища даних максимально уніфіковані й консолідовані в рамках рішення, що звичайно складає із продуктів декількох виробників. Гіперконвергентні системи продовжують курс на об'єднання ІТ-ресурсів у цілісне рішення. Даний підхід припускає об'єднання використовуваних ресурсів за допомогою типових апаратних блоків і програмно обумовлених засобів. Головним драйвером появи гіперконвергентних рішень стало прагнення замовників заощадити за рахунок відмови від дорогих традиційних (виділених) систем зберігання даних і мереж SAN.

Продукти Cisco HyperFlex побудовані на основі серверів Cisco UCS, до яких додана платформа NX Data. Остання поєднує твердотільні й дискові накопичувачі в єдине розподілене багаторівневе об'єктне сховище даних. HyperFlex підтримує широкий діапазон застосунків і робочих навантажень для ЦОДів. Крім середовищ VMware, також передбачена підтримка інших гіпервізорів, пристроїв bare metal і контейнерних середовищ. При розгортанні HyperFlex рекомендується встановлювати як мінімум тривузловий кластер для забезпечення високої доступності з реплікацією даних принаймні між двома вузлами. Третій вузол додатково підвищує надійність системи у випадку виходу з ладу одного з наявних вузлів.

Рішення HyperCloud дозволяє створювати публічні, гібридні й приватні хмари, а також ефективно зв'язувати їхній одну з одною і із уже існуючої ІТ-інфраструктурою за виділеними каналами або через Інтернет. Оскільки апаратна частина рішення HyperCloud представлена у вигляді готових типових блоків від одного виробника, істотно скорочуються часові витрати на розгортання хмарних систем і наступне збільшення їхньої потужності.

Завдяки тому, що гіперконвергентні системи HyperFlex поєднують обчислювальні, мережні потужності й ресурси зберігання в повністю інтегрованій платформі, її використання дозволяє знизити витрати на розгортання й експлуатацію рішення. Для керування серверними ресурсами й сховищами даних досить одного системного адміністратора замість цілої команди ІТ-фахівців.

Сервіс HyperCloud розгорнуть на основі гібридних систем і систем тільки із твердотільними накопичувачами (all-flash). За результатами тестів така конфігурація показала себе більше продуктивною, ніж гіперконвергентні рішення інших вендорів. У рамках тестів, у яких випробовувалися чотири гіперконвергентних рішення різних постачальників,

Cisco HyperFlex показав практично восьмикратну перевагу за значеннями операцій вводу-виводу в секунду при середньому часі реагування 2,46 мс.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи надання хмарних послуг на базі Cisco Hyperflex.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи надання хмарних послуг на базі Cisco HyperFlex.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем надання хмарних послуг на базі Cisco HyperFlex.
- Дослідження системи надання хмарних послуг на базі Cisco HyperFlex.
- Програмна реалізація системи надання хмарних послуг на базі Cisco HyperFlex.

Об'єктом дослідження є процес надання хмарних послуг на базі Cisco HyperFlex.

Предметом дослідження є методи надання хмарних послуг на базі Cisco HyperFlex.

Методи дослідження базуються на методах теорії побудови комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Система Cisco HyperFlex надає готове гіперконвергентне рішення, що поєднує програмно-визначаєму мережу й обчислення із платформою даних Cisco HX нового покоління. В основі цієї системи – платформа Cisco UCS. Cisco HyperFlex робить робочі процеси ефективніше й підвищує адаптивність вашого ЦОД, розкриваючи потенціал гіперконвергентної інфраструктури.

Гнучкість

Ми пропонуємо повністю настроєне комплексне рішення для впровадження цифрових технологій у вашій компанії.

Ми сполучимо програмно-визначаємі обчислення із системою Cisco UCS®. Це стосується процесорів Intel® Xeon®, програмно-визначаємих систем зберігання даних і платформи Cisco HyperFlex HX™, програмного забезпечення, програмно-визначаємих мереж і уніфікованої фабрики комутації Cisco®. Крім того, здійснюється інтеграція в архітектуру Cisco (Cisco ACI™), орієнтовану на застосунки.

Ефективність

Оптимальна інфраструктура для ваших даних і повна відповідність її можливостей потребам ваших застосунків. Ви можете почати з малого й легко масштабувати систему в міру росту потреб.

Можливість налаштування

Вибирайте найкраще співвідношення ресурсів ЦП і дискового простору для ваших застосунків. Розширте коло використовуваних застосунків і робочих моделей.

Таблиця 1 – Моделі й технічні характеристики

	Cisco HyperFlex HX220c M4 All Flash Node	Cisco HyperFlex HX240c M4 All Flash Node	Cisco HyperFlex HX220c M4 Node	Cisco HyperFlex HX240c M4 Node
Фокус	Висока продуктивність для критично важливих застосунків	Швидкість і висока ємність для максимальної ефективності	Проста система для невеликих проєктів	Максимальна ємність для ваших застосунків
Розмір блоку	1 rack unit	2 rack units	1 rack unit	2 rack units
Ємність блоку	1 x 400 GB SAS SSD 6 x 3.8 TB / 960 GB SDDs	1 x 400 GB SAS SSD 10 x 3.8 TB / 960 GB SDDs	1 x 480 GB SSD 6 x 1.2 TB HDDs	1 x 1.6 TB SSD 23 x 1.2 TB HDDs

Обчислювальна потужність	До 2 процесорів на вузол	До 2 процесорів на вузол	До 2 процесорів на вузол	До 2 процесорів на вузол
Масштабування	Незалежне для обчислювальних потужностей і системи зберігання	Незалежне для обчислювальних потужностей і системи зберігання	Незалежне для обчислювальних потужностей і системи зберігання	Незалежне для обчислювальних потужностей і системи зберігання

У даному розділі представлені результати перевірки й тестування продуктивності гіперконвергентної інфраструктури Cisco HyperFlex, у ході чого було проведене порівняння гібридного рішення й рішення all-flash Cisco HyperFlex з рішеннями по гіперконвергентній інфраструктурі (HCI) анонімних конкурентів.

Загальні відомості

Сьогодні організації повинні бути надзвичайно гнучкими, щоб мати можливість швидко додавати застосунки й віртуальні машини (VM) і задовольняти стрімко мінливі потреби бізнесу. В умовах розрізнених обчислювальних, мережних ресурсів і ресурсів зберігання, які статичні й вимагають індивідуального керування, зробити це досить складно. От чому гіперконвергентні інфраструктури (HCI) стають усе більше популярними. Рішення HCI – це єдиний модуль із програмно-визначаємих обчислювальними, мережними ресурсами й ресурсами зберігання, керованими централізовано, що забезпечує гнучкість, масштабованість і простоту розгортання.

Дослідження підтверджують популярність рішень HCI: в останнім дослідженні 85% респондентів сказали про те, що вони вже використовують або планують почати використовувати рішення HCI у найближчі місяці. Це не дивно, якщо докладніше розглянути фактори, що мотивують їх до переходу на рішення HCI. Розгортання або оцінки можливості розгортання гіперконвергентних рішень в організаціях сприяв цілий ряд переваг цих рішень: поліпшене обслуговування й підтримка, масштабованість, оперативна ініціалізація VM, передбачувані витрати, спрощене керування, швидке розгортання, краща загальна вартість володіння (TCO), менше число проблем із взаємосумісністю й простота придбання. Все це звучить занадто добре, щоб бути правдою.

У більшості випадків це дійсно занадто добре, щоб бути правдою. По-перше, тому що перше покоління рішень HCI, у яких використовувалося ПЗ на звичайних серверах x86, було орієнтовано в основному на простоту й швидкість проникнення на ринок. Але в процесі цього доводилося жертвувати такими істотними функціями, так необхідними сьогодні для забезпечення адаптивності й швидкості, як мережна автоматизація, незалежне масштабування ресурсів і висока продуктивність. Крім того, у перших рішеннях часто зберігалися розрізнені функції керування, що значно знижувало переваги, пов'язані із простим керуванням. Деякі організації не хотіли впроваджувати рішення HCI ще по одній причині – більшість із них не могли забезпечити постійно високу продуктивність, що потрібно робочим навантаженням, критично важливим для бізнесу. Простота більше не є єдиним пріоритетом; ніж більше рішень HCI з'являється на ринку, тим частіше ключовим критерієм для покупки стає критерій продуктивності.

Cisco HyperFlex

Системи Cisco HyperFlex поєднують обчислювальні, мережні потужності й потужності зберігання в повністю інтегрованій, інженерній платформі, розробленій для незалежного масштабування ресурсів і забезпечення постійно високої продуктивності. Рішення Cisco HyperFlex засноване на платформі Cisco UCS і сполучить переваги UCS (такі як автоматизація серверів і мереж на основі політик) з перевагами розподіленої файлової системи для гіперконвергенції платформи HX Data. Рішення підтримує широкий діапазон застосунків і робочих навантажень для ЦОД і віддалених площадок. У даний момент підтримуються середовища VMware, а також у дорожній карті передбачена підтримка інших гіпервізорів і «чистих» (bare metal) і контейнерних середовищ. Для розгортання HyperFlex

необхідний мінімум тривузловий кластер для забезпечення високої доступності з реплікацією даних мінімум на двох вузлах, а третій вузол підвищує надійність на випадок виходу з ладу одного з вузлів.

Вузли HyperFlex серії HX працюють на процесорах Intel Xeon і складаються з наступних компонентів:

- Сервери Cisco UCS. У кластер можна поєднувати й блейд-сервера, і стійкові сервера, з єдиною крапкою комутації між будь-якими двома вузлами для максимальної пропускної здатності в горизонтальному напрямку («схід-захід») і низької затримки. HyperFlex дозволяє змінювати співвідношення між блейд-серверами з інтенсивним навантаженням ЦП вузлами зберігання з інтенсивним навантаженням системи зберігання, щоб користувачі могли оптимізувати систему відповідно до потреб застосунків. Доступні вузли All-flash і гібридні вузли. Доступ у керуванню UCS реалізований через програмний модуль VMware vCenter, веб-інтерфейс GUI, інтерфейс командного рядка CLI або XML API-інтерфейс.

- Платформа даних Cisco HyperFlex HX для програмно-визначаємої системи зберігання. Платформа даних HX функціонує на кожному вузлі як контролер і забезпечує високу продуктивність, являючи собою розподілену файлову систему, що поєднує всю ємність дисків SSD і HDD по всьому кластері в розподілене, багаторівневе об'єктно-орієнтоване сховище даних з рівномірним чергуванням даних на дисках у кластері. Платформа також надає такі корпоративні сервіси обробки даних, такі як миттєві знімки, динамічна ініціалізація й миттєве клонування. Реплікація даних у кластері на основі політик забезпечує високу доступність. Динамічне розміщення даних у пам'яті, кешовані й рівні ємності дозволяють оптимізувати продуктивність застосунків, тоді як завжди активні, інтегровані функції дедуплікації й стиску оптимізують використовуваний дисковий простір.

- Платформа даних HX Data обробляє всі запити на читання й запис для томів, доступних гіпервізору. Рівномірний розподіл даних по кластері дозволяє обходити проблемні ділянки мережі й системи зберігання й забезпечити оптимальну продуктивність вводу/виводу ВМ незалежно від місця розташування. Записи здійснюються на локальний SSD-накопичувач (кеш-пам'ять) і реплікуються на віддалений SSD-накопичувач паралельно до підтвердження запису. Читання здійснюється, при можливості, з локального SSD-накопичувача, або, якщо такої можливості ні, з віддаленого.

- Файлова система зі структурою журналів являє собою сховище об'єктів, що використовує SSD-кеш для прискорення читання й запису, з постійним зберіганням даних на HDD-дисках (гібридна модель) або більших SSD-накопичувачах (all-flash модель). Дані переносяться на рівень постійного зберігання однією послідовною операцією, що записує великий обсяг даних, збільшує продуктивність. При перенесенні даних з їхнім видаленням відбувається оперативна дедуплікація й стиск; переміщення даних відбувається після підтвердження їхнього запису, тому це ніяк не позначається на продуктивності.

- Уніфікована фабрика Cisco/центральні пристрої (Fabric Interconnects) UCS 6200 забезпечують підтримку програмно-визначаємих мереж. Висока пропускна здатність, низька затримка й можливість підключення на швидкостях 40 Гбіт/с і 10 Гбіт/с у цій фабриці забезпечують високу доступність, тому що дані безпечно розподіляються й реплікуються по всьому кластері. Мережа легко масштабується, і забезпечується безпека кожного підключення. Архітектура єдиної крапки комутації збільшує продуктивність кластера.

- Інфраструктура Cisco, орієнтована на застосунки (ACI) для автоматичної ініціалізації. Архітектура ACI забезпечує автоматичне розгортання мережі, сервісів застосунків, політик безпеки й розміщення робочих навантажень відповідно до певних сервісних профілів. У такий спосіб гарантується більше точне, надійне розгортання з меншими витратами. ACI автоматично маршрутизує трафік для оптимізації продуктивності й використання ресурсів, а також перенаправляє трафік в обхід проблемних ділянок для забезпечення оптимальної продуктивності.

– VMware ESXi і vCenter. Рішення поставляється із уже встановленими гіпервізором VMware і додатком для керування, зі знайомим користувачеві інтерфейсом керування програмним і апаратним забезпеченням. Рішення Cisco HyperFlex надає безліч переваг, включаючи наступні:

– Висока продуктивність. Крім уже згаданих вище функцій підвищення продуктивності рішення HyperFlex надійно й безпечно розподіляє дані по серверах і сховищу в кластер для зменшення вузьких місць.

– Швидке, просте розгортання. Попередньо убудований кластер можна розгорнути відразу, підключившись у мережу й включивши живлення. Конфігурація вузла і його підключення відбувається через сервісні профілі Cisco UCS. По відомостях Cisco замовники говорять про те, що звичайно розгортання займає не більше години.

– Консолідоване керування. Моніторинг і керування системами здійснюється через VMware vCenter, що усуває необхідність в окремих модулях керування обчисленням і зберіганням. Дані ініціалізації, клонування й миттєві знімки вивантажуються в vSphere з використанням VAAI. API-інтерфейси підтримують хмарні типи даних.

– Незалежне масштабування. На відміну від інших HCI-систем, HyperFlex може незалежно масштабувати ресурси обчислення й зберігання, додаючи або забираючи або сервери або окремі диски; дані автоматично балансуються. У такий спосіб забезпечуються необхідні ресурси відповідно до різних потреб застосунків; відпадає необхідність у масштабуванні з попередньо заданим кроком збільшення.

Тестування

Тестування було проведено з використанням стандартних галузевих інструментів і методологій і його метою було порівняння продуктивності гібридного рішення й рішення all-flash HyperFlex із продуктивністю неназваних альтернативних рішень. Ці рішення містили в собі дві «тільки програмні» системи від провідних постачальників, які використовували стандартні x 86-сервери, а також пропріетарну систему одного постачальника, розроблену їм на базі власного апаратного забезпечення, що включає деяку частину власного програмного забезпечення. У більшій частині тестів використовувався інструмент HCIBench – інструмент на основі галузевих стандартів, розроблений для тестування продуктивності кластерів HCI, що виконуються на віртуальних машинах. Інструмент HCIBench використовує засіб Oracle Vdbench і дозволяє автоматизувати весь процес, від початку до кінця, включаючи розгортання тестових ВМ, координування виконання робочих навантажень, підсумовування результатів тестування й збір даних.

Таке розширене дослідження було виконано з використанням строгої методології, що включає тестування базових характеристик і ітеративне тестування протягом декількох місяців. Одержати гарні результати тестування продуктивності завжди простіше, проводячи короткі тести, тому порівняльні тести виконувалися протягом довгого часу, щоб мати можливість спостерігати за продуктивністю і її змінами в середовищі замовника. Крім того, тести виконувалися багато разів і ніколи не проводилися відразу один за іншим, а із проміжком у кілька годин і днів, щоб одержати результати в середньому. У такий спосіб ми могли одержати більше достовірні результати за рахунок зниження можливих випадкових факторів. Крім того, тестування проводилося з використанням досить більших наборів даних, щоб гарантувати, що дані не залишаються в кеші, і буде використаний внутрішній диск у кожному кластері.

Тестування гібридних систем

Тестування гібридних систем включає обидва диски – SSD і HDD. Тестування гібридної системи охоплює чотирьохвузловий кластер HyperFlex HX220c з одним твердотільним накопичувачем SSD на 480 Гбайт для кеш-пам'яті й шістьма жорсткими дисками SAS HDD на 1,2 Тбайт для ємності. Тести проводилися на 140 ВМ (35 ВМ на вузол), кожна з 4-ма віртуальними ЦП, оперативною пам'яттю RAM 4 Гбайт, одним диском 20 Гбайт і під керуванням ОС RHEL версії 7.2. Розмір робочого набору становив 2,8 Тбайт. Тести

проводилися мінімум у плинні години, з п'ятихвилинною підготовкою перед кожним тестом і мінімум годинною перервою між тестами.

Рішення HCI конкурентів також являли собою чотирьохвузлові системи в корпусі 2U схожої конфігурації, що відрізнялася лише тим, що в них використовувалися два SSD-кешу, тоді як у рішенні HyperFlex використовується тільки один. Постачальник А використовував два SSD-накопичувачі на 400 Гбайт і чотири жорсткі диски SATA HDD на 1 Тбайт; постачальник В використовував два SSD-накопичувачі на 400 Гбайт і 12 жорстких дисків SAS HDD на 1,2 Тбайт; постачальник С використовував чотири SSD-накопичувачі на 480 Гбайт і 12 жорстких дисків SAS HDD на 900 Гбайт.

Тестування було виконано з використання різних профілів читання/запису й розмірів блоку, з 100 %-але випадковими даними. По своїй природі віртуальні машини генерують випадкові дані вводу/виводу, поєднуючи дані вводу/виводу з різних застосунків і робочих навантажень. Компанія приділяла основну увагу результатам, отриманим з використанням робочих навантажень, призначених для моделювання застосунків у реальних умов, такі як OLTP і SQL-сервер, 4 кбайт і 8 кбайт.

По-перше, оцінила загальну масштабованість кластера. Тест почався з імітуемого робочого навантаження, створеної для емуляції типових змішаних даних вводу виводу OLTP I/O, 70 % читання, 100 % випадкових даних із цільовим показником 800 операцій вводу/виводу в секунду (IOPS) на ВМ. Тест проводився на 140 віртуальних машинах (ВМ) у кожному кластері протягом трьох-чотирьох годин, при цьому метою було залишитися на значенні затримки запису в 5 мс або нижче. HyperFlex стала єдиною платформою, що змогла виконати цей тест для всіх 140 ВМ і залишитися при цьому на значенні 5 мс (4,95 мс). Для кожного з інших кластерів тест виконувався знову й знову для меншого числа віртуальних машин доти, поки не була досягнута затримка запису в 5 мс. Постачальник А успішно пройшов випробування для 70 ВМ із середньому часом реагування 4,65 мс; середній час реагування постачальника В склало 5,37 мс для 36 ВМ, а постачальник С зміг забезпечити підтримку 48 ВМ із часом реагування 5,02 мс

Потім вивчила таке ж імітуєме робоче навантаження по 140 віртуальних машинах, щоб виміряти затримку кожного кластера щодо значення IOPS. Як видно на рисунку 4, кластер Cisco HyperFlex більш ніж удвічі перевершує значення IOPS постачальника А і підтримує майже у вісім разів більше значення IOPS постачальника В и постачальника Із із середнім часом реагування 2,46 мс. Для порівняння: середній час реагування постачальника А – 6,61 мс, постачальника В – 21,88 мс і постачальника С – найбільше – 44,45 мс

Далі досліджувала імітуєме робоче навантаження, призначену для моделювання зразків вводу/виводу SQL-сервера.4 Для створення імітуемого робочого навантаження, у якій задіяні різні розміри передачі й співвідношення читання/запису, застосовувався інструмент Vdbench. У профілі Vdbench коефіцієнт дедуплікації був установлений на 2 з розміром одиниці 4 Кбайт і коефіцієнтом стиску також рівним 2. І знову тест був проведений на 140 віртуальних машинах.

Показано, що значення IOPS кластера Cisco HyperFlex майже вдвічі перевершує це значення обох постачальників А и В і більш ніж в 5 разів більше, ніж значення IOPS постачальника С. Cisco HyperFlex показав середній час реагування рівне 8,2мс. Для порівняння: середній час реагування постачальника А – 30,6 мс, постачальника В – 12,8 мс і постачальника С – 10,33 мс.

Тестування All-flash

ESG Lab також досліджувала продуктивність конфігурацій all-flash рішень Cisco HyperFlex і постачальника В, програмного рішення HCI на стійкових серверах Cisco C240 M4. Тестування All-flash виконувалося для чотирьохвузлового кластера Cisco HyperFlex 220С з одним SSD-накопичувачем на 400 Гбайт і шістьма SSD-накопичувачами на 960 Гбайт. Кластер, з яким проводилося порівняння, також мав чотири вузли, але у два рази більше кешу – два SSD-накопичувачі по 400 Гбайт і теж шести SSD-накопичувачів по 960

Гбайт. Важливо відзначити, що система постачальника В була сконфігурована з такими ж характеристиками ЦП і пам'яті, що й кластер Cisco HyperFlex 220С.

У тестуванні знову брали участь 140 ВМ на кластер (35 на вузол). Кожна ВМ, під керуванням RHEL 7.2, задіяла чотири віртуальних ЦП, оперативну пам'ять 4 Гбайт і локальний диск 16 Гбайт, а також один неопрацьований диск 40 Гбайт. Робочий набір мав розмір 5,6 Тбайт, результати вводу/виводу були на 100 % випадковими; тести виконувалися з п'ятихвилинною підготовкою, тест тривала одна година, потім між тестами була перерва на годину. Якщо на практиці функції дедуплікації й стиску в кластері Cisco HyperFlex завжди активні, то при тестуванні порівняння з постачальником У проводилося, коли функції дедуплікації й стиску були встановлені на 50 %, а потім взагалі відключені. Кластер Cisco HyperFlex забезпечує більше значення IOPS з меншою затримкою, ніж у постачальника В, із включеною або виключеною дедуплікацією.

Далі досліджувала імітуєме робоче навантаження, призначену для моделювання результатів вводу/виводу SQL-сервера для конфігурацій all-flash Cisco HyperFlex і постачальника В. Для створення імітуємого робочого навантаження, що використовує різні розміри передачі й співвідношення читання/запису, застосовувався інструмент Vdbench. У профілі Vdbench коефіцієнт дедуплікації був установлений на 2 з розміром одиниці 4 Кбайт і коефіцієнтом стиску також рівним 2.

Значення IOPS кластера Cisco HyperFlex більш ніж у три рази перевершує значення IOPS постачальника В із середнім часом реагування 5,3 мс. Середній час реагування постачальника В склало 30,58 мс, що було пов'язане з винятково високим часом реагування запису 99,84 мс протягом усього тесту. Цей тест проводився кілька разів у різні дні й давав несуттєві результати.

Під час тестування all-flash було зроблено цікаве спостереження. Продуктивність постачальника В значно мінялася залежно від ВМ. Цей тест проводився з використанням інструмента HSBench для 140 ВМ у кожному кластері. Якщо Cisco HyperFlex показав зовсім невелику варіативність по всіх 140 ВМ – значення IOPS залишалися дуже близько до 600, то число операцій вводу/виводу в секунду (IOPS) постачальника В мінялося значно, від найнижчого (64) до найвищого (1024).

Важливо відзначити, що така варіативність спостерігалася в кожній ітерації тестування, і що в ході цих тестів, виконуваних на кожному із кластерів, параметри якості обслуговування (QoS) сховища не були використані ні в якій формі. Для обох систем використовувалася якість обслуговування (QoS) мережі. Така непогодженість може стати достатньою проблемою для адміністраторів, яким імовірно прийде скористатися якістю обслуговування QoS у якій би те не було формі (якщо це доступно в постачальника HSI), щоб постаратися проконтролювати ті ВМ, які споживають більше, ніж їм потрібно, відбираючи тим самим ресурси в інших.

Продуктивність дискової підсистеми – це стандартна проблема HSI-систем, з якої зіштовхувалися все. Замовники HSI-систем більше цікавилися економічною ефективністю й простотою керування, найчастіше зводячи роботу HSI-системи тільки до робочих навантажень другого рівня. Малоімовірно, що IT-Відділи проміняють виробничі застосунки першого рівня на нестабільну продуктивність із високою затримкою «гучних сусідів», віртуальних машин, пропоновану окремими рішеннями HSI.

По оцінках гібридні й all-flash системи Cisco HyperFlex забезпечують більше високу й стабільну продуктивність, ніж інші аналогічним образом сконфігуровані рішення HSI, що використовують змодельовані робочі навантаження OLTP і SQL. У тому що стосується гібридних кластерів, HyperFlex не тільки завжди обходить конкурентів по характеристиках операцій вводу/виводу в секунду (IOPS) і часу затримки, але й по числу підтримуваних ВМ (у два рази більше), ніж в обох систем – програмної й власної розробки – з незмінно високою продуктивністю. Кластер all-flash рішення HyperFlex з активними функціями дедуплікації й стиску, забезпечує більше високе значення IOPS і більше низький час затримки, ніж у конкурента із включеною або відключеною функцією скорочення обсягу даних.

Немаловажну роль грає факт, що продуктивність кластера all-flash рішення HyperFlex була стабільно високої по всім ВМ у кластері, усуваючи необхідність у застосуванні QoS для сховища, щоб гарантувати задоволеність користувача. І навпаки, окремі ВМ у кластері конкурента характеризувалися винятково великою різницею в значеннях IOPS, коли одні ВМ працювали з набагато більшою продуктивністю, ніж інші.

Основні результати тестування:

- Вразила можливість підтримки гібридним кластером HyperFlex у два рази більшого числа ВМ, ніж у його конкурентів, забезпечуючи при цьому низьку затримку й від двох до восьми разів більше значення IOPS для 140 ВМ у кластері з використанням робочого навантаження OLTP.

- З робочим навантаженням SQL гібридне рішення HyperFlex також забезпечувало значно більше значення IOPS і менший час затримки, ніж інші рішення.

- При тестуванні варіанта all-flash рішення HyperFlex також показало більше значення IOPS і менший час затримки, але ще більш вражаючим була здатність зберігати стабільно високу продуктивність по всім ВМ, що гарантує задоволеність користувача без додаткових зусиль на керування.

Що важливо врахувати:

- У даний момент рішення HyperFlex реалізоване для середовищ VMware, важливого сегмента ринку. ESG сподівається, що Cisco розширить можливості впровадження рішення на інших гіпервізорах, в «чистих» (bare metal) і контейнерних середовищах.

- Результати тестування, представлені в цьому звіті, засновані на застосунках і зразках, що розгортаються в керованому середовищі з використанням інструментів тестування відповідно до галузевих стандартів. Тому що у виробничому середовищі кожного ЦОД є свої нюанси, ми рекомендуємо проводити тестування й планування потужностей у власному середовищі. Незважаючи на те що в цих тестах застосовувалися самі строгі методології тестування, замовникам рекомендується завжди звертати увагу на деталі, які залишаються за рамками тестування будь-якого постачальника, щоб краще розуміти, наскільки це рішення відповідає вашому середовищу.

Незважаючи на те, що гіперконвергентні інфраструктури вже давно користуються популярністю, їх продовжують уважати підходящими в основному для робочих навантажень другого рівня. На питання, чому замовники віддають перевагу конвергентним інфраструктурам перед гіперконвергентними, респонденти дослідження ESG найчастіше відповідали, що це відбувається через більше високу продуктивність. Виходячи з інших відповідей можна було зробити вивід, що респонденти вважали, що конвергентна інфраструктура, тобто слабко інтегровані незалежні компоненти, скомпоновані разом, краще підходять для критично важливих робочих навантажень, і що їх можна придбати в найбільш надійних гравців ринку.

У компанії Cisco – дійсно надійного гравця – є відповіді на ці питання. Рішення HyperFlex забезпечує всі стандартні переваги систем HCI – є економічно ефективним, простим у керуванні й дозволяє організаціям починати з малого, а потім рости до більших розмірів. Але воно також забезпечує продуктивність, так необхідну критично важливим віртуалізованим робочим навантаженням. Стабільна продуктивність у будь-який момент часу по всім ВМ у кластері – це важлива відмінна риса. Крім іншого, завдяки незалежній масштабованості ресурсів організації можуть швидко адаптувати до мінливих вимог, відповідно до потреб сучасних середовищ.

Рішення Cisco HyperFlex HCI – це високо інтегровані, повністю технічно пророблені системи під керуванням процесорів Intel Xeon, що надають попередньо інтегровані кластери, які включають мережну фабрику, оптимізацію даних, уніфіковані сервери й VMware ESXi/vSphere, що забезпечує швидке розгортання. Таким чином, цим рішенням просто управляти і його зручно масштабувати. підтверджує, що рішення HyperFlex забезпечує стабільно високу продуктивність у середовищах VMware, у гібридні й all-flash кластерах. Рішення HyperFlex обходить цілий ряд анонімних рішень конкурентів завдяки більше

високій продуктивності операцій вводу/виводу/сек, низькій затримці й більшій стабільності в часі й по всіх ВМ.

При зміні галузевих критеріїв покупки на ринку часто замовники зіштовхуються з тим, що не можуть одержати того, що хочуть. Переваги одержать ті постачальники, які розуміють, чого не вистачає замовникам, і які зможуть заповнити цей пробіл. Cisco надає рішення HCI, що забезпечує найважливіші вимоги – простоту й економічну ефективність, а також стабільно високу продуктивність, який раніше не діставало цим рішенням, але без якої неможливе виконання замовниками їх критично важливих робочих навантажень. У даний момент рішення HyperFlex реалізоване тільки в середовищах VMware, тому важливим доповненням стане розширення цього рішення й підтримка їм інших гіпервізорів, чистих (bare metal) і контейнерних середовищ.

Рішення HCI були орієнтовані на робочі навантаження другого рівня, але завдяки стабільно високій продуктивності, забезпечуваної рішенням Cisco HyperFlex, немає ніяких причин по яких системи HCI не змогли б підтримувати виробничі навантаження першого рівня. Cisco HyperFlex зможе стати прекрасним своєчасним рішенням для організацій, зацікавлених у придбанні економічно ефективних, масштабованих, високопродуктивних інфраструктурних рішень.

Ще вчора ви купували сервери, сховища й мережі по-окремі. До того ж була потрібна інтеграція. А вже сьогодні ми представляємо вашій увазі зверхконверговане рішення Cisco Hyperflex. Призначення Hyperflex у тому, щоб надати вам ЦОД за принципом «усе в одному» (in-a-box), де обчислення, зберігання й мережна взаємодія зв'язані один з одним. Це єдине рішення на ринку, що автоматизує мережну роботу й дозволяє незалежно масштабувати обчислювальні ресурси й сховища.

Hyperflex дозволяє вам не витратити сили на те, що може бути придбане в готовому до використання виді, а зосередитися на мережах і застосунках.

Опис

Повна конвергентність

HyperFlex уніфікує мережу структури комутації й технологію організації обчислень із платформою даних нового покоління.

Гнучке масштабування

Незалежне масштабування вузлів, обчислювальних ресурсів і ємності в кластерах HyperFlex з урахуванням бізнес-потреб.

Безперервна оптимізація даних

HyperFlex дозволяє більш ефективно використовувати доступний простір без шкоди для продуктивності. Це можливо завдяки убудованим засобам дедуплікації й стиску даних.

Нові застосунки

Забезпечте підтримку використовуваних корпоративних застосунків і нових хмарних робочих навантажень за допомогою ПЗ платформи даних HyperFlex HX.

Cisco HyperFlex – це новітня гіперконвергентна система, що вирішує проблему високої складності відказостійких систем ЦОД-ів і корпоративних інфраструктур.

Традиційний підхід до побудови ЦОД ґрунтується на поділі серверів, мережі зберігання даних і систем зберігання даних. Такий підхід робить інфраструктуру вкрай складною й дорогою.

Cisco HyperFlex по суті є «ЦОД-ом у коробці», що поєднує обчислювальну інфраструктуру, віртуальні машини й систему зберігання даних у єдину відказостійку й високопродуктивну інфраструктуру.

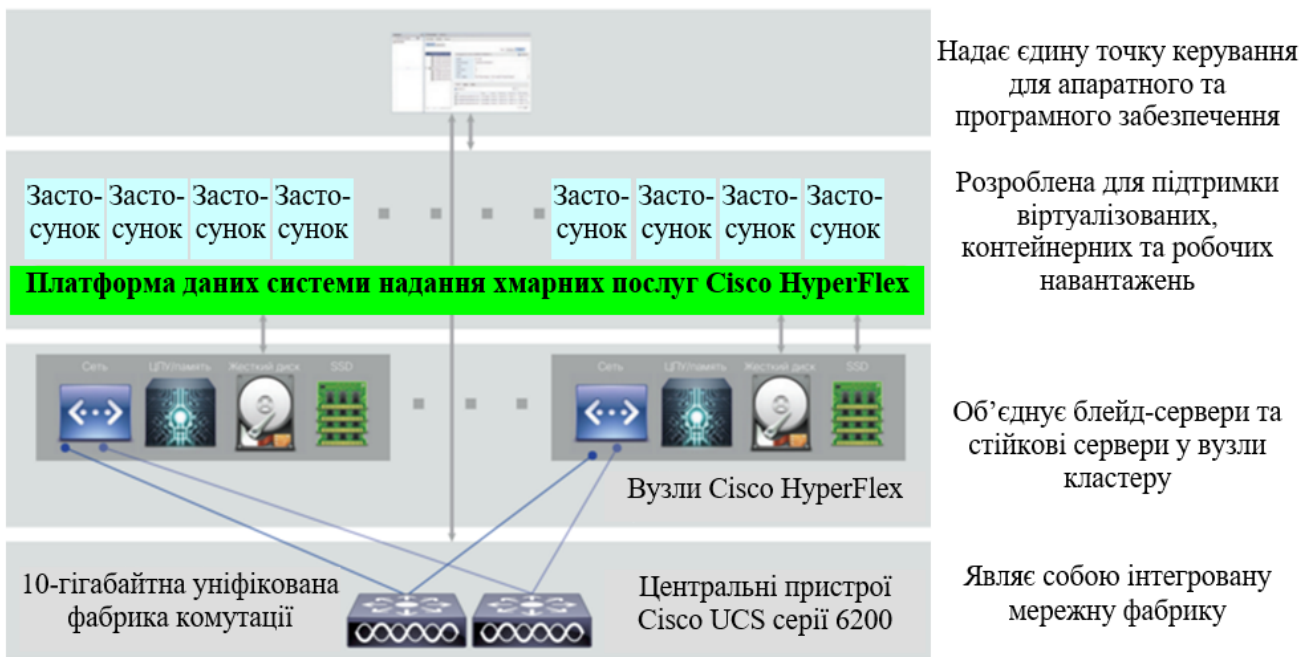


Рисунок 1 – Структурна схема системи

Також HyperFlex є вкрай простим рішенням для впровадження й дозволяє організувати високодоступну ІТ-інфраструктуру з нуля в максимально стислий термін усього з 3-х серверів.

Ще в 2017-ом році незалежна лабораторія Enterprise Strategy Group (ESG Lab) провела порівняльні тести продуктивності Cisco HyperFlex і конкурентних рішень.

Тести проводилися за допомогою HClBench, що є стандартним галузевим інструментом для тестування гіперконвергентних рішень. В основі HClBench лежить Oracle Vdbench, що емулює робоче навантаження на віртуальних машинах.

Тести проводилися для двох сценаріїв: гібридний і all-flash.

Для гібридного сценарію використовувався чотирьохвузловий кластер HyperFlex HX220c з одним SSD-диском 480 Гб для кешу й шістьма SAS дисками по 1,2 Тб на кожному вузлі кластера (разом 4xSSD+24xSAS HDD). Навантаження генерувалося з 140 віртуальних машин (по 35 на ноду кластера), з 4-ма vCPU, 4 GB RAM і віртуальних HDD 20 GB (сумарно на кластер 560 vCPU, 560 GB RAM, 2800 GB HDD).

У ході тестування використовувалися різні профілі навантаження, але при цьому завжди з 100% випадковими даними, що найбільше характерно для середовищ із більшою кількістю віртуальних машин.

Найцікавішим тестом був вимір затримок щодо значень IOPS при співвідношенні читання й запису 70%/30% і блоці 4k, full random.

Як видно з результатів, гібридний варіант HyperFlex більш ніж у два рази перевершує найближчого конкурента (~120 000 IOPS проти ~60 000 IOPS).

Якщо звернутися до тесту All-flash сценарію, то в цьому випадку тестувалося те ж навантаження, але використовувався чотирьохвузловий кластер HyperFlex HX220c тільки з SSD-дисків (один SSD 400 GB для кешу й шість SSD 960 GB для даних, сумарно 4xSSD 400GB+24xSSD 960 GB на весь кластер). В альтернативного постачальника використовувалася аналогічна конфігурація.

При тих же профілях навантаження (співвідношення читання й запису 70%/30% і блоці 4k, full random) результати були наступні:

У підсумку при All-flash сценарії рішення HyperFlex уже в три рази перевершило найближчого конкурента (400 000 IOPS проти 150 000 IOPS).

З моменту незалежного тестування від уже пройшов рік, і з тих пір в HyperFlex з'явилися нові можливості – розтягнутий кластер, підтримка платформи розробки з Kubernetes, а недавно SAP сертифікував HyperFlex для SAP HANA.

Таким чином, Cisco HyperFlex став першим гіперконвергентним рішенням, сертифікованим по всім трьох класах обчислювального навантаження SAP: SAP Applications, SAP Data HUB і HANA.

Це ще раз підтверджує, що HyperFlex з'єднає в собі високу надійність, продуктивність і безпрецедентну простоту використання.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів надання хмарних послуг на базі Cisco HyperFlex. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем надання хмарних послуг на базі Cisco HyperFlex.
- Досліджена система надання хмарних послуг на базі Cisco HyperFlex.
- На основі отриманих результатів досліджень створена програмна реалізація системи надання хмарних послуг на базі Cisco HyperFlex.

Розроблені алгоритми дозволяють успішно вирішувати завдання надання хмарних послуг на базі Cisco HyperFlex. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Смірнова Т.В., Коноплицька-Слободенюк О.К., Буравченко К.О., Смірнов С.А., Кравчук О.В., Козірова Н.Л., Смірнов О.А. «Дослідження технологій забезпечення кібербезпеки хмарних сервісів IaaS, PaaS та SaaS». Кібербезпека: освіта, наука, техніка. 2024. №4(24), С. 6-27.
2. Батрак О., Смірнова Т., Гнатюк В., Одарченко Р., Смірнов О. «Дослідження показників ефективності функціонування та перспектив розвитку систем IP-телефонії». Підводні технології, 2024, № 13, с. 28-35.
3. Kuznetsov, O., Kryvinska, N., Ilchenko, O., Smirnova, T., Ulianovska, Y. «Comparative Analysis of Cryptocurrency Trading Platforms Using the Analytic Hierarchy Process». CEUR Workshop Proceedings, 2023, 3628, pp. 106-115.
4. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». Advanced Information Systems, 2023, 7(2), pp. 49-56.
5. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchey, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». CEUR Workshop Proceedings, Volume 3530, 2023, pp. 256-265.
6. Smirnov, O., Odarchenko, R., Smirnova, T., Bondar, S., Volosheniuk, D. «Optimal Structure Construction of Private 5G Network for the Needs of Enterprises». Lecture Notes on Data Engineering and Communications Technologies, 2023, 178, pp. 208–223.
7. Аль-Мудхафар Акіл Абдулхуссейн М., Смірнова Т.В., Буравченко К.О., Смірнов О.А. «Метод оцінки та підвищення користувацького досвіду абонентів в програмно-конфігурованих мережах на основі використання машинного навчання». Сучасні інформаційні системи, 2023, том 7, № 2, С. 49-56.
8. Smirnova, T., Gnatyuk, S., Yudin, O., Sydorenko, V., Polozhentsev, A., «The Model for Calculating the Quantitative Criteria for Assessing the Security Level of Information and Telecommunication Systems». CEUR Workshop Proceedings Volume 3156, 2022, Pages 390-399.
9. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». Проблеми інформатизації та управління, № 2(70). 2022. С. 28-37.
10. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції ґешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 3(69). С. 93-98.
11. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції ґешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Вісник Хмельницького національного університету. Серія: «Технічні науки», № 2 (307). С. 46-52. 2022.
12. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості

до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 1(67). С. 84-89.

13. Smirnova T., Gnatyuk S., Berdibayev R., Avkurova Zh., Iavich M. «Cloud-Based Cyber Incidents Response System and Software Tools». Communications in Computer and Information Science, 2021, vol 1486. Springer, Cham. pp 169-184.
14. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
15. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». Journal of theoretical and applied information technology Vol.98. No 21, 2020, P. 3334-3346.
16. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177.
17. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587.
18. Smirnov, O., Markovets, O. Vovk, N., Turchyn, Y., «Model of informational support for social network administrators' content creation». CEUR Workshop Proceedings Volume 2616, 2020, Pages 125-136.
19. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». CEUR Workshop Proceedings Volume 2616, 2020, Pages 366-379.
20. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645.
21. Smirnov O. Kuznetsov A., Zaichenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019; Odessa; Ukraine; 9-13 September 2019. P.22-28.
22. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.
23. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019 . P.517-522.
24. Smirnov, O., Odarchenko, R., Abakumova, A., Usik, P., Kundyz, M., «QoE optimization technique for media delivery in 5G networks». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019. P.597-601.
25. Smirnov, O., Krasnobayev, V., Yanko, A., Kuznetsova, T. «Methods of nulling numbers in the system of residual classes». CEUR Workshop Proceedings, Vol 2588, P. 90-106, 2019.
26. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Averchev, A., Pastukhov, M., Kuznetsova, K., «Formation of Pseudorandom Sequences with Special Correlation Properties», 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT -2019/ Lviv, Ukraine, 2-6 July, 2019, P. 395-399.
27. Smirnov, O., Kuznetsov, A., Kiian, A., Zamula, A., Rudenko, S., Hryhorenko, V., «Variance Analysis of Networks Traffic for Intrusion Detection in Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 353-358.
28. Smirnov, O., Kuznetsov, A., Kavun, S., Babenko, B., Nakisko, O., Kuznetsova, K., «Malware Correlation Monitoring in Computer Networks of Promising Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 347-352.
29. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Pastukhov, M., Kuznetsova, K., Prokopovych-Tkachenko, D., «Discrete Signals with Special Correlation Properties», CEUR Workshop Proceedings Volume 2353, CEUR Workshop Proceedings 2019, Pages 618-629.
30. Smirnov A.A., Kuznetsov A.A., Danilenko D.A., Berezovsky A., «The statistical analysis of a network traffic for the intrusion detection and prevention systems», Telecommunications and Radio Engineering. – Volume 74, Issue 1. – Begel House Inc. – 2015. – P. 61-78.
31. Смірнов О.А., Смірнова Т.В., Буравченко К.О., Кравченко С.С., Горбов В.О., «Хмарна система підтримки прийняття рішень технологічного процесу відновлення поверхонь конструкцій і деталей машин». Сучасні інформаційні системи. 2021. Т. 5, № 4. С. 79-95

УДК 004

А.Шарова, магістр гр. КН-24М,

Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ КЕШУВАННЯ, ФЛЕШ-ТЕХНОЛОГІЇ ТА РЕПЛІКАЦІЇ ЦОД

У статті розроблено програмне забезпечення, яке призначено для системи кешування, флеш-технології та реплікації ЦОД. Метою розробки є дослідження та принципи побудови системи кешування, флеш-технології та реплікації ЦОД. Об'єктом дослідження є процес кешування, флеш-технології та реплікації ЦОД. Предметом дослідження є методи кешування, флеш-технології та реплікації ЦОД. Методи дослідження базуються на методах теорії кодування, теорії великих даних, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи кешування, флеш-технології та реплікації ЦОД. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

кешування, флеш-технологія, реплікація, ЦОД

Постановка проблеми. Надійне зберігання даних – завдання, що доводиться вирішувати кожній організації. Що саме потрібно компаніям, щоб організувати роботу з інформацією щонайкраще? Зорієнтуватися на високотехнологічному ринку – непросте, але розв'язне завдання. Для зберігання даних використовують центри обробки даних.

Необхідність у центрах обробки даних (ЦОД) виникла, коли масиви збереженої й переданої інформації перевищили всі мислимі на той момент межі.

Згідно даним TAdviser, з 2010 р. обсяг збереженої інформації щороку зростає приблизно на 50% від її первісного обсягу. Ростає й вартість інформації, оскільки від її прямо залежать всі бізнес-процеси.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи кешування, флеш-технології та реплікації цод.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи кешування, флеш-технології та реплікації ЦОД.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем кешування, флеш-технології та реплікації ЦОД.
- Дослідження системи кешування, флеш-технології та реплікації ЦОД.
- Програмна реалізація системи кешування, флеш-технології та реплікації ЦОД.

Об'єктом дослідження є процес кешування, флеш-технології та реплікації ЦОД.

Предметом дослідження є методи кешування, флеш-технології та реплікації ЦОД.

Методи дослідження базуються на методах теорії кодування, теорії великих даних,, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Цілком розумно очікувати, що повністю флеш-центри обробки даних стануть більш поширеними в майбутньому. Однак перехід до повністю флеш-центрів обробки даних може зайняти деякий час через такі фактори, як вартість, сумісність та вимоги до продуктивності.

Існують дві причини невизначено тривалого майбутнього дискових накопичувачів. Першою є різниця в ціні за терабайт ємності між флеш-накопичувачами та дисковими накопичувачами у п'ять-сім разів. Другою є потреба підприємств зберігати великі та

постійно зростаючі обсяги даних, які активно не використовуються, для таких цілей, як навчання зі штучного інтелекту/машинного навчання та аналітики, архівування та дотримання вимог, а також резервне копіювання.

Потреба в дешевшому архівному сховищі, яке в багатьох місцях все ще включає стрічку, залишиться. Обсяг диска, який купують гіперскейлери, перевищує кількість флеш-накопичувачів сьогодні. Вам потрібне швидке сховище лише для того, над чим ви активно працюєте, а не для того, що ви просто зберігаєте для подальшого використання.

Незважаючи на прогнози щодо смерті стрічок протягом останніх двох десятиліть, використання стрічок – принаймні з точки зору обсягу даних, що зберігаються на них – збільшилося, а не скоротилося, через необхідність зберігати постійно зростаючі обсяги холодних або рідко використовуваних даних.

Як не парадоксально, нові технології, такі як штучний інтелект/модельне навчання, підсилюють цей аргумент. Компаніям потрібен доступ до величезних пулів сховищ для навчання машинному навчанню, але як тільки це буде завершено, дані потрібно буде перенести на більш економічно ефективні технології зберігання. Тож, хоча це може здатися парадоксальною, можна навести вагомий аргумент, що нові програми штучного інтелекту фактично збільшують потребу в системах зберігання другого та третього рівнів, таких як диски та навіть стрічки.

Я сумніваюся, що коли-небудь з'являться повністю флеш-центри обробки даних з кількох причин. Завжди буде потреба в стрічках або дисках просто тому, що вони можуть зберігати величезні обсяги даних дешевим способом офлайн, і буде зростати обсяг даних, до яких рідко звертаються, але які все одно потрібно зберігати. І до того часу, як флеш-пам'ять захопить центри обробки даних, новіші NVM [незалежні пам'яті], такі як ReRAM та MRAM, почнуть займати частину центрів обробки даних.

Сьогодні економія коштів у 5 разів на флеш-пам'ять порівняно з диском робить більший простір для зберігання дисків, що використовуються в об'єктному сховищі, сильнішою альтернативою стрічці, а Seagate протягом наступних кількох років представить довгоочікувані дискові накопичувачі ємністю 30, 40 і 50 ТБ, що розширить можливості для дисків.

Однак, обираючи між дисковою та флеш-пам'яттю, ІТ-команди враховують не лише початкові витрати на придбання. Є один аспект переходу на флеш-технологію, який часто недооцінюється щодо її цінності для клієнтів: зі збільшенням продуктивності завдяки флеш-пам'яті з'являється цінність простоти. Під простотою я маю на увазі необхідність керування характеристиками пристрою для розміщення/розподілу даних з точки зору продуктивності. Це просто простіше, коли є вища продуктивність сховища. Це фактор, який спонукатиме організації до використання високопродуктивних технологій.

Однак деякі центри обробки даних вже повністю використовують флеш-пам'ять.

Відповідь на це питання про повністю флеш-центри обробки даних буде залежати від розміру, масштабу та обсягу роботи центру обробки даних. Існує багато менших та середніх центрів обробки даних, які вже повністю використовують флеш-пам'ять. Але це, як правило, центри обробки даних для одного клієнта. Великі підприємства, регіональні хостинг-постачальники послуг та масивні гіперскейлери матимуть «живу іржавію» протягом будь-якого прогнозованого періоду часу.

До 2028 року існує клас корпоративних центрів обробки даних, які будуть повністю флеш-сховищами. Це центри обробки даних, що експлуатуються підприємствами, які все частіше використовують хмарні інфраструктури публічної інфраструктури для розміщення своїх менш чутливих до продуктивності або критично важливих програм, що не потребують флеш-сховища та використовують ті ж хмари для зберігання своїх холодних або рідко використовуваних даних.

Локальні центри обробки даних, які здебільшого зосереджені на запуску критично важливих програм, швидко переходять на повністю флеш-сховище. Omdia прогнозує, що

протягом наступних трьох-п'яти років більшість цих локальних центрів обробки даних повністю перейдуть на флеш-технологію.

Іншими словами, дискові накопичувачі переходять з корпоративних центрів обробки даних у гіперхмарні, де вони існуватимуть ще багато років через низьку вартість та відсутність потреби в продуктивності під час зберігання холодних даних. Хан навів ще одну причину, чому не варто використовувати флеш-пам'ять для зберігання цього типу даних: «Оскільки ці [сховища масового зберігання, архівування та резервного копіювання] часто взаємодіють з відносно повільним Інтернетом, пропускна здатність, а не низька затримка пошуку, є більш важливою». З тієї ж причини, чому пропускна здатність важливіша за випадковий доступ, він додає: «Основні випадки використання, такі як відео та мультимедіа, зможуть ефективно використовувати жорсткі диски протягом тривалого часу, а також інші технології, такі як IoT та ELT [Вилучення, завантаження, перетворення] конвеєрів збору даних.

Ще одним міркуванням є тенденція до продовження терміну служби ІТ-обладнання як частини стратегії екологічної стійкості та економії коштів. Тому клієнти зараз менш охоче позбавляються від технології, яка здається старою, та замінюють її блискучою новою. Вплив на центри обробки даних полягатиме в використанні низки технологій, яким у деяких випадках може бути до семи років, а це означає, що поява повністю флеш-центрів обробки даних не є найближчою перспективою.

Вважаємо, що існує межа, де розгортання з ємністю менше заданої мають сенс як повністю флеш-пам'яті, а розгортання вище цієї межі можуть бути недоцільними. Ця межа повільно рухатиметься вгору, але, на нашу думку, здебільшого йтиме в ногу зі зростанням потреб у ємності, тому центри обробки даних, що використовують лише флеш-пам'ять, залишаться назавжди «через два роки».

Компанія може бути рада зберігати відносно невеликі файлові системи обсягом 200 ТБ у флеш-пам'яті, оскільки це коштуватиме лише приблизно на 150 000 доларів більше, ніж зберігання на диску, і працюватиме набагато краще. Але для зберігання в 100 разів більшої ємності, 20 ПБ, додаткові витрати становитимуть 12 мільйонів доларів, що важко виправдати. Якщо у вас немає якихось особливих вимог, ці гроші краще було б використати для придбання процесорів та графічних процесорів.

Розвиток технологій часто слідує кривій, за якою темпи покращення вартості або продуктивності повільно зменшуються з часом, слідуючи кривій, яка поступово стає більш пологою, оскільки технічний прогрес стає дедалі складнішим для досягнення. Дійсно, приблизно до 2010 року багато спостерігачів передбачали, що технічний розвиток NAND-флеш-пам'яті ось-ось зіткнеться з проблемою кількості комірок пам'яті, які можна упакувати в один флеш-чіп. На той час флеш-пам'ять була добре утвердженою та зростаючою рисою корпоративного ІТ-ландшафту не лише завдяки своїй продуктивності та іншим перевагам порівняно з диском, але й тому, що її ціна падала протягом попереднього десятиліття. Якби виробники флеш-чипів зіткнулися з цією прогнозованою технологічною проблемою, ціни почали б падати набагато повільніше в перерахунку на одиницю ємності пам'яті.

Однак у 2013 році Samsung обійшла передбачуване обмеження, випустивши перші так звані 3D-флеш-чіпи, які склалися з кількох шарів комірок пам'яті, а не з одного шару комірок, що використовувався раніше. Це означало більше комірок пам'яті на чіп, і як надзвичайно цінний побічний ефект, можливість зберігати більше бітів даних у кожній комірці пам'яті, що знову ж таки знизило ціни за терабайт. Усі основні виробники флеш-пам'яті невдовзі наслідували приклад Samsung, і з того часу кількість шарів на чіп швидко зростала. Але це було десять років тому. Чи наближається флеш-пам'ять зараз до кінця чи до більш пологої частини своєї технологічної кривої?

Люди, які кажуть: «Закон Мура мертвий», ігнорують 3D NAND. Ця технологія дала флеш-пам'яті NAND новий механізм для подальшого додавання бітів до чіпа, і щороку інженери-технологи знаходять геніальні способи просунути його далі, ніж хтось міг би вважати можливим. Це далеко не те, щоб сказати «ні» на це питання. Очікуйте побачити

щонайменше ще кілька порядків зниження вартості протягом наступних кількох років, оскільки щільність чіпів продовжуватиме зростати.

Виробники флеш-пам'яті, такі як Samsung, SK Hynix, Kioxia, Western Digital та Micron, продовжуватимуть впроваджувати інновації з дорожніми картами для більшої щільності з більшою кількістю шарів, використовуючи методи стекування, інновації в архітектурі та дизайні, а також більше бітів на комірку (наприклад, п'ятирівнева комірка або ПЛК). Перші багатошарові флеш-чіпи, що вийшли на ринок у 2013 році, склалися з 24 шарів комірок пам'яті та зберігали 128 Гбіт/с. Ю згадав про демонстрацію SK Hynix цього року 321-шарового чіпа, що зберігає 1 Тбіт/с, а також прогноз Samsung, зроблений минулого року, що до 2030 року вона поставить 1000-шарові чіпи.

Дискова технологія також все ще розвивається, і тому ціни на диски також продовжуватимуть падати приблизно з тією ж швидкістю, що й на флеш-пам'ять. «Флеш-технологія продовжить свою неблаганну криву вдосконалення, але ми не бачимо, щоб ця крива прискорювалася, щоб набирати обертів на дисках, тобто знижувала множник 5х-7х (\$/ТБ) або уповільнювала його порівняно з дисками.

Є кілька факторів, деякі з яких були окреслені в попередніх відповідях, які свідчать про те, що флеш-пам'ять все ще перебуває на підйомі з точки зору технологічної кривої. Існує аргумент, який слід враховувати, де поточна технологія флеш-пам'яті переходить у нові технології, проте, враховуючи рівні розвитку, які все ще досягають компанії, що розробляють флеш-сховища, це, здається, свідчить про те, що ще є багато можливостей для просування вгору, перш ніж буде досягнуто плато.

Флеш-пам'ять має багато технологічних переваг не лише всередині чіпів

Ми тільки починаємо бачити, як флеш-пам'ять можна використовувати в центрах обробки даних. Цінність комунікаційних протоколів NVMe тільки починає визнаватися в центрах обробки даних, і знадобиться щонайменше десятиліття, щоб вони замінили масивну інфраструктуру на основі SCSI. Крім того, еволюція інтерфейсу PCIe та нові технології, такі як CXL, відкриють нові можливості для реалізації флеш-сховищ. Крім того, транспортні протоколи, такі як NVM-oF, зазвичай через RDMA Ethernet, тільки починають об'єднуватися як життєздатна альтернатива. Тож, замість того, щоб досягти піку, я вважаю, що ми тільки починаємо бачити перші кроки революції флеш-технологій.

Флеш-пам'ять трансформувала корпоративне сховище даних і була головною рушійною силою, яка рушійною силою революції мобільних обчислень. Зараз це основна технологія. Окремо від виробництва продуктів на базі флеш-пам'яті, таких як накопичувачі або повноцінні системи зберігання даних, виробництво лише NAND-флеш-чіпів зараз генерує близько 80 мільярдів доларів річного доходу, і ця цифра продовжує зростати.

Це викликає очевидне питання: коли з'явиться наступна нова технологія твердотілого зберігання даних з таким самим впливом на масовий ринок? Протягом останніх кількох десятиліть у дослідницьких лабораторіях було витрачено мільярди доларів на спроби знайти іншу таку технологію. Спільно розроблена Intel та Micron пам'ять Optane стала результатом таких досліджень і вперше була поставлена у твердотілих накопичувачах у 2017 році. Швидше, але дорожче за флеш-пам'ять, Optane була проголошена першою з майбутнього класу так званих пам'ятей класу сховищ (SCM), які мали доповнити або замінити флеш-пам'ять і мати так само великий загальний вплив на ІТ. Однак Optane продавалася погано, і у 2021 році Intel оголосила про свій план припинити виробництво цієї пам'яті, лише через чотири роки після її перших поставок.

Тим часом дослідження інших потенційних SCM тривають. Для Objective Analysis, яка зосереджена на нових моделях пам'яті, Генді сказав, що протягом цього та наступного десятиліття, ймовірно, не з'явиться нових технологій пам'яті з потенціалом такого ж впливу, як флеш-пам'ять. Він розрізняв два типи пам'яті: ті, що вбудовані в процесори або інші чіпи, та ті, що, як NAND-флеш та Optane, продаються або продавалися як чіпи лише для дискретної пам'яті у набагато більших кількостях і тому мають набагато більший ринковий потенціал.

Optane зазнав невдачі через свою вартість. Ми попереджали про це, щойно його оголосили. Але інші технології, ймовірно, процвітатимуть на певних ринках, особливо як вбудована пам'ять у мікроконтролерах, ASIC та інших SoC [процесорах Systems-on-a-Chip]. Однак дискретні мікросхеми пам'яті навряд чи масово перетворяться на нові SCM у 2020-х роках, і, ймовірно, не у 2030-х роках.

Optane, також відомий як 3D XPoint, зазнав невдачі з економічних причин, але створення альтернативи флеш-пам'яті неминуче:

Кілька технологій NVM, включаючи ReRAM, MRAM, PCM та FRAM, стають потенційними альтернативами флеш-пам'яті. 3D XPoint від Intel була першою спробою вирішити цю проблему, але не увінчалася успіхом значною мірою з економічних причин. Ключем до успішної альтернативи флеш-пам'яті є розробка пам'яті, яка може масштабуватися до достатньо великої щільності, але за достатньо низькою ціною. Intel змогла впоратися лише з частиною цієї проблеми, пов'язаною з щільністю. Це лише питання часу, коли ми побачимо технологію, яка зможе відповідати обом критеріям, і ми вважаємо, що ReRAM буде відповіддю, оскільки вона має фундаментальні технічні переваги, включаючи швидкість, енергоефективність та вартість. Триває розробка, щоб довести технологію до ще більшої щільності.

За 10 років може статися багато чого – сказати, що станеться, легко (наприклад, атомну пам'ять, яку досліджує IBM); сказати коли – набагато важче.

Технологічний імпульс та варіант флеш-пам'яті SLC стануть перешкодою для будь-якої нової пам'яті.

Нездатність досягти достатніх продажів, щоб виправдати обсяги виробництва, необхідні для забезпечення життєздатно низьких цін, призвела до скасування Optane. Відносно нові високошвидкісні варіанти флеш-пам'яті SLC [single-level cell] виконують завдання, для яких була призначена Optane. Легко уявити, де пам'ять класу сховища може вписатися в піраміду пам'яті сховища, але було важко забезпечити правильне поєднання характеристик продуктивності, затримки та вартості, забезпечуючи при цьому збереження даних у реальному світі. Optane SCM здавався гарним проєктом, але його виробництво згортається через відсутність належної економіки обсягу. Очевидно, що є кілька хороших варіантів використання для Optane SCM, але, чесно кажучи, вони вирішуються за допомогою нещодавно випущеної технології NAND-флеш SLC. Пропозиції SLC NAND SSD набирають популярності завдяки своїй фантастичній довговічності та хорошій продуктивності запису, особливо для багаторівневого створення масивів даних та кешування даних.

«Будь-яка нова технологія має перевершити існуючу технологію, яка виграє від десятиліть оптимізації та великомасштабного виробництва. Отже, нова технологія буде у значно не вигідному становищі.

SCM мали/мають величезний потенціал, але зміна архітектури програмного забезпечення, необхідна для того, щоб програми отримали всі переваги, які може запропонувати SCM, була занадто високою, тому програми так і не прийняли їх. Флеш-пам'ять не зіткнулася з цією перешкодою, оскільки її специфічне поєднання вартості та продуктивності ніколи не вимагало та не виправдовувало її використання як доповнення до пам'яті DRAM.

Крім планування оптимального використання дискової підсистеми, деякі ЦОД дозволяють вибрати й розмір кешу. Про те, як використовується кеш у системі зберігання даних і скільки його мабуть, існує багато думок. Одне з найважливіших призначень кешу – зберігання метаданих ЦОД. Для реалізації будь-якої функціональності ЦОД, будь те дискові групи, логічні томи, багаторівневе зберігання або реплікація, необхідні службові дані – це і є метадані. Вони постійно використовуються мікрокодом ЦОД, і для їхнього зберігання потрібний самий швидкодіючий носій інформації в системі. Їм і є кеш, для реалізації якого використовується оперативна пам'ять рівня DDR3 або DDR4, чия продуктивність на порядок вище, ніж у самого швидкісного флеш-диска.

Друга важлива функція кешу – безпосереднє кешовані даних. Оброблювані хостами дані розміщуються в кеші й можуть використовуватися повторно без звертання до більше повільних дисків. Крім того, кешовані дозволяє оптимізувати запис даних на диски.

Однак використання кешу ефективно не для всіх профілів навантаження. Дані, які послідовно зчитуються із системи зберігання, кешуються добре – це так зване лінійне читання. Навіть якщо додаток зчитує дані, наприклад, дрібними блоками по 8 Кбайт замість що рекомендуються 256 Кбайт і більше, система зберігання розпізнає лінійне читання й, знаючи, які дані будуть запитані наступними операціями вводу-виводу, зчитує їх заздалегідь. Таким чином, що впливає операція вводу-виводу не викликає звертання до більше повільної дискової підсистеми – дані надходять із кешу, що істотно прискорює вводу-вивід.

У той же час кеш майже марний, коли мова йде про випадкове читання (random read) даних зі ЦОД. У цьому випадку ймовірність знаходження потрібних даних у кеші прагне до нуля, оскільки обсяг кешу в системі зберігання на порядок менше, ніж максимальний корисний обсяг даних сучасних ЦОД. Саме тому кілька років назад з'явилася ідея використовувати флеш-диски для прискорення випадкового читання.

Флеш-технології дозволяють оптимізувати й інші типи навантажень. Однак приріст продуктивності, у порівнянні з використанням механічних дисків, виходить не настільки значним, тоді як різниця у вартості зберігання 1 Тбайт даних на флеш-диску й механічному диску поки залишається досить відчутної.

При будь-яких операціях запису дані спочатку містяться в кеш і лише після цього записуються на диски. Крім повторного використання для наступних операцій вводу-виводу, нові дані можуть групуватися спеціальним образом, але тільки в тому випадку, якщо надалі вони будуть записані на групи RAID з парністю (RAID5 і RAID6).

Чому важлива оптимізація запису при використанні RAID-груп з парністю? Вся справа в тому, що в них застосовується особливий захист даних від збою диска в групі. Якщо, допустимо, робити запис на масив RAID5 випадковим образом, без оптимізації, то одна операція запису, зроблена хостом, буде генерувати чотири операції вводу-виводу на системі зберігання (два читання й два записи). Для RAID6 цей показник дорівнює вже шести. У результаті продуктивність ЦОД серйозно знизиться.

Що в цьому випадку може почати система зберігання даних? У першу чергу вона спробує сформувати в кеш-пам'яті набір даних (full stripe), щоб зробити розрахунок парності без додаткового звертання до дисків і записати відразу всі дані на диски. При послідовному записі зібрати full stripe у кеш-пам'яті досить легко, але при випадковій – система або буде чекати, поки в кеші не збереться необхідний набір даних, або почне зчитувати відсутні блоки даних з дисків. Тому кешовані запису даних практично у всіх випадках прискорює вводу-вивід.

Існує думка, що, якщо збільшити обсяг кешу, ЦОД стане працювати швидше. Як правило, між корисним обсягом збережених даних і ємністю кешу є деяке визначене співвідношення, що бажано витримувати. Однак це повністю здійснено тільки в системах зберігання старшого класу, де можливий більше гнучкий вибір обсягу кешу. У системах зберігання середнього класу не завжди вдається розширити кеш до бажаних величин.

Якщо ЦОД не справляється із читанням або записом даних, справа аж ніяк не в кеші. Швидше за все, обрана невідповідна модель ЦОД або неправильно зроблена конфігурування дискової підсистеми, який просто не вистачає ресурсів для читання й запису всіх даних, що надходять. Точна оцінка планованого навантаження й вибір потрібної конфігурації ЦОД є ключовими критеріями для одержання бажаної продуктивності ІТ-системи. Тому збільшення обсягу кешу не панацея для підвищення продуктивності.

Особливості флеш-накопичувачів

Говорячи про продуктивність, неможливо не торкнутися докладніше теми флеш-технологій. Якщо обчислювальна потужність контролерів ЦОД не є вузьким місцем, то використання флеш-дисків завжди дозволяє збільшити продуктивність доступу до даних при будь-якому профілі навантаження – лінійному й випадковому, при читанні й при записі.

Однак треба брати до уваги й фінансову складову: при послідовному читанні й записі флеш-диски можуть працювати в кілька разів швидше механічних, але вартість зберігання 1 Тбайт даних буде в десятки разів вище. Тому для лінійних навантажень звичайно використовуються самі повільні механічні диски NL-SAS, оскільки навіть вони прекрасно справляються з поставленим завданням.

Флеш-технології дуже ефективні при випадковому профілі вводу-виводу – особливо при випадковому читанні, коли кеш нічим допомогти не може. Вони відрізняються не тільки можливістю здійснювати більше операцій вводу-виводу (IOPS), але й низьким часом відгуку таких операцій: дві мілісекунди й менше. Саме тому при високих вимогах до продуктивності постачальники рішень пропонують флеш-диски в складі ЦОД або систему, повністю оснащену флеш-дисками (All Flash Array, AFA).

У той же час флеш-диски «не люблять» операції запису – дані на них записуються повільніше, ніж зчитуються. Це пов'язане з використанням пам'яті NAND. На відміну від механічних дисків, на які можна довільно записувати й перезаписувати будь-які дані, флеш-диск потрібно спочатку очистити. Причому не можна стерти один біт або байт – дані стираються блоками по 1-2 Мбайт залежно від типу диска, виробника й інших параметрів. Попередньо необхідно перенести всі актуальні дані у вже чисті (стерті) блоки. Таким чином, якщо при занадто інтенсивному записі місце в блоках звільняється недостатньо швидко, флеш-диск починає «гальмувати».

Флеш і синхронна реплікація

Чи ефективні флеш-диски при віддаленій синхронній реплікації? Дані реплікуються на віддалену площадку для забезпечення їхньої схоронності й доступності на той випадок, якщо основна ЦОД повністю вийде з ладу. Як правило, площадка розташовується досить далеко, і тому до звичайних затримок вводу-виводу додається ще й затримка від реплікації.

Існує думка, що флеш-диски неефективні при такому виді реплікації. Це пов'язане з тим, що синхронна реплікація може звести нанівець одну з основних особливостей флеш-дисків – дуже невелику затримку вводу-виводу. Насправді додаткові затримки в основному стосуються тільки операцій запису, а їхня частка в профілі навантаження застосунку, як правило, не перевищує 20-30%. Таким чином, навіть при синхронній реплікації флеш-диски будуть досить ефективні і їхнє використання в подібних конфігураціях цілком виправдано.

Необхідна конфігурація для синхронної реплікації

Чи потрібні при віддаленій синхронній реплікації дві однаково зконфігуровані ЦОД? Це залежить від виду синхронної реплікації (Active/Active або Active/Passive), розподілу навантаження вводу-виводу між двома центрами обробки даних, вимог SLA і інших параметрів. Інтенсивність навантаження на ідентичні набори даних, що зберігаються на віддалених площадках, завжди буде різною. У випадку синхронної реплікації Active/Active (див. рисунок 1) навантаження буде залежати від балансування вводу-виводу застосунку між двома ЦОДами. Якщо використовується Active/Passive, копія основних даних перебуває чекаючи «години ікс», коли основний набір стане недоступний і їй буде потрібно відповідати за все вводу-вивід. І в тому і в іншому випадку для зберігання додаткового набору даних потрібні ресурси: дискові, обчислювальні й т.д.

Необхідність використання флеш-дисків і однакових обчислювальних контролерів ЦОД для обох наборів даних залежить від того, яку продуктивність вводу-виводу повинна забезпечити що залишилася ЦОД після виходу з ладу основної системи. Якщо до усунення аварії допускаються зниження продуктивності ЦОД і погіршення роботи ІТ-системи, то для зберігання другого набору даних досить ресурсів з меншою продуктивністю.

Як правило, такі схеми застосовуються в тих випадках, коли фінансові втрати від погіршення роботи ІТ-системи менше вартості зберігання другого набору даних на високопродуктивних ЦОД. Якщо ж відмова одного із ЦОДів приведе до фінансових втрат, що перевищують вартість зберігання копії даних на високопродуктивної ЦОД, то використання тих же самих ресурсів для зберігання нехай навіть неактивної копії даних обов'язково.

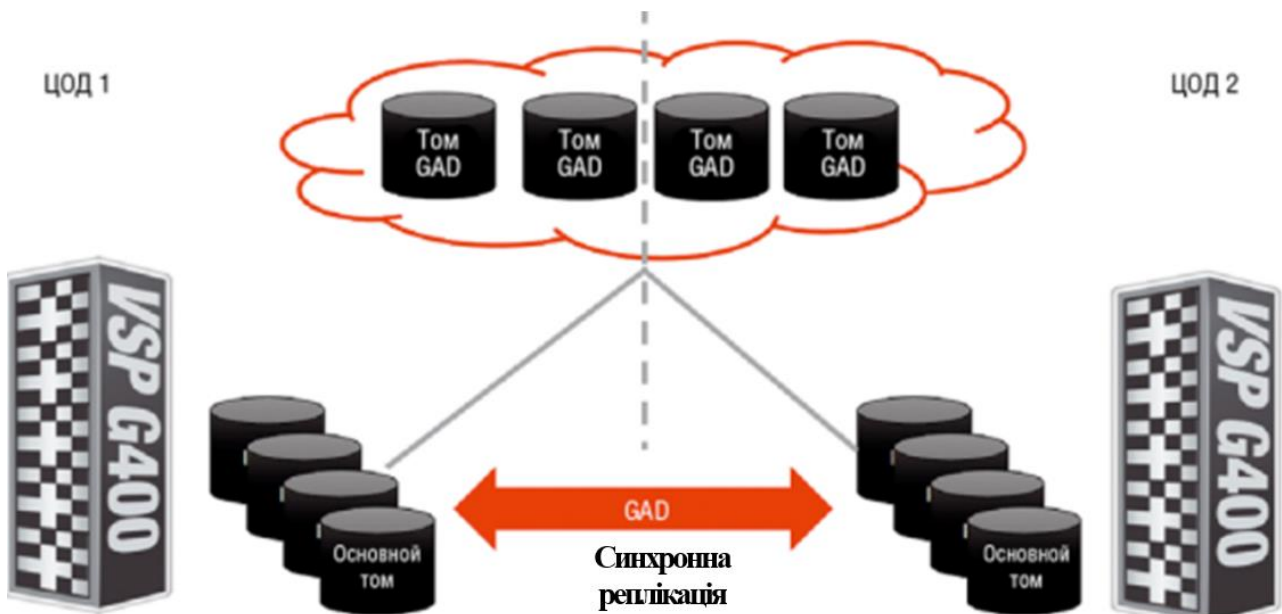


Рисунок 1 – Структурна схема системи

Продуктивність СЗД при збоях

Продуктивність ЦОД при апаратних збоях – не менш важливий момент, на який ІТ-фахівці не завжди звертають увагу при виборі конфігурації ЦОД. Продуктивність ЦОД завжди оцінюється в той момент, коли всі її складові функціонують у штатному режимі. Але так буває не завжди: іноді вихід з ладу одних компонентів ЦОД не робить ніякого впливу на продуктивність, у той час як поломка інших приводить до її істотного зниження.

Наприклад, при виході з ладу обчислювального контролера у двоконтролерної ЦОД продуктивність може знизитися більш ніж у два рази. Це пов'язане із забезпеченням захисту цілісності даних: при роботі на запис кеш переводиться в режим Write-through, що поряд із втратою обчислювальної потужності одного контролера приводить до подальшого зменшення продуктивності ЦОД.

Таким чином, щоб при виході з ладу будь-якого компонента продуктивність як і раніше відповідала певним вимогам, у конфігурації ЦОД доводиться передбачати додаткові ресурси, які в штатному режимі роботи ЦОД використовуватися не будуть. Якщо ж передбачається застосування віддаленої синхронної реплікації для захисту від збою ЦОД, у випадку сильного зниження продуктивності основний ЦОД, викликаного збоєм одного з її компонентів, ввід-вивід ІТ-системи може перемикатися на резервну площадку.

Проблема вибору конфігурації

Вибір конфігурації як ЦОД, так і рішення в цілому залежить від вимог до продуктивності ІТ-системи й від можливих фінансових втрат при погіршенні якості її роботи.

Ми торкнулися далеко не всі аспекти вибору конфігурації ЦОД і планування її експлуатації, пов'язані із продуктивністю. Існує безліч різних методик оптимізації конфігурації рішення, у яких ураховуються вихідні вимоги, тип застосунку й багато чого іншого. Більше того, зі зміною підходу до зберігання даних – від приватних сховищ до хмарних, від блокового зберігання даних до файлового й об'єктного зберігання – будуть трансформуватися й методики розрахунку параметрів сховищ даних, що забезпечують необхідні експлуатаційні характеристики. Однак можна із упевненістю затверджувати, що тема продуктивності зберігання даних була, є й буде важливою складовою при виборі будь-якого сучасного ІТ-рішення.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів кешування, флеш-технології та реплікації ЦОД. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем кешування, флеш-технології та реплікації ЦОД.
- Досліджена система кешування, флеш-технології та реплікації ЦОД.
- На основі отриманих результатів досліджень створена програмна реалізація системи кешування, флеш-технології та реплікації ЦОД.

Розроблені алгоритми дозволяють успішно вирішувати завдання кешування, флеш-технології та реплікації ЦОД. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Al-Azzeh, J., Ayyoub, B., Mesleh, A., Smirnova, T., Gnatyuk, S., Drieiev, O., Smirnov, O., Dorenskyi, O. «Cloud-Based Information System for Evaluating Caverns in the Process of Blasting Metal Surfaces of Details». *International Review on Modelling and Simulations* 18 (1), 2025. pp. 32-42.
2. Смірнова Т.В., Коноплицька-Слободенюк О.К., Буравченко К.О., Смірнов С.А., Кравчук О.В., Козірова Н.Л., Смірнов О.А. «Дослідження технологій забезпечення кібербезпеки хмарних сервісів IaaS, PaaS та SaaS». *Кібербезпека: освіта, наука, техніка*. 2024. №4(24), С. 6-27.
3. Батрак О., Смірнова Т., Гнатюк В., Одарченко Р., Смірнов О. «Дослідження показників ефективності функціонування та перспектив розвитку систем IP-телефонії». *Підводні технології*, 2024, № 13, с. 28-35.
4. Kuznetsov, O., Kryvinska, N., Ilchenko, O., Smirnova, T., Ulianovska, Y. «Comparative Analysis of Cryptocurrency Trading Platforms Using the Analytic Hierarchy Process». *CEUR Workshop Proceedings*, 2023, 3628, pp. 106-115.
5. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». *Advanced Information Systems*, 2023, 7(2), pp. 49-56.
6. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchев, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». *CEUR Workshop Proceedings*, Volume 3530, 2023, pp. 256-265.
7. Smirnov, O., Odarchenko, R., Smirnova, T., Bondar, S., Volosheniuk, D. «Optimal Structure Construction of Private 5G Network for the Needs of Enterprises». *Lecture Notes on Data Engineering and Communications Technologies*, 2023, 178, pp. 208-223.
8. Аль-Мудхафар Акіл Абдулхуссейн М., Смірнова Т.В., Буравченко К.О., Смірнов О.А. «Метод оцінки та підвищення користувацького досвіду абонентів в програмно-конфігурованих мережах на основі використання машинного навчання». *Сучасні інформаційні системи*, 2023, том 7, № 2, С. 49-56.
9. Smirnova, T., Gnatyuk, S., Yudin, O., Sydorenko, V., Polozhentsev, A., «The Model for Calculating the Quantitative Criteria for Assessing the Security Level of Information and Telecommunication Systems». *CEUR Workshop Proceedings Volume 3156*, 2022, Pages 390-399.
10. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». *Проблеми інформатизації та управління*, № 2(70). 2022. С. 28-37.
11. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» *Системи управління, навігації та зв'язку*, 2022, № 3(69). С. 93-98.
12. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» *Вісник Хмельницького національного університету. Серія: «Технічні науки»*, № 2 (307). С. 46-52. 2022.
13. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» *Системи управління, навігації та зв'язку*, 2022, № 1(67). С. 84-89.
14. Smirnova T., Gnatyuk S., Berdibayev R., Avkurova Zh., Iavich M. «Cloud-Based Cyber Incidents Response System and Software Tools». *Communications in Computer and Information Science*, 2021, vol 1486. Springer, Cham. pp 169-184.
15. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». *CEUR*

Workshop Proceedings. Volume 2740, 2020, Pages 102-114.

16. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». *Journal of theoretical and applied information technology* Vol.98. No 21, 2020, P. 3334-3346.
17. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177.
18. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) *Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies*, vol 48. Springer, Cham. 2021. pp 557-587.
19. Smirnov, O., Markovets, O. Vovk, N., Turchyn, Y., «Model of informational support for social network administrators' content creation». *CEUR Workshop Proceedings Volume 2616*, 2020, Pages 125-136.
20. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». *CEUR Workshop Proceedings Volume 2616*, 2020, Pages 366-379.
21. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», *CEUR Workshop Proceedings Volume 2608*, 2020, Pages 633-645.
22. Smirnov O. Kuznetsov A., Zaichenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». *International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019; Odessa; Ukraine; 9-13 September 2019*. P.22-28.
23. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». *International Journal of Computing*; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.
24. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019 . P.517-522.
25. Smirnov, O., Odarchenko, R., Abakumova, A., Usik, P., Kundyz, M., «QoE optimization technique for media delivery in 5G networks». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019. P.597-601.
26. Smirnov, O., Krasnobayev, V., Yanko, A., Kuznetsova, T. «Methods of nulling numbers in the system of residual classes». *CEUR Workshop Proceedings, Vol 2588*, P. 90-106, 2019.
27. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Averchev, A., Pastukhov, M., Kuznetsova, K., «Formation of Pseudorandom Sequences with Special Correlation Properties», 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT -2019/ Lviv, Ukraine, 2-6 July, 2019, P. 395-399.
28. Smirnov, O., Kuznetsov, A., Kiian, A., Zamula, A., Rudenko, S., Hryhorenko, V., «Variance Analysis of Networks Traffic for Intrusion Detection in Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 353-358.
29. Smirnov, O., Kuznetsov, A., Kavun, S., Babenko, B., Nakisko, O., Kuznetsova, K., «Malware Correlation Monitoring in Computer Networks of Promising Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 347-352.
30. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Pastukhov, M., Kuznetsova, K., Prokopovych-Tkachenko, D., «Discrete Signals with Special Correlation Properties», *CEUR Workshop Proceedings Volume 2353*, CEUR Workshop Proceedings 2019, Pages 618-629.
31. Smirnov A.A., Kuznetsov A.A., Danilenko D.A., Berezovsky A., «The statistical analysis of a network traffic for the intrusion detection and prevention systems», *Telecommunications and Radio Engineering. – Volume 74, Issue 1. – Begel House Inc. – 2015. – P. 61-78.*

УДК 004

А.Яковенко, магістр гр. КІ-24М,

Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ КЕРУВАННЯ РОЗПОДІЛЕНОЮ СЗД ЗА ДОПОМОГОЮ СПЕЦИФІКАЦІЇ NVME OVER FABRICS

У статті розроблено програмне забезпечення, яке призначено для системи керування розподіленою СЗД за допомогою специфікації NVMe over Fabrics. Метою розробки є дослідження та принципи побудови системи керування розподіленою СЗД за допомогою специфікації NVMe over Fabrics. Об'єктом дослідження є процес керування розподіленою СЗД за допомогою специфікації NVMe over Fabrics. Предметом дослідження є методи керування розподіленою СЗД за допомогою специфікації NVMe over Fabrics. Методи дослідження базуються на методах теорії побудови комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи керування розподіленою СЗД за допомогою специфікації NVMe over Fabrics. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

керування розподіленою СЗД, NVMe over Fabrics

Постановка проблеми. Багато компаній інвестують у NVMe-накопичувачі, очікуючи блискавичної швидкості, але вони все одно можуть зіткнутися зі зниженням продуктивності в мережі. Це пояснюється тим, що традиційні архітектури сховищ не розраховані на роботу з великими робочими навантаженнями сучасного часу, і, як наслідок, вони обмежують продуктивність.

На щастя, NVMe over Fabrics змінює все. Завдяки цій технології ви можете розкрити весь потенціал пристроїв NVMe Express у мережі, не витрачаючи інвестиції на застарілі протоколи.

NVMe поверх Fabrics дозволяє організаціям скорочувати час відгуку програм і масштабувати сховище незалежно від обчислень. Він навіть підтримує робочі навантаження штучного інтелекту (ШІ) та машинного навчання (ML), які б перевершили традиційні мережі зберігання даних (SAN).

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи керування розподіленою СЗД за допомогою специфікації NVMe over Fabrics.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи керування розподіленою СЗД за допомогою специфікації NVMe over Fabrics.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем керування розподіленою СЗД за допомогою специфікації NVMe over Fabrics.
- Дослідження системи керування розподіленою СЗД за допомогою специфікації NVMe over Fabrics.
- Програмна реалізація системи керування розподіленою СЗД за допомогою специфікації NVMe over Fabrics.

Об'єктом дослідження є процес керування розподіленою СЗД за допомогою специфікації NVMe over Fabrics.

Предметом дослідження є методи керування розподіленою СЗД за допомогою специфікації NVMe over Fabrics.

Методи дослідження базуються на методах теорії побудови комп'ютерних мереж, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. NVMe over Fabrics – це протокол, який передає набір команд NVMe через високошвидкісні мережеві транспортні мережі, або «фабрики», завдяки чому хости можуть отримувати доступ до віддаленого сховища NVMe з майже локальною продуктивністю. Замість того, щоб обмежувати пристрої NVMe прямим підключенням PCIe, NVMe-oF дозволяє отримати доступ до такої ж блискавичної продуктивності в мережевих фабриках.

Масиви NVMe стають спільними ресурсами, оскільки кілька серверів можуть використовувати один і той самий високошвидкісний пул сховища, не жертвуючи часом відгуку в мікросекундах.

Специфікація NVMe over Fabrics також підтримує ті ж ефективні набори команд, що й локальний NVMe. Ви зберігаєте всі ті характеристики продуктивності, які роблять NVMe особливим:

- Архітектура паралельної черги.
- Оптимізований стек протоколів.
- Можливості прямого доступу до пам'яті.

В результаті, інфраструктура більше не обмежується одним корпусом, а це означає, що обчислювальні системи та системи зберігання даних можуть розташовуватися в різних стійках або навіть у різних будівлях.

NVMe-oF проти традиційного NVMe: ключові відмінності

Традиційний NVMe підключається безпосередньо через PCIe з одним диском та одним хостом, що просто, але обмежує можливості.

Сервери NVMe поверх Fabric змінюють це. Ваша специфікація NVMe тепер працює в мережах Ethernet, Fibre Channel або InfiniBand, забезпечуючи таку ж ефективність протоколу, але з розширеним охопленням.

Традиційний NVMe:

- Тільки локальний доступ.
- Один хост на диск.
- Обмежено доступністю слота PCIe.
- Масштабування означає купівлю більшої кількості серверів.

NVMe-oF:

- Доступ по всій мережі.
- Кілька хостів спільно використовують сховище.
- Необмежений потенціал масштабування.
- Додайте потужність, не торкаючись обчислювальних ресурсів.

Ця технологія по суті перетворює локальне сховище на мережеве без типового зниження продуктивності.

Основні компоненти архітектури NVMe-oF

Побудова інфраструктури NVMe-oF вимагає трьох критично важливих елементів, які безперервно працюють разом.

1. Підсистеми та контролери NVMe формують основу. Кожна підсистема керує колекцією просторів імен (уявіть їх як віртуальні диски). Контролери обробляють фактичні операції вводу/виводу, підтримуючи ті паралельні черги, які дають NVMe перевагу в швидкості.

Ваша підсистема може містити десятки просторів імен. Кожен хост підключається до певних просторів імен на основі вимог до доступу, і всі вони керуються через одну ефективну платформу.

2. Рівень Storage Fabric об'єднує все разом. Незалежно від того, чи ви оберете конвергентний Ethernet, мережі зберігання даних (SAN) чи спеціалізовані мережі, цей рівень передає команди NVMe по мережі.

3. Технологія віддаленого прямого доступу до пам'яті (RDMA) забезпечує зв'язок з наднизькою затримкою, міняючи традиційні накладні витрати мережевого стеку.

Існує три основні варіанти RDMA:

- RoCE NVMe поверх Fabric (RDMA поверх конвергентного Ethernet) – працює з існуючою інфраструктурою Ethernet.
- iWARP – сумісний з TCP/IP, але менш поширений.
- InfiniBand – максимальна продуктивність, але вимагає спеціального обладнання.

Пояснення транспортних протоколів

Вибір транспортного протоколу визначає складність розгортання та потенціал продуктивності.

NVMe через Fibre Channel використовує існуючі інвестиції в SAN. Ви можете зберегти своє зонування, комутатори та інструменти керування. Просто оновіть прошивку, і система готова до роботи.

NVMe через TCP не потребує спеціального обладнання, і будь-яка мережа Ethernet його підтримує. Продуктивність не зрівняється з опціями RDMA, але ви все одно побачите значні покращення порівняно з iSCSI. Він ідеально підходить для віддалених офісів або хмарних розгортань, де спеціалізоване обладнання непрактичне.

NVMe поверх RoCE забезпечує продуктивність, близьку до InfiniBand, у мережах Ethernet. Вам знадобляться мережеві карти з підтримкою RoCE та конфігурацією Ethernet без втрат. Хоча налаштування складніше, ніж TCP, інвестиції варті того для робочих навантажень, чутливих до затримки.

Ключові переваги NVMe над Fabrics для корпоративних IT-технологій

NVMe-oF пропонує кілька ключових переваг, які змінюють підхід до проектування рішень для корпоративних IT:

- Радикальне скорочення затримки. Затримка може становити всього 10 мікросекунд для віддаленого доступу до сховища, тоді як у застарілій мережі зберігання даних вона вимірюється мілісекундами. Це 100-кратне покращення для критичних робочих навантажень.
- Масовий паралелізм. Кожне з'єднання підтримує 65 535 черг з 65 535 командами кожна.
- Справжня масштабованість. Ви можете додавати NVMe-диски до свого пулу без налаштування серверів або оновлювати обчислювальні ресурси без перенесення даних. Така архітектура дозволяє незалежне масштабування кожного рівня залежно від фактичних потреб.
- Захист інвестицій. Існуюча інфраструктура NVMe стає спільним ресурсом, доступним для всіх серверів у вашому середовищі, що максимізує використання та усуває невикористані потужності.

NVMe-oF у дії: варіанти використання

Організації розгортають NVMe-oF для робочих навантажень, які потребують продуктивності, що перевищує ту, яку можуть забезпечити традиційні сховища, у кількох ключових випадках використання:

- Навчання зі штучного інтелекту/машинного навчання (ШІ/МО) виграє від масивних паралельних потоків даних.
- Платформи аналітики в режимі реального часу обробляють поточкові дані без затримок буферизації. Наприклад, фінансові торгові системи можуть приймати рішення за мікросекунди.
- Інфраструктура віртуальних робочих столів забезпечує локальну продуктивність тисячам користувачів. Завдяки оптимізованим віртуальним робочим столам і тонким

клієнтам організації стикаються з меншою кількістю скарг на повільний вхід у систему або запуск програм.

– Кластери баз даних досягають раніше неможливої кількості операцій вводу/виводу за секунду (IOPS).

NVMe-oF проти інших архітектур сховищ

Порівняння NVMe-oF зі старими протоколами виявляє разючі відмінності в продуктивності:

iSCSI не може конкурувати за затримкою, оскільки додає накладні витрати TCP/IP, яких NVMe-oF уникає. У деяких випадках, перейшовши на NVMe-oF, можна досягти покращення затримки до 10 разів.

Традиційному Fibre Channel бракує ефективної структури команд NVMe. Навіть використовуючи одну й ту саму фізичну мережу, системи можуть мати суттєво різну продуктивність з NVMe-oF.

Масиви SAS/SATA досягають межі приблизно 100-200 тисяч IOPS. Кластери NVMe-oF забезпечують мільйони IOPS.

Міркування та проблеми розгортання

Незважаючи на всі переваги управління конфігурацією, успішне розгортання вимагає ретельного планування.

Ваша мережа повинна підтримувати передачу даних без втрат для протоколів RDMA. Комутатори потребують належного керування буфером та потоком. Сумісність драйверів та прошивок різних постачальників залишається складною, тому перед розгортанням у робочому середовищі ретельно протестуйте їх, порівнюючи веб- та хмарні рішення. Крім того, конфігурації з кількома шляхами потребують особливої уваги до NVMe.

Крім того, моделі безпеки відрізняються від традиційних мереж SAN, а варіанти шифрування під час роботи залежать від транспортного засобу. Тому важливо дотримуватися всіх застосовних правил кібербезпеки IT-інфраструктури та заздалегідь планувати стратегію автентифікації та шифрування.

У середовищі Fibre Channel технологія NVMe-oF підтримує протокол зв'язку NVMe-oF на FC-SAN (мережі зберігання даних Fibre Channel) з використанням існуючих мережевих пристроїв Fibre Channel.

Щоб налаштувати систему, що складається з хоста та системи зберігання даних, використовуючи протокол зв'язку NVMe-oF, зареєструйте логічний том системи зберігання даних як простір імен у підсистемі NVM, а потім налаштуйте маршрут вводу/виводу даних від хоста до логічного тому.

Звичайні Fibre Channel та iSCSI вимагають зіставлення LU для порту для керування маршрутом доступу між хостом і логічним томом. NVMe-oF, з іншого боку, вимагає налаштування наступних системних компонентів на системі зберігання даних між хостом і логічним томом.

– Підсистема NVM: Система керування флеш-пам'яттю, яка підтримує протокол зв'язку NVMe-oF з одним або кількома просторами імен та одним або кількома портами зв'язку (порти підсистеми NVM).

– Простір імен: простір флеш-пам'яті, відформатований у логічний блок.

– Порт підсистеми NVM: порт FC, налаштований на режим NVMe.

– Ідентифікація хоста (NQN хоста): кваліфікатор імені хоста.

– Шлях простору імен хоста: дозвіл на доступ до простору імен для кожного NQN хоста, зареєстрованого в підсистемі NVM.

Огляд безпеки простору імен

NVMe-oF дозволяє використовувати функції безпеки простору імен замість безпеки LUN, яка використовує звичайне з'єднання Fibre Channel (FC-SCSI).

Щоб використовувати функції безпеки простору імен, необхідно ввімкнути налаштування безпеки простору імен у підсистемі NVM. Вам не потрібно налаштовувати налаштування безпеки LUN для порту Fibre Channel.

Коли ввімкнено безпеку простору імен, логічний том, до якого хост може отримати доступ, визначається налаштуваннями NQN хоста для підсистеми NVM та простору імен. Хост може отримати доступ лише до логічного тому, призначеного підсистемі NVM та простору імен, для якого встановлено NQN хоста.

Обмеження на використання NVMe поверх FC

Конфігурації та налаштування мережі зберігання даних:

– NVMe-oF вимагає налаштування мережі зберігання даних Fibre Channel. Налаштування зонування комутатора FC та з'єднання оптоволоконного кабелю мають бути такими ж, як і для звичайного Fibre Channel. Існуючі функції зонування мережі доступні на рівні комутатора для пристрою NVMe-oF.

– Перевірте правильність конфігурації комутатора FC, дотримуючись інструкцій, наданих постачальником комутатора FC.

Конфігурації та налаштування хост-сервера:

– Хост, який підключається до цільової системи зберігання даних, має бути налаштований з ОС та адаптером шини хоста (HBA), що підтримують NVMe-oF. Щоб отримати додаткові відомості про комбінацію ОС та адаптера HBA, що підтримують підключення до системи зберігання даних, зверніться до служби підтримки клієнтів.

– Можливо, знадобиться встановити програмне забезпечення, необхідне для використання NVMe-oF, на хост або прошивку, а також драйвер для HBA. Після встановлення HBA його налаштування, можливо, знадобиться змінити. Дотримуйтесь інструкцій, наданих кожною ОС та постачальником HBA.

– Перевірка розпізнавання пристрою на хості може відрізнятися від звичайної перевірки Fibre Channel (FC-SCSI). Дотримуйтесь інструкцій для платформ, які підтримують підключення до системи зберігання даних.

Налаштування NVMe-oF:

– Операції з підготовки до роботи на NVMe-oF (підсистема NVM, порт підсистеми NVM, простір імен, налаштування NQN хоста тощо) не можуть бути реалізовані з Диспетчера пристроїв – Storage Navigator та Storage Advisor Embedded. Ці операції необхідно виконувати за допомогою Command Control Interface.

– Порт Fibre Channel для NVMe-oF не можна використовувати для деяких налаштувань хоста SCSI та деяких операцій Fibre Channel.

Додаткові обмеження:

– Перш ніж виконувати наступну операцію, переконайтеся, що на хості не виконуються операції вводу-виводу та що томи не змонтовано. Виконання операції під час виконання операції вводу-виводу або монтування тома призведе до відключення системи зберігання даних та хоста:

- Увімкнення безпеки простору імен.

– Перш ніж виконувати наступні операції, переконайтеся, що хост не виконує операції вводу-виводу та що не змонтовано жодних томів:

- Видалення простору імен

- Видалення шляху доступу (шляху простору імен хоста) між NQN хоста та простором імен

- Видалення порту підсистеми NVM

- Зміна швидкості передачі даних для порту Fibre Channel

- Зміна налаштування перемикача тканини

- Зміна топології

- Зміна режиму хоста

- Видалення групи хостів

– Перш ніж змінювати режим роботи порту, переконайтеся, що на порту каналу не виконуються такі операції:

- Додавання віддаленого шляху
- Додавання зовнішнього шляху

○ Налаштування з'єднання між системою зберігання даних і сервером, зареєстрованим у Storage Advisor Embedded

– Встановіть глибину черги хоста таким чином, щоб кількість множинних виконань команд становила 1024 або менше для кожного порту каналу. Значення вище 1024 може призвести до значного зниження продуктивності хоста, а потім до збою, такого як переривання завдання.

Налаштування NVMe через FC для хоста та системи зберігання даних

Щоб використовувати NVMe-oF як протокол зв'язку між хостами та системами зберігання даних, необхідно вказати певні параметри.

Рекомендації щодо керування підсистемою NVM як ресурсом керування сховищем

NVMe-oF вимагає реєстрації підсистеми NVM, яка не використовується у звичайних FC та iSCSI, як ресурсу керування сховищем. Ви несете відповідальність за створення груп ресурсів та розподіл ресурсів відповідно до операцій підсистеми NVM, таких як спільне використання або виключне використання підсистеми NVM користувачем або відділом сховища.

Дотримуйтесь цих інструкцій щодо керування підсистемою NVM як ресурсом сховища:

– Щоб включити підсистему NVM до групи ресурсів користувача, вкажіть ідентифікатор підсистеми NVM, який є номером керування підсистемою NVM у системі зберігання даних. Якщо ідентифікатор підсистеми NVM не переміщено до жодної групи ресурсів, підсистема NVM доступна як ресурс, призначений мета-ресурсом за замовчуванням.

– Щоб перенести ресурси, що використовуються для NVMe-oF, скористайтеся командою Command Control Interface `raidcom add resource`.

У наступному прикладі перенесено ідентифікатор 1 підсистеми NVM до групи ресурсів. `sql_srv`.

`raidcom` додати ресурс `-resource_name sql_srv -nvm_subsystem_id 1`

Щоб отримати додаткові відомості про те, як виконати команду Command Control Interface та вказати опцію, див. Посібник користувача та довідник з Command Control Interface та Довідник з команд Command Control Interface.

– Віртуальні сховища не підтримують протокол NVMe-oF. Ресурси, що використовуються для NVMe-oF, не можна перемістити до групи ресурсів, для якої встановлено віртуальний ідентифікатор як віртуальне сховище.

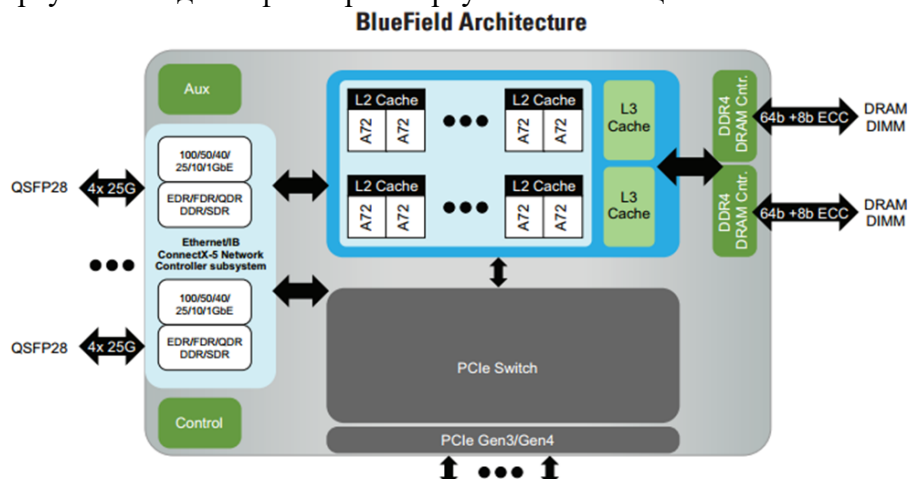


Рисунок 1 – Структурна схема системи

Налаштування порту Fibre Channel, з яким взаємодіє підсистема NVM

Ви можете налаштувати порт Fibre Channel, з яким зв'язується підсистема NVM:

1. Перевірте розрив з'єднання між хостом та портом цільового каналу.
2. Встановіть режим роботи порту на режим NVMe.
3. Встановіть топологію та швидкість каналу порту.

Встановлення режиму роботи порту Fibre Channel на режим NVMe

Ви можете налаштувати режим NVMe, щоб увімкнути зв'язок на порту Fibre Channel за допомогою протоколу NVMe-oF, а потім встановити порт Fibre Channel як порт підсистеми NVM у підсистемі NVM. Режим роботи порту за замовчуванням – це режим SCSI. Якщо змінити режим роботи порту на режим NVMe, наведені нижче параметри неможливо буде налаштувати. Обов'язково встановіть режим NVMe після виконання попередніх вимог.

- Підключення до порту адаптера хост-шини, який працює за протоколом FC-SCSI, або до зовнішнього порту на системі зберігання даних.
- Визначте шлях SCSI (додайте шлях LU).
- Змініть налаштування групи хостів за допомогою Диспетчера пристроїв – Навігатора сховища
- Додати віддалений шлях.
- Додайте зовнішній шлях.
- Налаштування з'єднання між системою зберігання даних та сервером, зареєстрованим у Storage Advisor Embedded.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів керування розподіленою СЗД за допомогою специфікації NVMe over Fabrics. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем керування розподіленою СЗД за допомогою специфікації NVMe over Fabrics.
- Досліджена система керування розподіленою СЗД за допомогою специфікації NVMe over Fabrics.
- На основі отриманих результатів досліджень створена програмна реалізація системи керування розподіленою СЗД за допомогою специфікації NVMe over Fabrics.

Розроблені алгоритми дозволяють успішно вирішувати завдання керування розподіленою СЗД за допомогою специфікації NVMe over Fabrics. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». Advanced Information Systems, 2023, 7(2), pp. 49-56.
2. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchov, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». CEUR Workshop Proceedings, Volume 3530, 2023, pp. 256-265.
3. Smirnov, O., Odarchenko, R., Smirnova, T., Bondar, S., Volosheniuk, D. «Optimal Structure Construction of Private 5G Network for the Needs of Enterprises». Lecture Notes on Data Engineering and Communications Technologies, 2023, 178, pp. 208–223.
4. Аль-Мудхафар Акіл Абдулхуссейн М., Смірнова Т.В., Буравченко К.О., Смірнов О.А. «Метод оцінки та підвищення користувацького досвіду абонентів в програмно-конфігурованих мережах на основі використання машинного навчання». Сучасні інформаційні системи, 2023, том 7, № 2, С. 49-56.
5. Smirnova, T., Gnatyuk, S., Yudin, O., Sydorenko, V., Polozhentsev, A., «The Model for Calculating the Quantitative Criteria for Assessing the Security Level of Information and Telecommunication Systems». CEUR Workshop Proceedings Volume 3156, 2022, Pages 390-399.
6. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». Проблеми інформатизації та управління,

№ 2(70). 2022. С. 28-37.

7. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 3(69). С. 93-98.
8. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Вісник Хмельницького національного університету. Серія: «Технічні науки», № 2 (307). С. 46-52. 2022.
9. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 1(67). С. 84-89.
10. Smirnova T., Gnatyuk S., Berdibayev R., Avkurova Zh., Iavich M. «Cloud-Based Cyber Incidents Response System and Software Tools». Communications in Computer and Information Science, 2021, vol 1486. Springer, Cham. pp 169-184.
11. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
12. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». Journal of theoretical and applied information technology Vol.98. No 21, 2020, P. 3334-3346.
13. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177.
14. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587.
15. Smirnov, O., Markovets, O. Vovk, N., Turchyn, Y., «Model of informational support for social network administrators' content creation». CEUR Workshop Proceedings Volume 2616, 2020, Pages 125-136.
16. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». CEUR Workshop Proceedings Volume 2616, 2020, Pages 366-379.
17. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645.
18. Smirnov O. Kuznetsov A., Zaichenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019; Odessa; Ukraine; 9-13 September 2019. P.22-28.
19. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.
20. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019 . P.517-522.
21. Smirnov, O., Odarchenko, R., Abakumova, A., Usik, P., Kundyz, M., «QoE optimization technique for media delivery in 5G networks». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019. P.597-601.
22. Smirnov, O., Krasnobayev, V., Yanko, A., Kuznetsova, T. «Methods of nulling numbers in the system of residual classes». CEUR Workshop Proceedings, Vol 2588, P. 90-106, 2019.
23. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Averchev, A., Pastukhov, M., Kuznetsova, K., «Formation of Pseudorandom Sequences with Special Correlation Properties», 2019 3rd International Conference on Advanced Information and Communications Technologies, AICT -2019/ Lviv, Ukraine, 2-6 July, 2019, P. 395-399.
24. Smirnov, O., Kuznetsov, A., Kiian, A., Zamula, A., Rudenko, S., Hryhorenko, V., «Variance Analysis of Networks Traffic for Intrusion Detection in Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 353-358.
25. Smirnov, O., Kuznetsov, A., Kavun, S., Babenko, B., Nakisko, O., Kuznetsova, K., «Malware Correlation Monitoring in Computer Networks of Promising Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 347-352.
26. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Pastukhov, M., Kuznetsova, K., Prokopovych-Tkachenko, D., «Discrete Signals with Special Correlation Properties», CEUR Workshop Proceedings Volume 2353, CEUR

- Workshop Proceedings 2019, Pages 618-629.
27. Smirnov A.A., Kuznetsov A.A., Danilenko D.A., Berezovsky A., «The statistical analysis of a network traffic for the intrusion detection and prevention systems», Telecommunications and Radio Engineering. – Volume 74, Issue 1. – Begel House Inc. – 2015. – P. 61-78.
 28. Смірнов О.А., Смірнова Т.В., Буравченко К.О., Кравченко С.С., Горбов В.О., «Хмарна система підтримки прийняття рішень технологічного процесу відновлення поверхонь конструкцій і деталей машин». Сучасні інформаційні системи. 2021. Т. 5, № 4. С. 79-95
 29. Смірнов О.А., Усік П.С., Миронець І.В., Буравченко К.О., Якименко Н.М. «Метод підвищення ефективності розподіленої обробки даних у комп'ютерних системах операторів стільникового зв'язку» Вісник Черкаського державного технологічного університету. Технічні науки. №4. С. 103-110. 2020.
 30. О.А.Смірнов, Т.В.Смірнова, Л.І. Поліщук, К.О. Буравченко, А.О.Макевнін, «Дослідження хмарних технологій як сервісів», Кібербезпека: освіта, наука, техніка. № 3(7). С. 43-62. 2020.
 31. Смірнов О.А., Коноплицька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Поліщук Л.І. Інформаційна безпека в комп'ютерних мережах. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2020. – 294 с.
 32. О.А. Смірнов, П.С. Усік, «дослідження перспектив використання технологічних рішень в мережах 5g» у Кібербезпека та інформаційні технології: монографія. – Х. : ТОВ «ДІСА ПЛЮС», 2020.С. 122-135.

ЗМІСТ

П.Лобода

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ІЄРАРХІЧНОГО ЗБЕРІГАННЯ ДАНИХ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ TIERED STORAGE	4

В.Маламуж

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ УПРАВЛІННЯ У РОЗПОДІЛЕНИХ CLOUD-СИСТЕМАХ GENI	12

Б.Марченко

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПРИ ДОСТУПІ ДО WEB-СЕРВЕРУ ЗА РАХУНОК ОПОРТУНІСТИЧНОГО ШИФРУВАННЯ	22

Ю.Молчанов

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ SOFTWARE DEFINED STORAGE	30

В.Мороз

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ІНТЕЛЕКТУАЛЬНОГО КЕРУВАННЯ КАБЕЛЬНОЮ ІНФРАСТРУКТУРОЮ AIM	38

А.Мукієнко

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ХМАРНОГО СЕРВІСУ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ РОЗУМНОГО БУДИНКУ	45

Д.Нагірняк

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ІНТЕЛЕКТУАЛЬНОГО АРКАДНОГО МУЛЬТИМЕДІА ПРОЕКТУ НА ОСНОВІ ФРЕЙВОРКУ PHASER	54

А.Норов

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ІОТ З ВИКОРИСТАННЯМ BLUETOOTH	64

С.Олексієнко

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ КОМПЛЕКСНИХ ІНТЕЛЕКТУАЛЬНИХ РІШЕНЬ ДЛЯ ВІДЕОНАГЛЯДУ	72

В.Оніщук

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ РИЗИКІВ БЕЗПЕКИ ПРИ ВИКОРИСТАНІ МІЖМЕРЕЖЕВИХ ЕКРАНІВ	81

О.Осуський

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ МЕРЕЖЕВОГО УПРАВЛІННЯ КОРПОРАТИВНИМИ ВІДЕОРЕСУРСАМИ НА ОСНОВІ ТЕХНОЛОГІЇ EVRP	90

В.Павлюхін

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ КОНТЕЙНЕРНОЇ ВІРТУАЛІЗАЦІЇ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ДЛЯ ХОСТИНГУ	96

О.Бершадський

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ЕМУЛЯТОРА ПЕРЕТВОРЕННЯ ЛОГІЧНОЇ АДРЕСИ В ЛІНІЙНУ ТА ЛІНІЙНОЇ У ФІЗИЧНУ ДЛЯ НАВЧАЛЬНИХ ЦІЛЕЙ	103

В.Плужник

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ ТА ДОСТУПОМ ДО МЕРЕЖЕВИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ	111

*Б.Подольн*ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ПРОЕКТУВАННЯ ТА ПОБУДОВИ
ТОПОЛОГІЇ МЕРЕЖ У ЦЕНТРАХ ОБРОБКИ ДАНИХ 123*С.Приймак*ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ОНЛАЙН-СЕРВІСУ ДЛЯ
РЕДАГУВАННЯ ЗОБРАЖЕНЬ ЗА ДОПОМОГОЮ ШТУЧНОГО ІНТЕЛЕКТУ 130*Є.Прокопенко*ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ АПАРАТНО-ПРОГРАМНИХ КОМПЛЕКСІВ
ДЛЯ ВИЯВЛЕННЯ АТАК НА РІВНІ ІОТ-ПРИСТРОЇВ З ВИКОРИСТАННЯМ КВАНТОВАНИХ
НЕЙРОМЕРЕЖ 139*Д.Радін*ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ АПАРАТНО-ПРОГРАМНИХ ЗАСОБІВ
ОТРИМАННЯ ФОТОЗОБРАЖЕННЯ, ЙОГО СТИЛІЗАЦІЇ ТА ВІДТВОРЕННЯ ЗА
ДОПОМОГОЮ РЕАЛІЗАЦІЇ ПРИСТРОЮ ІОТ ПЛОТТЕРУ 147*М.Рисований*ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ПОБУДОВИ ПРОГРАМУЄМОЇ
МЕРЕЖІ SDN НА БАЗІ SD-WAN 152*А.Розиєв*ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ БЕЗПЕЧНОЇ РОЗРОБКИ ПРИ
ВИКОРИСТАННІ ТЕХНОЛОГІЇ AGILE 161*Я.Рябовол*ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ВІРТУАЛІЗАЦІЇ ОБ'ЄДНАНИХ
КОМУНІКАЦІЙ У МЕРЕЖІ 171*О.Семенюк*ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ЗБЕРІГАННЯ ДАНИХ SAN НА
ОСНОВІ СТАНДАРТУ FC GEN 182*М.Скрипка*ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ІНТЕЛЕКТУАЛЬНОГО
КЕРУВАННЯ ЦИФРОВИМИ ПРАВАМИ НА ОСНОВІ DRM 189*Р.Слабінога*ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ІНТЕЛЕКТУАЛЬНОГО
МОНІТОРИНГУ ТА ЗАПОБІГАННЯ АКТИВНОСТІ ДОДАТКІВ 198*О. Сопіна*ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ЗБОРУ ТА ОБРОБКИ АНАЛІТИКИ
ВІД МЕРЕЖІ WI-FI 211*О.Сосна*ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ КОНТРОЛЮ ІНТЕРНЕТ ШЛЮЗІВ
НА БАЗІ ОС UBUNTU 220*С.Талмазан*ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ПРОТИДІЇ МЕРЕЖЕВИМ DDOS-
АТАКАМ 228*Д.Татаров*ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ВИЗНАЧЕННЯ КОНТЕКСТУ
КОРИСТУВАЧА НА ОСНОВІ АРХІТЕКТУРИ CODA 239

Б.Турик

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ВІРТУАЛІЗАЦІЇ МЕРЕЖІ NUAGE NETWORKS 254

С.Фоменко

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ПРОТИДІЇ ЗЛОВМИСНИМ ПРОГРАМАМ З ВИКОРИСТАННЯМ МЕТОДІВ МАШИННОГО НАВЧАННЯ 261

М.Хромочкін

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ МЕРЕЖЕВОГО ВІДЕОСПОСТЕРЕЖЕННЯ НА ОСНОВІ ВИКОРИСТАННЯ DIRECTX 270

Д.Хуторний

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ПІДВИЩЕННЯ НАДІЙНОСТІ ЗБЕРЕЖЕННЯ ІНФОРМАЦІЇ НА SSD ДИСКАХ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ RAID 281

М.Черкашин

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ НАДАННЯ ХМАРНИХ ПОСЛУГ НА БАЗІ CISCO HYPERFLEX 291

А.Шарова

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ КЕШУВАННЯ, ФЛЕШ-ТЕХНОЛОГІЇ ТА РЕПЛІКАЦІЇ ЦОД 303

А.Яковенко

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ КЕРУВАННЯ РОЗПОДІЛЕНОЮ СЗД ЗА ДОПОМОГОЮ СПЕЦИФІКАЦІЇ NVME OVER FABRICS 313