

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ
ТЕХНІЧНИЙ УНІВЕРСИТЕТ



Збірник
праць молодих науковців
ЦНТУ

Випуск 16
Частина 1



МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

**Збірник
праць молодих науковців
ЦНТУ**

Випуск 16
Частина 1

Кропивницький – 2026

Збірник праць молодих науковців ЦНТУ. – Вип. 16, ч.1 – Кропивницький: ЦНТУ, 2026 – 308 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 378.005.92

О. Коломієць, к.пед.н., доцент

В. Рябовол, магістр гр. ІС-24 М (1,4)

Центральноукраїнський національний технічний університет

ВИКОРИСТАННЯ ЗАРУБІЖНОГО ДОСВІДУ КОНТРОЛЮ ЯКОСТІ ОСВІТНЬОЇ ДІЯЛЬНОСТІ

У статті розглянуто проблему забезпечення якості освітніх послуг у вищій школі. Акцентовано увагу на необхідності вивчення зарубіжного досвіду контролю якості освітньої діяльності, порівняння результатів функціонування освітньої системи України з національними освітніми системами інших держав. Визначено важливі орієнтири розвитку вищої освіти в Україні згідно з вимогами інноваційного розвитку суспільства в цілому, що мають забезпечувати й особистісний розвиток людини в процесі навчання протягом життя.

заклад вищої освіти, освіта, контроль якості, система управління якістю вищої освіти, стандарти якості, стратегії управління

Актуальність статті. В наш час зростає роль інтелектуального потенціалу, знань, високих технологій. З'являється потреба у фахівцях нової якості та їх швидкої адаптації до нових суспільних реалій. Проблема якості освітніх послуг постає як один з ключових запитів суспільства. Актуальність цієї проблеми лише підсилюється в умовах глобалізації, активного впровадження інноваційних технологій, динамічного суспільного поступу.

Нині європейські країни спрямовують зусилля на посилення привабливості Єдиного європейського освітнього простору, дбаючи про формування спільної системи управління якістю вищої освіти. Виникає необхідність вивчення зарубіжних освітніх практик, дослідження процесів контролю якості освіти, можливостей використання іноземного досвіду вітчизняними ЗВО.

Мета статті. Ознайомитися з міжнародними освітніми практиками контролю якості освітніх послуг, розкрити перспективи використання зарубіжного досвіду забезпечення якості освіти вітчизняними ЗВО.

Якість освіти – це категорія багатоаспектна. Вона включає низку складників, які є показниками якості: системи управління освітою; змісту освіти; методів і технологій навчання; знань, способів вирішення завдань; механізмів контролю якості освітньої діяльності тощо. Європейський центр із вищої освіти ЮНЕСКО (СЕПЕС) вимогами до якості освіти вважає також: «інституціональну місію й мету закладу освіти; параметри освітньої моделі, програми або дисципліни; гарантоване виконання базових стандартів та еталонів; прагнення до постійного вдосконалення навчального процесу; якість персоналу; якість інфраструктури та умов реалізації освітнього процесу в конкретному закладі освіти» [1;50].

Ідея розробки стратегії управління якістю освіти в Європейському Союзі (ЄС) має досить тривалу історію (з 1985 року), коли у Великій Британії, Франції і Нідерландах було ініційовано процеси із забезпечення якості освіти у вищій школі. У 1994 – 1998 рр. було реалізовано пілотний проєкт Європейського Союзу із забезпечення якості освіти, підсумком якого стало прийняття Радою міністрів з освіти ЄС «Рекомендацій про Європейське співробітництво в забезпеченні якості вищої освіти (98/561/ЕС)». Далі відбулося підписання європейськими країнами низки декларацій щодо реформ у вищій освіті, започаткування Європейської мережі агентств з якості освіти.

В основу європейської системи управління якістю вищої освіти покладена так звана американська модель, що поєднує внутрішнє самооцінювання якості в межах певного закладу освіти і зовнішню оцінку діяльності ЗВО з точки зору його відповідальності перед

суспільством. Система освіти у США характеризується тісним зв'язком із великими корпораціями, різними фірмами. Як правило, діяльність ЗВО забезпечується місцевим законодавством того чи іншого штату.

Регулятором системи освіти постає суспільство, яке через потребу роботодавців у трудових ресурсах формує відповідні запити до закладів вищої освіти й здійснює контроль за якістю фахової підготовки. У ЗВО працюють служби підтримки працевлаштування випускників. На педагога покладається відповідальність за рівень викладання окремих дисциплін у ЗВО. Програми навчальних дисциплін схвалюються радою факультету, деканом, університетською комісією з навчальних планів. Проте, здебільшого цей розгляд має формальний характер. Зовнішній контроль за якістю навчання здійснюється комісіями, що формуються з числа випускників, викладачів інших ЗВО, членів опікунської ради. [3].

Кожна європейська країна напроцювала власні підходи до контролю якості освіти та оцінювання її результатів.

Так, Німеччина презентує дуальну модель професійної освіти, побудовану на зв'язку системи професійного навчання з виробничими процесами конкретного підприємства. В рамках дуальної системи перелік освітніх програм визначається відповідно до економічних потреб і в тісній взаємодії з партнерами на різних рівнях. Траєкторія та зміст освітніх програм ґрунтується на вимогах, які згодом висуватимуться до потенційних працівників. А сама підготовка фахівців здійснюється на основі паралельного навчання у вищій школі та на підприємствах. Модель дуальної освіти в Німеччині є національною програмою, що фінансується з бюджету.

У Франції більшість здобувачів обирає університетську освіту, що обумовлено високою якістю навчання та наданням необмежених можливостей, які відкриваються перед випускниками університетів. У Франції дуже високий рівень вимог до рівня знань студентів, проте французька система дозволяє здобувачам освіти формувати індивідуальний навчальний план, доповнюючи обов'язкові дисципліни предметами за вибором. Французька система вищої освіти має також чітку практичну орієнтацію освітніх програм, які включають обов'язкове стажування, під час проходження якого студентам пропонується перетворити знання у навички і довести їх до досконалості на реальних прикладах.

Повністю відповідає європейським стандартам система освіти у Польщі. Популярність отримання вищої освіти тут пояснюється високою якістю навчання і чудовими перспективами в плані подальшого працевлаштування. Дипломи випускників ЗВО дійсні у всіх країнах ЄС, що значно розширює можливості фахівців і збільшує їх шанси на отримання престижної роботи. Висока якість освіти в польських ЗВО забезпечується за рахунок: відповідності матеріальної та методичної бази до європейських порядків; обов'язкового виконання програм двома мовами (польською та англійською); високим рівнем кваліфікації професорсько-викладацького складу.

Загальною тенденцією в організації освітнього процесу європейських ЗВО є відмова від жорсткої регламентації структури і змісту програм, введення гнучких систем навчання. Цей досвід активно впроваджують й вітчизняні заклади вищої освіти, зокрема і ЦНТУ.

Згодом було розроблено та узгоджено стандарти, рекомендації та процедури із забезпечення та оцінки якості освіти – European quality assurance standards and guidelines (ESG). Їхнє головне призначення полягає у наданні допомоги та визначенні орієнтирів як для закладів вищої освіти, що розробляють власні системи забезпечення якості, так і для агенцій, які здійснюють незалежний контроль й оцінювання якості.

Міжнародним стандартом ISO 21001:2018 визначено фундаментальні засади щодо створення внутрішньої системи гарантування якості у закладі освіти на основі процесного підходу. Увагу до процесного підходу можна пояснити тим, що він, на думку науковців, гарантує ефективність результатів завдяки «здійсненню управління ресурсами і діяльністю як процесом» [2].

Запровадження політики підтримки системи контролю якості освітньої діяльності у закладах вищої освіти має ґрунтуватися на засадах студентоцентрованого освітнього

середовища, традиціях і культурі ЗВО, системі ціннісних орієнтирів, що зумовлюють поведінку закладу освіти на освітньому ринку. Усе це має гарантувати ефективне виконання місії та стратегії закладу вищої освіти, прокласти шлях у майбутнє.

Отже, актуальним завданням є впровадження стратегії безперервного покращення якості, до якої мають бути долучені усі зацікавлені особи; задіяні механізми погодження, контролю та моніторингу власних програм контролю якості освіти.

Щодо зовнішньої оцінки ЗВО, то необхідно зазначити про відповідність всіх процедур меті і завданням, а будь-яких рішень розробленим критеріям оцінювання, що застосовуються однаково для всіх. Результати зовнішньої оцінки у формі зведень з опису та аналізу виявлених даних оприлюднюються агенствами з гарантування якості, що мають повноваження для провадження зовнішнього оцінювання. Ці агенства діють на основі встановлених правових норм й отримують визнання з боку компетентних органів влади європейського простору вищої освіти.

У Великій Британії Агенство забезпечення якості вищої освіти (QAA) – це незалежний орган, на який покладено відповідальність за перевірку стандартів та якості вищої освіти. Агенство проводить огляди оцінки якості, розробляє посібники, проводить відповідні дослідження.

Особливе місце у європейській практиці оцінювання якості освіти посідає акредитація закладів освіти. Більшість національних акредитаційних структур мають незалежний статус, залучають зовнішніх експертів, проводять спільну зі ЗВО експертизу, публікують звіти.

Як правило, акредитація спрямовується на освітні програми (програмна, спеціалізована акредитація) і на ЗВО (інституційна акредитація). В різних освітніх системах співвідношення між обома типами акредитації вибудовується неоднаково. За останній період намітилася тенденція до їх поєднання (суміщення). Продовжується пошук необхідного балансу, оскільки просте інституційне оцінювання не досягає базових основ діяльності ЗВО, а програмне оцінювання може обернутися для багатьох ЗВО зайвим адміністративним тягарем.

Отже, у зарубіжних країнах створені та успішно функціонують національні системи оцінювання якості освіти. Ці системи, як правило, є достатньо незалежними від органів управління освітою, вони продукують цілком об'єктивну інформацію, яку використовують для корегування стратегії і тактики освітніх політик, дослідження результативності освітнього процесу, удосконалення діяльності закладів освіти.

Аналіз існуючих зарубіжних систем контролю якості вищої освіти підтверджує різноманітність та специфіку повноважень відповідних організацій, зайнятих їх забезпеченням. Традиційний комплекс реалізованих ними завдань включає покращення якості освітньої діяльності в контексті суспільних потреб; надання ресурсної підтримки та інформаційного супроводу закладам вищої освіти для реалізації різноманітних програм контролю якості освіти; поширення кращих практик та інновацій.

Аналіз Європейських стандартів гарантування якості вищої освіти дає можливість визначити ключові вимоги й тенденції розвитку європейської системи контролю якості освіти в Україні. Йдеться про:

- чітку окресленість політики забезпечення якості;
- визначення стратегічних цілей, змісту окремих процедур і виконавців;
- безумовне дотримання критеріїв діяльності із забезпечення якості;
- дієва система постійного спостереження, контролю та аналізу;
- доступність і відкритість інформації з проблем якості освіти.

Виконання цих вимог потребує реалізації низки важливих заходів:

- створення Національного освітнього центру акредитації;
- підвищення міжнародного статусу України у системі зовнішнього забезпечення якості;

- створення та впровадження механізмів правового регулювання участі зацікавлених осіб у процедурі дотримання соціальної відповідальності за рівень освітнього сервісу;
- активне залучення здобувачів освіти до національних служб якості освіти;
- запровадження моніторингу якості вищої освіти (на постійно діючій основі);
- удосконалення системи контролю й оцінювання ефективності освітньої діяльності ЗВО, гарантування її відкритості та прозорості.

Отже, кожна країна має право самостійно вирішувати питання щодо гарантування якості вищої освіти беручи до уваги національну специфіку. У питанні вироблення стандартів якості освіти Україна мусить наближати і поєднувати власні напрацювання та сучасний зарубіжний досвід. Тому вважаємо доцільним посилити увагу до розробки систем менеджменту якості; функціонування незалежних агентств з питань надання якісних освітніх послуг; створення різнорівневих систем якості.

Список літератури

1. Гарашук О. В., Куценко В. І. Якісна освіта – інструмент сталого розвитку (зарубіжний досвід та українські реалії). Науковий вісник Ужгородського національного університету. Серія: Міжнародні економічні відносини та світове господарство, 2019. Вип.1, частина 1. С. 49-55/50
2. Іванишин А. В. Європейські та міжнародні підходи до управління якістю освіти з використанням інтелектуальних технологій. URL: <https://science.lpnu.ua/sites/default/files/journal-paper/2023/mar/29952/stattyaiivanyshyn2023.pdf>.
3. Локшина О. І. Моніторинг якості освіти: світові досягнення та українські перспективи / О. І. Локшина. Київ. К.І. С.2004. 128с.

УДК 02.004.8

О. Коломієць, к.пед.н., доцент

К. Сипко, магістр гр. ІС-24 М (1,4)

Центральноукраїнський національний технічний університет

ШТУЧНИЙ ІНТЕЛЕКТ ЯК ІНСТРУМЕНТ ПІДТРИМКИ ІНФОРМАЦІЙНОГО ОБСЛУГОВУВАННЯ КОРИСТУВАЧІВ

У статті здійснено порівняльний аналіз традиційної та інтелектуалізованої моделей інформаційного обслуговування. Досліджено еволюцію інструментарію від алгоритмічних пошукових систем до генеративних моделей. Обґрунтовано ефективність впровадження архітектури RAG для мінімізації ризиків «галюцинацій» ШІ в управлінській діяльності.

штучний інтелект, інформаційне обслуговування, семантичний пошук, RAG, великі мовні моделі, порівняльний аналіз, цифровізація.

Актуальність статті. Сучасна цифрова парадигма характеризується не лише експоненційним зростанням обсягів даних (за прогнозами IDC [4], глобальна датасфера перевищить 175 зетабайт до 2025 року), але й кризою традиційних методів їх обробки. Класичні системи документообігу та пошуку, побудовані на індексації ключових слів, стикаються з проблемою «семантичного розриву» — нездатності системи зрозуміти контекст запиту користувача. Це зумовлює необхідність переходу до нових технологічних рішень на базі штучного інтелекту (ШІ).

Мета статті. Провести системний аналіз інструментів ШІ, порівняти їх функціональні можливості з традиційними засобами та визначити оптимальні моделі їх інтеграції в процеси інформаційного обслуговування.

Виклад основного матеріалу. Трансформація інформаційного обслуговування під впливом ШІ відбувається не шляхом простої автоматизації рутинних операцій, а через зміну когнітивної моделі взаємодії «людина-система». Якщо традиційні автоматизовані системи (АС) працюють за жорстко детермінованими алгоритмами (if-then), то інтелектуальні системи на базі машинного навчання (ML) здатні адаптуватися до непередбачуваних запитів.

На основі проведеного дослідження нами було розроблено класифікацію інструментів ШІ, які інтегруються в сучасні інформаційні сервіси (Рис. 1).

Особливої уваги потребує порівняльний аналіз технологій пошуку. Традиційний **лексичний пошук** (keyword search) є ефективним лише за умови точного співпадіння термінології користувача та автора документа. Натомість, **семантичний пошук** на базі NLP (Natural Language Processing) використовує векторне представлення слів, що дозволяє знаходити релевантні документи навіть за відсутності спільних ключових слів, орієнтуючись на зміст (інтент).

Аналогічна еволюція спостерігається у сфері комунікації. Перше покоління чат-ботів (скриптові боти) вимагало від користувача руху по заданому «дереву рішень». Сучасні ж великі мовні моделі (LLM) забезпечують вільний діалог. Проте, як зазначають дослідники [1; 2], головним недоліком генеративних моделей є схильність до фактологічних помилок («галюцинацій»).

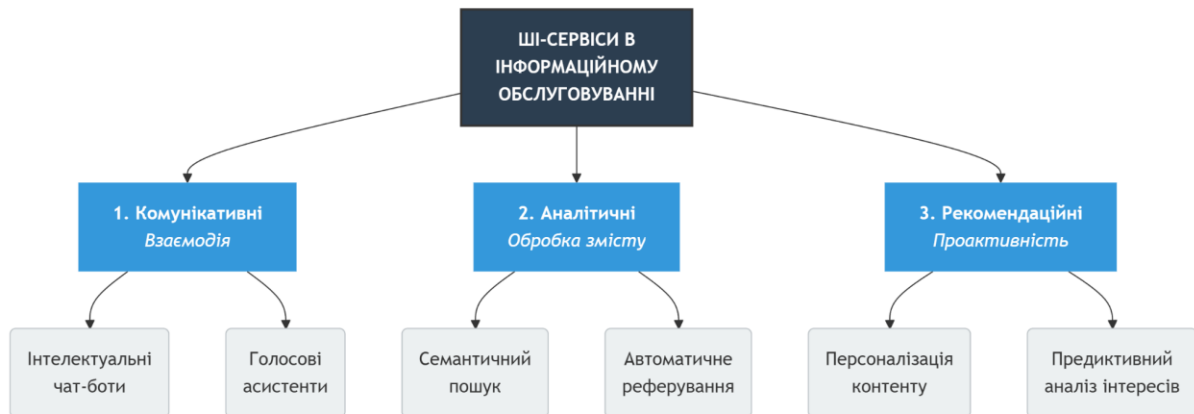


Рис. 1. Класифікація інструментів ШІ в інформаційному обслуговуванні

Для нівелювання цього ризику в корпоративному та державному секторі доцільно використовувати не «чисті» моделі (як ChatGPT), а гібридну архітектуру **RAG (Retrieval-Augmented Generation)**. Суть методу полягає в тому, що генеративна модель не вигадує відповідь, а синтезує її виключно на основі перевірених даних, знайдених у внутрішній базі знань установи.

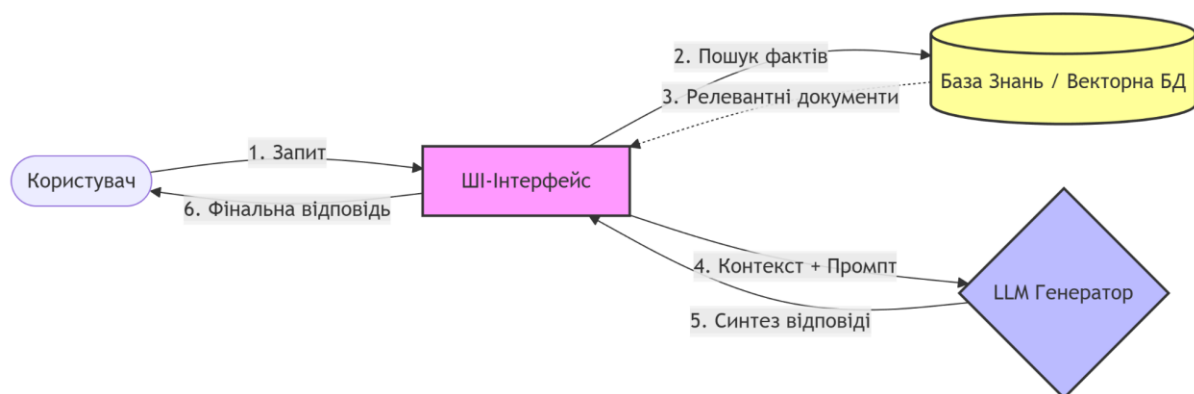


Рис. 2. Архітектура системи з верифікацією даних (RAG)

Цей підхід поєднує гнучкість генеративного ШІ з надійністю традиційних баз даних. Узагальнюючи результати дослідження, ми провели порівняльний аналіз зміни парадигми обслуговування (Таблиця 1).

Таблиця 1 – Порівняльна характеристика моделей інформаційного обслуговування

Критерій порівняння	Традиційна модель	Інтелектуалізована (ШІ) модель	Аналіз змін
Принцип дії	Реактивний	Проактивний	Система не чекає запиту, а передбачає потребу на основі аналізу поведінки.
Механізм пошуку	Синтаксичний (співпадіння символів)	Семантичний (співпадіння сенсів)	Подолання проблеми синонімії та полісемії слів.
Персоналізація	Статична (анкетні дані)	Динамічна (поведінковий профіль)	Формування рекомендацій у реальному часі.
Доступність	Обмежена робочим часом	24/7	Повна автоматизація консультацій першого рівня.

Як свідчать дані таблиці, перехід до інтелектуалізованої моделі дозволяє вирішити проблему інформаційного шуму: замість списку з тисяч посилань користувач отримує синтезовану, верифіковану відповідь.

Висновки. Проведений аналіз дозволяє стверджувати, що інтеграція ШІ в інформаційне обслуговування є якісним стрибком, а не простою модернізацією. Ключовою перевагою є перехід від реактивного надання доступу до фондів до проактивного управління знаннями. Разом з тим, безконтрольне використання генеративних моделей несе ризики дезінформації, що вимагає впровадження архітектурних рішень типу RAG та обов'язкового збереження контролю людини (Human-in-the-Loop) над критично важливими процесами.

Список літератури

1. Про схвалення Концепції розвитку штучного інтелекту в Україні : Розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р. URL: <https://zakon.rada.gov.ua/laws/show/1556-2020-p>.
2. Мар'єнко М. В., Коваленко В. В. Штучний інтелект та відкрита наука в освіті. Фізико-математична освіта. 2023. Т. 38. № 1. С. 48–53. URL: <https://fmo-journal.org/index.php/fmo/article/view/225>.
3. Reinsel D., Gantz J., Rydning J. The Digitization of the World – From Edge to Core: IDC White Paper. Framingham: International Data Corporation, 2018. 28 p. URL: <https://www.seagate.com/files/www-content/our-story/trends/files/dataage-idc-report-final.pdf>.
4. Recommendation on the Ethics of Artificial Intelligence. Paris: UNESCO, 2021. 60 p. URL: <https://unesdoc.unesco.org/ark:/48223/pf0000381137>.

УДК 069.53-028.27:930

О. Коломієць, к. пед. н., доцент

Т. Щетініна, здобувачка вищої освіти II курсу гр. ІС-24Мз

Центральноукраїнський національний технічний університет

ПРАВОВІ ЗАСАДИ ДОКУМЕНТАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ЗВЕРНЕНЬ ГРОМАДЯН В ОРГАНИ ПУБЛІЧНОЇ ВЛАДИ

У статті досліджено правові засади документаційного забезпечення звернень громадян в органи державної влади та місцевого самоврядування. Визначено основні чинники впливу на появу підзаконного-нормативно правового акту, який встановлює норми практичної діяльності із документаційного забезпечення звернень громадян в органи публічної влади.

Нормативно-правові акти, документаційне забезпечення, звернення громадян, комунікація.

Постановка проблеми. Робота органів публічної влади із зверненнями громадян є складовою щоденної діяльності посадовців, у якій вони спираються на багаторічний досвід, уніфіковані підходи та чітко налагоджену систему документаційного забезпечення. Системний розвиток в українському суспільстві питання звернення громадян та його документаційного забезпечення стало можливим завдяки належному правовому регулюванню. Правовий фундамент документаційного забезпечення звернень громадян в органи публічної влади становлять норми Конституції України та Закон України «Про звернення громадян». На особливу увагу заслуговує підзаконний нормативно-правовий акт, положення якого втілюють засади практичного забезпечення документування роботи із зверненнями громадян.

Аналіз останніх досліджень та публікацій. Питання теоретичного обґрунтування та практичного впровадження належного документаційного забезпечення звернень громадян є предметом всебічного дослідження науковців. Фундаментом формування комплексного підходу до вивчення всіх аспектів роботи з документами щодо звернень громадян є питання правового характеру. Зокрема, науковцями Міняйло М. [1], Петровою І. О[2],Соболь В.А.[3] деталізовано ряд питань унормування права громадян на звернення. У межах цих досліджень розкрито, у тому числі, правові засади документаційного забезпечення звернень громадян до органів публічної влади. Але з часом все більшу увагу науковців починають привертати питання практичної реалізації роботи із документами із звернення громадян в установах та організаціях публічної сфери. Це позначилось появою методичних рекомендацій для забезпечення практики реалізації роботи з відповідними документами[4]. Із розвитком в Україні засад електронної демократії та електронного урядування постала необхідність висвітлити проблему реалізації електронних звернень громадян, що було зроблено рядом науковців[1]. Зазначимо, що поданий короткий огляд публікацій за темою дослідження залишає відкритим питання щодо багатьох аспектів документаційного забезпечення звернення громадян в сфері публічного управління.

Мета й завдання дослідження. Проаналізувати стан правового регулювання документаційного забезпечення звернень громадян в Україні.

Завданнями роботи є: проаналізувати науковий стан розробки проблеми правового регулювання документаційного забезпечення звернень громадян до органів публічної влади; систематизувати та проаналізувати групи законодавчих та нормативно-правових актів, які врегульовують принципи та порядок документаційного забезпечення звернень громадян;

визначити шляхи удосконалення правової роботи у цій сфері.

Об'єктом дослідження є діяльність органів публічної влади щодо документування звернень громадян.

Предметом дослідження виступає документаційне забезпечення письмових, особистих звернень громадян та звернень у форматі електронних петицій.

Виклад основного матеріалу. Правову основу документаційного забезпечення звернень громадян складають цілий ряд законодавчих актів. Фундаментальну основу становить стаття 40 Конституції України, яка встановлює основоположні гарантії прав людини і громадянина на звернення до органів державної влади, органів місцевого самоврядування, посадових і службових осіб органів публічної влади. Визначено, що такі звернення можуть бути викладені письмо індивідуально чи колективно, а також це можуть бути особисті звернення, які реалізуються у ході особистого прийому громадян або уповноважених ними осіб (наприклад, адвокатів) керівниками органів влади, керівниками підприємств, установ і організацій. Норми Конституції України зобов'язують всі органи публічної влади та їх посадових осіб, а також інших суб'єктів (підприємства, організації незалежно від форми власності) розглянути звернення та надати обґрунтовану відповідь у встановлений законом строк.

Закон України «Про звернення громадян»[1] було прийнято у тому ж 1996 році, що і Конституцію України. У його нормах дістали подальшого розвитку конституційні засади побудови демократичного суспільства шляхом відкритого та конструктивного діалогу з громадськістю через звернення громадян до органів публічної влади. Потрібно зауважити, що значення вказаного законодавчого акту тільки зростає, адже у зв'язку з появою формату звернень у вигляді електронних петицій, до закону було внесено суттєві доповнення, які сформували правову основу для процедури розгляду та збереження документів за результатами надходження цифрових звернень громадян.

У практичній площині реалізація документаційного забезпечення звернення громадян відбувається у відповідності до Інструкції з діловодства за зверненнями громадян в органах державної влади і місцевого самоврядування, об'єднаннях громадян, на підприємствах, в установах, організаціях незалежно від форм власності, у медіа (далі – Інструкція)[2]. Впровадження Інструкції було зумовлене комплексом правових, управлінських і суспільних чинників, пов'язаних із необхідністю забезпечення ефективної реалізації права громадян на звернення.

Передусім, ухвалення та запровадження Інструкції обумовлене конституційними засадами демократичної держави, яка гарантує громадянам право на звернення, право доступу до інформації тощо. Реалізація цього права від самого початку потребувала чітко врегульованого механізму діловодства, єдиного для всіх суб'єктів процесу звернень. Відповідна уніфікація мала захистити інтереси громадян, сформувавши єдині підходи та єдині вимоги до процедур та етапів документаційного забезпечення.

Крім того, реалізація норм Закону України «Про звернення громадян» у практичній площині – процедурні аспекти їх обліку, реєстрації, контролю виконання та зберігання звернень громадян як документів, – вимагала додаткового унормування та конкретизації, що покликані забезпечити підзаконні нормативні акти. Відповідне завдання і покладено на Інструкцію, яка конкретизувала ці процеси та забезпечила їх єдність.

Третім важливим чинником стала необхідність уніфікації діловодних процедур. До запровадження Інструкції практика роботи зі зверненнями громадян була фрагментарною й нерідко залежала від внутрішніх рішень конкретних установ. Це призводило до урізноманітнення, а фактично до хаотизації, у строках розгляду, формах відповіді, порядку контролю та архівного зберігання документів. Інструкція встановила єдині стандарти діловодства для всіх суб'єктів, незалежно від форми власності, а в останній редакції 2023 року, зокрема і для медіа.

Підвищення рівня відповідальності посадових осіб за роботу зі зверненнями громадян – це ще одна вагома причина появи Інструкції. Чітке регламентування процедур дозволило

мінімізувати прояви бюрократизму, формального підходу та безпідставного затягування розгляду звернень, а також створило правові підстави для контролю й притягнення винних осіб до відповідальності.

Крім того, впровадження Інструкції сприяло підвищенню прозорості та підзвітності діяльності органів влади й організацій. Наявність чітко визначеного порядку реєстрації та контролю за виконанням звернень забезпечує можливість відстеження руху документа на всіх етапах його розгляду, що є важливим елементом демократичного врядування.

Таким чином, Інструкція з діловодства за зверненнями громадян була впроваджена як необхідний інструмент реалізації конституційних прав громадян, удосконалення управлінської діяльності, уніфікації ділових процесів та зміцнення довіри суспільства до органів влади й інших суб'єктів публічної та приватної сфери.

Висновки. Документаційне забезпечення звернень громадян до органів публічного управління здійснюється у відповідності з нормами чинного законодавства, що є гарантією своєчасного, відповідального та конструктивного їх розгляду посадовими особами. Зафіксовані у нормах Конституції України гарантії права громадян на звернення, як засадничі принципи демократичної держави, забезпечують практичне втілення роботи із зверненнями та їх документаційне забезпечення у підзаконних нормативно-правових актах.

Список літератури

1. Дерев'янюк С. Електронні петиції до органів влади України як інструмент електронної демократії. Вісник Прикарпатського університету. Серія: Політологія. 2016. Вип. 10. С. 43–53
2. Смельянова А.Г. Аналіз динаміки розвитку електронної петиції як форми реалізації права на участь в управлінні місцевими справами на прикладі деяких обласних центрів та інших міст України. *Вісник Південно-регіонального центру Національної академії правових наук України*. 2018. № 14. С. 58–64.
3. Інструкції з діловодства за зверненнями громадян в органах державної влади і місцевого самоврядування, об'єднаннях громадян, на підприємствах, в установах, організаціях незалежно від форм власності, у медіа: Постанова Кабінету Міністрів України від 14 квітня 1997 року № 348; редакція від 24 червня 2023 року. URL: <https://ips.ligazakon.net/document/kp970348?an=35228>
4. Лациба М. В., Хмара О. С., Андрусів В. В. та ін. Методичні рекомендації щодо практичного впровадження Закону України «Про доступ до публічної інформації»: 2-е вид. доп. Київ : Агенство «Україна». 2012. 164 с.
5. Методичні рекомендації по роботі із зверненнями громадян: для керівників та інших посадових осіб органів державної влади, органів місцевого самоврядування, установ, підприємств, організацій, об'єднань громадян. Суми. 2019. 23 с.
6. Міняйло М. П. Соціально-правова сутність інституту права громадян на звернення. Форум права. 2011. № 1. С. 681–689.
7. Міняйло М. П., Кішак Ю. І. Адміністративно-правове забезпечення реалізації права громадян на звернення: монографія. Миколаїв: ТОВ «Фірма «Іліон». 2009. 192 с.
8. Петрова І.О. Організація роботи за зверненнями громадян в Україні у ХХ сторіччі. Гілея: науковий вісник. 2014. Вип. 80. С. 112–115
9. Про звернення громадян: Закон України від 2 жовтня 1996 р. № 393/96-ВР; редакція від 31.12.2023 р. URL: <https://zakon.rada.gov.ua/laws/show/393/96-%D0%B2%D1%80#top>
10. Соболь В. А. Актуальні проблеми забезпечення реалізації права громадян на звернення до органів влади. *Збірник наукових праць НАДУ*. 2013. Вип. 1. С. 159–169

УДК 621.753.5

Є. Сергієнко, магістр гр. ПМ-24М-3

О. Скібінський, канд. техн. наук, доцент

В. Селєхова, асистент

Центральноукраїнський національний технічний університет

ВДОСКОНАЛЕННЯ КОНСТРУКЦІЇ РІЗЬБОВОЇ ФРЕЗИ

В статті описано фрезерування різьби, як прогресивний метод різьбообробки. Розглянуто вплив сил різання на точність обробки різьбових поверхонь. Проаналізовано варіанти боротьби із негативним явищем відгинання інструменту під час обробки. Розраховано та спроектовано вдосконалену різьбову фрезу зі зворотною конусністю різальної частини інструменту.

фрезерування різьби, різьбова фреза, відгинання, жорсткість, зворотна конусність

Постановка проблеми. Якість і точність різьби визначають міцність і надійність з'єднання, тому вибір способу її нарізання є важливим аспектом. Існують різні методи обробки різьб, які відрізняються за способом виконання, використовуваними інструментами та вимогами до точності. Серед основних способів обробки різьбових поверхонь можна виділити точіння, нарізання мітчиками, фрезерування, шліфування, накатування та електроерозію.

Фрезерування різьби є сучасним і високопродуктивним методом, при якому матеріал знімається спеціальним різьбофрезерним інструментом для утворення різьбової поверхні. На відміну від традиційних методів, таких як нарізання мітчиками або плашками, фрезерування дозволяє обробляти різьбу різних профілів, діаметрів та з різним кроком, забезпечуючи високу точність, якість поверхні та стабільність розмірів навіть при обробці складних матеріалів.

Основним інструментом є різьбова фреза — інструмент спеціальної конструкції, що має профіль, який відповідає профілю різьби (метричної, дюймової, трубної тощо). Фрезерування різьби здійснюється на верстатах з числовим програмним управлінням (ЧПУ), здебільшого на горизонтальних або вертикальних обробних центрах. Верстат повинен мати можливість гвинтової інтерполяції по осях X, Y та Z із точністю позиціонування не менше $\pm 0,01$ мм, мінімальні вібрації шпинделя та високу жорсткість, а також достатню потужність шпинделя для забезпечення стабільних обертів при великих швидкостях подачі.

Процес фрезерування заснований на гвинтовому русі фрези, тобто на гвинтовій інтерполяції щодо деталі. Інструмент виконує кілька рухів: обертання навколо власної осі (різання), планетарний рух (інтерполяція по площині XY для формування діаметра), осьова подача (переміщення по осі Z, що відповідає кроку різьби за один повний оберт). Ці рухи координуються за допомогою системи ЧПУ, що дозволяє фрезі одночасно описувати спіральну траєкторію, утворюючи профіль різьби. Такий принцип обробки дає можливість виготовляти як з внутрішні, так і зовнішні різьби. На відміну від нарізання мітчиками або точіння різьби, фрезерування дозволяє обробляти різьбу в деталях складної форми, оскільки не потрібно обертати саму деталь під час обробки.

Вибір діаметра фрези залежить від діаметра різьби, матеріалу деталі та глибини обробки. Занадто малий діаметр фрези може знизити жорсткість інструмента та призвести до прогину, тоді як занадто великий діаметр може викликати зачеплення фрези з деталлю або перевантаження шпинделя.

Сили, що виникають під час обробки, безпосередньо впливають на перебіг процесу різання, причому визначальною є радіальна складова, оскільки саме вона спричиняє відгинання інструмента. Відгинання різбової фрези проявляється у відхиленні її осі від осі різбового отвору. Унаслідок цього зменшується зачеплення фрези з формованою різбою. Це призводить до неповного зняття матеріалу й, як результат, до появи конусності різби, що виражається у зменшенні висоти профілю зі збільшенням глибини обробки вздовж осі Z. Таким чином, актуальним є пошук конструктивних рішень щодо вдосконалення геометрії різбофрезерного інструменту з метою підвищення його жорсткості.

Аналіз останніх досліджень і публікацій. Конструктивна особливість фрези у вигляді негативного кута конусності позитивно впливає на експлуатаційні характеристики: подовжує термін служби різальної частини та мінімізує дефекти профілю різби, що в цілому підвищує продуктивність операції. Конструктивна реалізація зворотного конуса різбової фрези спрямована на нівелювання пружних відтиснень інструменту в процесі різання. В роботах [3, 5, 6] пропонуються такі значення конусності зворотного конуса: 0,05/100, 0,1/100-10/100 та 0,25/100-0,3/100 відповідно. В роботі [4] описано конструктивне рішення різбової фрези, особливістю якої є наявність ступінчастої зворотної конусності різальної частини. Конструкція передбачає поділ робочої зони на секції, при цьому величина зворотної конусності зовнішнього діаметра послідовно зростає у напрямку від торцевої поверхні до хвостовика та становить: 0,2-0,3/100, 0,4-0,5/100 та 0,6-0,7/100 відповідно. В роботі [4] дослідно доведено, що різбова фреза зі зворотним конусом дозволяє втричі підвищити точність формування профілю та забезпечує конусність різби в межах 0,01 мм.

Мета й завдання. Метою є розробка вдосконаленої конструкції різбової фрези з впровадженням зворотного конуса в її геометрію. Таке рішення дозволяє досягти наступних результатів: зниження сил різання завдяки поступовому входу зубців у метал та зменшенню кількості одночасних контактів із заготовкою на початковому етапі: підвищення точності завдяки компенсації пружного відгинання інструменту; усунення небажаної конусності готової різби; зменшення інтенсивності зношування різальних кромок різбової фрези.

Завданнями, що слугують досягненню поставленої мети є:

- вибір матеріалу та габаритних розмірів інструменту;
- розрахунок параметрів інструменту;
- проектування розрахованої різбової фрези.

Об'єктом дослідження є фрезерна обробка різбових поверхонь.

Предметом дослідження є проектування вдосконаленої конструкції різбової фрези з впровадженням зворотного конуса в її геометрію.

Виклад основного матеріалу. Об'єктом обробки є внутрішня різба M14×1,5-6H, що формується методом гвинтової інтерполяції на верстаті HAAS UMC 500. Для цього розроблено твердосплавну фрезу (матеріал — BK8). При визначенні габаритних розмірів фрези було знайдено компроміс між жорсткістю стержня та вільним простором в отворі для видалення стружки та безперешкодного руху за коловою траєкторією.

Аналітичне визначення профілю поверхні інструменту виконано за методикою [2].

Результати проведеного аналізу досліджень та публікацій дозволили встановити оптимальний діапазон конусності зворотного конуса різальної частини різбових фрез, що становить 0,01/100 – 1,2/100. При розрахунку параметрів вдосконаленого інструмента було прийнято значення 0,4/100 мм. Враховуючи довжину робочої частини фрези (8,75 мм), було визначено зміну зовнішнього діаметра ниток: від 8,417 мм для першої до 8,264 мм для шостої. Таким чином, загальна різниця діаметрів у межах робочої зони спроектованого інструмента становить 0,153 мм.

На рисунку 1 представлено креслення вдосконаленої різбової фрези зі зворотним конусом.

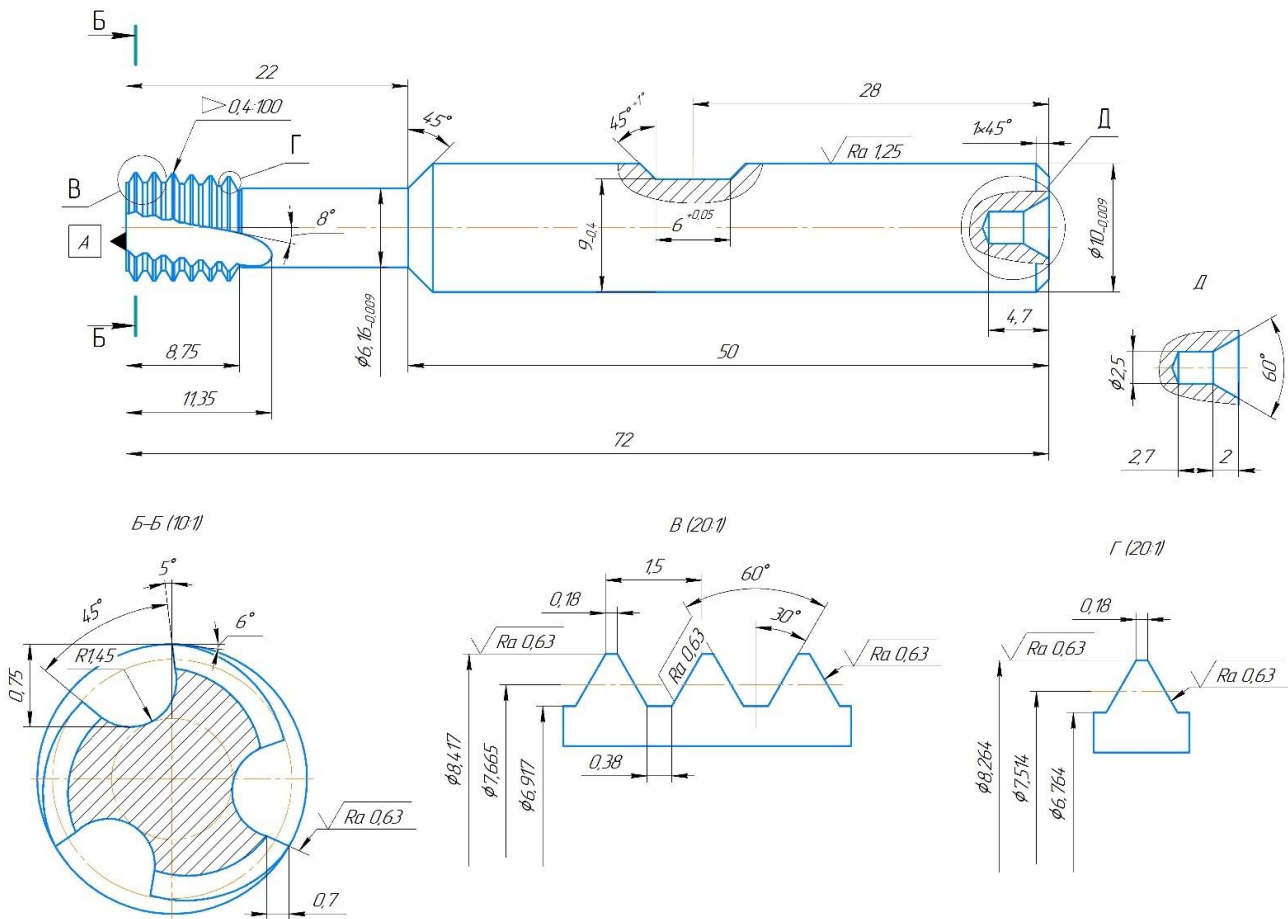


Рисунок 1 – Різьбова фреза зі зворотним конусом

Висновки. В статті описано фрезерування різьби, як прогресивний метод різьбообробки. Розглянуто вплив сил різання на точність обробки різьбових поверхонь. Проаналізовано варіанти боротьби із негативним явищем відгинання інструменту під час обробки. Розглянуто питання вдосконалення геометрії різьбофрезерного інструменту через застосування зворотного конуса. Проаналізовано варіації виконання робочої частини різального інструмента. Розраховано та спроектовано вдосконалену різьбову фрезу зі зворотною конусністю різальної частини.

Список літератури

1. Lee S.W. Analytic mechanistic cutting force model for thread milling operations / S.W. Lee, A. Kasten, A. Nestler // Procedia of the 14th CIRP Conference on Modeling of Machining Operations (CIRP CMMO, 2013). – June 13 - 14, 2013. Turin, Italy: Luca Settineri, 2014. – Vol. 8. – P. 546-551.
2. Stankov N. Analytical and Graphical Profiling of Thread-Milling Cutters for forming Internal Threads / N. Stankov, A. Ivanov // Applied Sciences. – 2025. – Vol. 15, iss. 13. – Art. 7308.
3. Пат. 2003/0231934 США, МПК B23G 5/18. Thread milling tool / Richard D. Kienzle; заявник Richard D. Kienzle. – № 10/174,138; заявл. 18.06.2002; опубл. 18.12.2003. – 7 р.
4. Пат. 203018865 Китай, МПК B23G 5/18. Thread processing milling cutter / Sun Zhenmei, Zhou Lei; заявник та патентовласник Chengdu Best Diamond Tools Co Ltd. – № 201220623253.3; заявл. 22.11.2012; опубл. 26.06.2013. – 7 р.
5. Пат. 108620694 Китай, МПК B23G 5/18. A kind of self-compensation screw cutter suitable for the finishing of small-diameter thread hole height / Dong Liangliang, Wang Jing, Zhu Xiaohua; заявник та патентовласник Chengdu Best Diamond Tools Co Ltd. – № 201810488663.2; заявл. 21.05.2018; опубл. 09.10.2018. – 8 р.
6. Пат. 112191956 Китай, МПК B23G 5/18. Thread milling cutter for high-temperature nickel-based alloy / Zhou Panke, Zhou Dongyang, Shuai Jiangnan, Xi Xudong; заявник та патентовласник Zigong Cemented Carbide Co Ltd. – № 202011082538.5; заявл. 12.10.2020; опубл. 08.01.2021. – 13 р.

УДК 004

Б. Андрусик, магістр гр. КІ-24М,

Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ СКРЕМБЛЮВАННЯ ЦИФРОВОГО СИГНАЛУ НА МОБІЛЬНИХ ПРИСТРОЯХ

У статті розроблено програмне забезпечення, яке призначено для системи скремблювання цифрового сигналу на мобільних пристроях. Метою розробки є дослідження та принципи побудови системи скремблювання цифрового сигналу на мобільних пристроях. Об'єктом дослідження є процес скремблювання цифрового сигналу на мобільних пристроях. Предметом дослідження є методи скремблювання цифрового сигналу на мобільних пристроях. Методи дослідження базуються на методах теорії сигналів та теорії захисту інформації в мережі, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи скремблювання цифрового сигналу на мобільних пристроях. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

скремблювання цифрового сигналу, мобільні пристрої

Постановка проблеми. Сучасному суспільству часом доводилося зіштовхуватися із проблемою прослуховування телефонних розмов. І цим нікого не здивуєш. В еру новітніх технологій ніколи не можна бути впевненим у повній конфіденційності чого-небудь. Зловмисники, намагаючись заволодіти анонімною інформацією, найчастіше підключаються до телефонних ліній як мобільних, так і стаціонарних телефонів, приносячись абонентам як стаціонарних, так і стільникових телефонів безліч проблем.

Скремблером називають пристрій, призначений для шифрування мови, що проходить через телефон, тим самим воно забезпечує захист і анонімність переговорів.

Шифрування відбувається за допомогою розбивки звукових сигналів на, так звані, під діапазони. Далі кожна частина піддається частотної інверсії, тобто перетворенню високих частот у низькі й навпаки. Поділ спектра на під діапазони відбувається на певній частоті, що називають крапкою розбивки. Крапка розбивки може бути фіксованою (під час розмови не виконується перемикання між режимами) або приймає одне з декількох можливих значень, коли під час телефонного переговору користувачі самі перемикаються між режимами скремблювання.

Процес розшифровки відбувається в тому випадку, якщо алгоритми скремблювання стоять на обох телефонах. Програми, працюючи одночасно, синхронно шифрують розмову. Таким чином, абоненти відмінно розуміють один одного, а зловмисники чують мову, що спотворюється повністю.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні скремблювання цифрового сигналу на мобільних пристроях.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи скремблювання цифрового сигналу на мобільних пристроях.

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

- Огляд існуючих систем скремблювання цифрового сигналу на мобільних пристроях.
- Дослідження системи скремблювання цифрового сигналу на мобільних пристроях.

– Програмна реалізація системи скремблювання цифрового сигналу на мобільних пристроях.

Об'єктом дослідження є процес скремблювання цифрового сигналу на мобільних пристроях.

Предметом дослідження є методи скремблювання цифрового сигналу на мобільних пристроях.

Методи дослідження базуються на методах теорії сигналів та теорії захисту інформації в мережі, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. У 2025 році ваш смартфон – це не просто засіб зв'язку, це портативне сховище, яке містить усе ваше цифрове існування. Від цінних спогадів та фінансових даних до конфіденційних робочих документів, ваш телефон – це центр вашого життя. Але наскільки безпечно це сховище?

В епоху постійно мінливих кіберзагроз та витончених фішингових шахрайств питання про те, як захистити свій телефон, ще ніколи не було таким критичним, особливо для новачків, які орієнтуються в цьому складному цифровому середовищі. Ви можете почуватися приголомшеними технічним жаргоном або не знати, з чого почати захист свого пристрою від сторонніх очей та зловмисників.

За межами екрана блокування: вичерпне визначення

Захист вашого телефону виходить за рамки простого блокування екрана. Він охоплює комплексний набір методів і технологій, розроблених для захисту вашого пристрою, даних, що зберігаються на ньому, та вашої особистої конфіденційності від несанкціонованого доступу, шкідливого програмного забезпечення та різних кіберзагроз.

По суті, захист телефону передбачає впровадження надійних заходів для захисту вашого цифрового життя, незалежно від того, чи використовуєте ви його для особистого спілкування, банківських операцій чи конфіденційних бізнес-операцій.

Такий багаторівневий підхід гарантує, що як апаратні, так і програмні компоненти вашого пристрою стійкі до потенційних вразливостей. Це забезпечує основу довіри у світі, що дедалі більше взаємопов'язаний. Зрештою, йдеться про створення цифрової фортеці навколо вашої найперсональнішої та найважливішої інформації, забезпечуючи її цілісність та конфіденційність.

Основні переваги та особливості мобільної безпеки

Переваги розуміння того, як захистити свій телефон, численні та критично важливі в сучасному цифровому середовищі. По-перше, це забезпечує першорядний захист від витоків даних та крадіжки особистих даних. Ваш телефон часто містить конфіденційну інформацію – контакти, фотографії, фінансові програми, електронні листи та особисті документи – які, якщо їх скомпрометувати, можуть призвести до серйозних особистих та фінансових наслідків.

По-друге, надійні заходи безпеки гарантують конфіденційність ваших повідомлень та особистих файлів. Це запобігає прослуховуванню або несанкціонованому доступу до ваших приватних розмов і документів. Це особливо важливо для фахівців, які працюють з конфіденційною інформацією, та для людей, які цінують свій особистий простір.

Чому це так важливо на сучасному ринку? Мобільні пристрої стали центральним центром нашого цифрового існування. Від керування розумними будинками до проведення фінансових транзакцій та доступу до робочих ресурсів, телефони постійно піддаються впливу кіберзагроз, що постійно змінюються. Добре захищений телефон пропонує душевний спокій, знаючи, що ваш цифровий слід захищений. Він також допомагає у дотриманні нормативних вимог для бізнесу, оскільки закони про захист даних дедалі більше вимагають безпечного поводження з особистою інформацією. Інвестування часу у вивчення того, як захистити свій телефон, більше не є необов'язковим; це фундаментальна необхідність для кожного, хто орієнтується в сучасному цифровому світі, захищаючись від постійних ризиків кіберзлочинності.

Галузеві стандарти мобільної безпеки

Перевірені стратегії безпеки телефонів узгоджуються з ширшими принципами кібербезпеки, підкреслюючи багаторівневий захист. Дотримання галузевих стандартів забезпечує надійну основу для захисту вашого пристрою:

- Надійна автентифікація: Завжди використовуйте складні паролі, відбитки пальців або розпізнавання обличчя. Уникайте легко вгадуваних шаблонів, простих PIN-кодів або паролів за замовчуванням.

- Регулярні оновлення програмного забезпечення: оновлюйте свою операційну систему (ОС) та всі програми. Ці оновлення часто містять критичні виправлення безпеки, які усувають нещодавно виявлені вразливості, захищаючи ваш пристрій від експлойтів.

- Керування дозволами програм: Будьте дуже вибірковими щодо дозволів, які ви надаєте програмам. Обмежте доступ до вашого місцезнаходження, камери, мікрофона та контактів, якщо це не є абсолютно необхідним для основної функції програми.

- Зашифрований зв'язок: для конфіденційних розмов та обміну даними використовуйте програми обміну повідомленнями з наскрізним шифруванням та безпечні служби електронної пошти.

- Безпечне використання Wi-Fi: Уникайте проведення конфіденційних транзакцій або доступу до особистих облікових записів у публічних мережах Wi-Fi без віртуальної приватної мережі (VPN). Публічні мережі часто не зашифровані та вразливі до прослуховування.

До поширених помилок, яких слід уникати, належать натискання на підозрілі посилання (спроби фішингу), повторне використання паролів у кількох онлайн-сервісах та нехтування регулярним резервним копіюванням даних вашого пристрою.

Рекомендації експертів щодо покращення безпеки телефону

Експерти з кібербезпеки постійно рекомендують конкретні, передові заходи для підвищення безпеки телефону та оптимізації вашого захисту:

- Розширений двоетапний вхід (2FA): Для всіх ваших облікових записів ми наполегливо рекомендуємо використовувати сучасні, безпечніші методи двоетапного входу (2FA), такі як Okta Verify, Google Authenticator або біометричні дані. Ці методи генерують коди, залежні від часу, або використовують унікальні фізичні атрибути, що значно знижує ризик несанкціонованого доступу, навіть якщо ваш пароль скомпрометовано.

- Поступова відмова від старих методів: Важливо зазначити, що традиційні методи 2FA, такі як SMS та голосові дзвінки, є застарілими методами та можуть бути недоступними в майбутньому через їхню схильність до атак заміни SIM-картки та інших вразливостей. Пріоритет багатофакторної автентифікації на основі додатків або біометричної багатофакторної автентифікації є ключовою порадою щодо оптимізації для кращої безпеки.

- Проактивне управління безпекою: Як наголошують експерти, «управління продуктами безпеки є важливим для забезпечення безпеки вашого веб-сайту від кіберзагроз», цей принцип поширюється безпосередньо на ваш мобільний пристрій. Проактивне та безперервне управління продуктами безпеки вашого телефону є життєво важливим. Це включає регулярний перегляд налаштувань безпеки вашого телефону, увімкнення функцій віддаленого стирання даних для втрачених або викрадених пристроїв та регулярне резервне копіювання даних у безпечне, зашифроване місце. Ці поради щодо оптимізації гарантують, що ваш телефон залишатиметься фортецею від постійно зростаючих кіберзагроз.

Професійні поради щодо безпеки мобільних пристроїв

Захист вашого телефону на розширеному рівні починається з фундаментальних професійних знань та надійних методів впровадження. Критичним аспектом є використання апаратного рівня безпеки, що включає безпечні процеси завантаження та апаратне шифрування. Це гарантує, що цілісність пристрою перевіряється з моменту запуску, а всі дані, що зберігаються на ньому, шифруються в стані спокою, що робить його недоступним без належної автентифікації.

Крім того, професійна безпека поширюється на всю екосистему зв'язку. Так само, як підприємства ретельно керують безпекою серверів, наприклад, вивчаючи «Як встановити SSL-сертифікати на серверах Zimbra» для забезпечення безпечної передачі даних, розширена безпека телефону вимагає наскрізного шифрування для всіх комунікацій – дзвінків, повідомлень та передачі даних. Це гарантує, що ваша особиста інформація залишається конфіденційною від вашого пристрою до одержувача і назад, захищаючи від прослуховування та перехоплення даних. Регулярні та своєчасні оновлення безпеки мають першочергове значення, виправляючи вразливості, перш ніж їх можна буде використати.

Розширені стратегії для забезпечення майбутнього вашого телефону

Виходячи за рамки базової безпеки, передові стратегії захисту вашого телефону передбачають проактивні заходи та врахування майбутніх факторів. Впровадження моделі безпеки з нульовою довірою для мобільних пристроїв є надзвичайно важливим; це означає, що жоден користувач чи пристрій не є довіреним за своєю суттю, незалежно від їхнього місцезнаходження, і кожен запит на доступ має бути автентифікований та авторизований. Такий підхід значно зменшує поверхню для атаки.

Ще один передовий метод передбачає розгортання складних механізмів виявлення загроз. Це включає виявлення аномалій на основі штучного інтелекту, яке може виявляти незвичайні моделі поведінки, що вказують на шкідливе програмне забезпечення або вторгнення, а також моніторинг шкідливих програм у режимі реального часу. Заглядаючи в майбутнє, майбутні міркування щодо безпеки телефонів все частіше включатимуть квантовостійку криптографію для захисту від потенційних можливостей розшифрування майбутніх квантових комп'ютерів, забезпечуючи довгострокову конфіденційність даних. Ці стратегії професійного рівня є важливими для підтримки найвищого рівня цифрового захисту від кіберзагроз, що розвиваються.

Оцінка ризиків та вразливостей безпеки мобільних пристроїв

Перш ніж запроваджувати конкретні заходи, важливо зрозуміти, як кібербезпека та мобільні пристрої впливають на діяльність компанії. Підприємства повинні виявляти потенційні загрози безпеці мобільних пристроїв та оцінювати поточні вразливості, щоб краще зрозуміти наслідки порушення безпеки та як відповідно реагувати у разі порушення.

Організації можуть розробляти індивідуальні стратегії безпеки, що відповідають унікальним викликам та потребам, шляхом проведення оцінки ризиків.

Зокрема, зростання занепокоєння щодо безпеки даних та шифрування пов'язане з кількома тенденціями:

- З розвитком програмного забезпечення для генеративного штучного інтелекту (ГШІ), зловмисники вже створили складніші форми кібератак.
- Оскільки все більше компаній переходять на віддалені та гібридні моделі роботи, злочинці націлюються на пристрої, що належать компанії, або особисті пристрої поза межами захищених корпоративних мереж.
- Зростаюча нестача фахівців з кібербезпеки також вплинула на здатність компаній захищати інформацію.

Основні стратегії безпеки мобільних пристроїв

Надійна стратегія мобільної безпеки повинна включати технічні засоби контролю, політики безпеки та програми підвищення обізнаності користувачів. Впровадження методів шифрування, забезпечення багатофакторної автентифікації та реалізація можливостей віддаленого стирання допомагають зменшити ризик втрати даних.

Найкращі рекомендації щодо безпеки мобільних пристроїв

1. Впроваджуйте політику нульової довіри

- Вимагати від користувачів встановлення унікальних надійних паролів.
- Відмовляйте співробітників від поширення паролів.
- Заохочуйте використання багатофакторної автентифікації або біометричних методів.

- Не радите натискати на посилання від незнайомих відправників та не завантажувати програмне забезпечення з незнайомих джерел.
- Уникайте обміну особистою інформацією з неперевіреними веб-сайтами або особами.

2. Шифруйте мобільні дані для запобігання витокам даних

- Шифруйте дані, що зберігаються на мобільних пристроях, зокрема шифруйте дані мобільних додатків, щоб захистити їх від несанкціонованого доступу у разі втрати або крадіжки.
- Використовуйте симетричні або асиметричні методи шифрування для підвищення безпеки.

3. Оновіть мобільну ОС та програми, щоб виправити вразливості безпеки

- Оновлюйте мобільні операційні системи та програми, щоб виправляти вразливості та запобігати атакам.
- Плануйте регулярні аудити, щоб забезпечити регулярні оновлення на всіх пристроях.

4. Посилення безпеки мобільних пристроїв за допомогою політик управління

- Впроваджуйте політики для забезпечення налаштувань безпеки, таких як захист паролем і шифрування.
- Забезпечити дотримання керівниками політики.

5. Захистіть мобільні з'єднання за допомогою безпечних віртуальних приватних мереж (VPN)

- Зменште ризики злому мобільних мереж, зобов'язавши використовувати VPN під час доступу до конфіденційної інформації або підключення до загальнодоступних мереж Wi-Fi. Загальнодоступні мережі Wi-Fi є небезпечними та часто стають мішенню злочинців.
- Мінімізуйте використання публічного Wi-Fi для віддаленої роботи.

6. Увімкніть функції віддаленого стирання та блокування для втрачених пристроїв

- Активуйте функції віддаленого стирання та блокування на пристроях, що належать компанії.
- Дозвольте ІТ-командам дистанційно видаляти дані та запобігати несанкціонованому доступу у разі крадіжки або втрати пристрою.

7. Моніторинг активності мобільних пристроїв для виявлення кіберзагроз

- Регулярно контролюйте та перевіряйте активність пристроїв, щоб виявляти підозрілу поведінку або несанкціонований доступ.
- Усувайте вразливості за допомогою проактивних заходів, таких як оцінка вразливостей та тестування на проникнення.

8. Контролюйте використання мобільних додатків для зменшення ризиків безпеки

- Контролюйте встановлення та використання програм.

9. Створіть резервні копії мобільних даних, щоб запобігти їх втраті через шкідливе програмне забезпечення або збій пристрою

- Заохочуйте регулярне резервне копіювання даних, щоб запобігти втраті у разі пошкодження або збою пристрою.
- Автоматизуйте резервне копіювання за допомогою хмарних платформ для безперебійного захисту даних.

10. Захист мобільних пристроїв за допомогою програмного забезпечення MDM/EMM

- Використовуйте програмне забезпечення для керування мобільними пристроями або корпоративного управління мобільністю для віддаленого керування пристроями та їх захисту.
- Отримуйте аналітику бізнес-операцій та забезпечуйте дотримання політик на всіх пристроях.

11. Навчіть співробітників передовим практикам безпеки мобільних пристроїв та кіберзагрозам

- Забезпечувати постійне навчання щодо найкращих практик безпеки мобільних пристроїв та важливості захисту даних.
- Запропонуйте довідковий контекст щодо нових правил та проілюструйте реальними прикладами кіберзлочинності.
- Заохочуйте участь співробітників та зміну їхньої поведінки за допомогою ефективних ініціатив у сфері лідерства та навчання.

Захист інтересів співробітників: як навчання знижує ризики мобільної безпеки

Окрім технічних заходів безпеки, організації повинні зосередитися на навчанні співробітників передовим практикам кібербезпеки.

Сприяючи розвитку культури обізнаності та відповідальності, компанії можуть надати співробітникам можливість відігравати активну роль у захисті своїх мобільних пристроїв і даних. Регулярні аудити можуть допомогти виявити проблеми відповідності та забезпечити дотримання заходів безпеки.

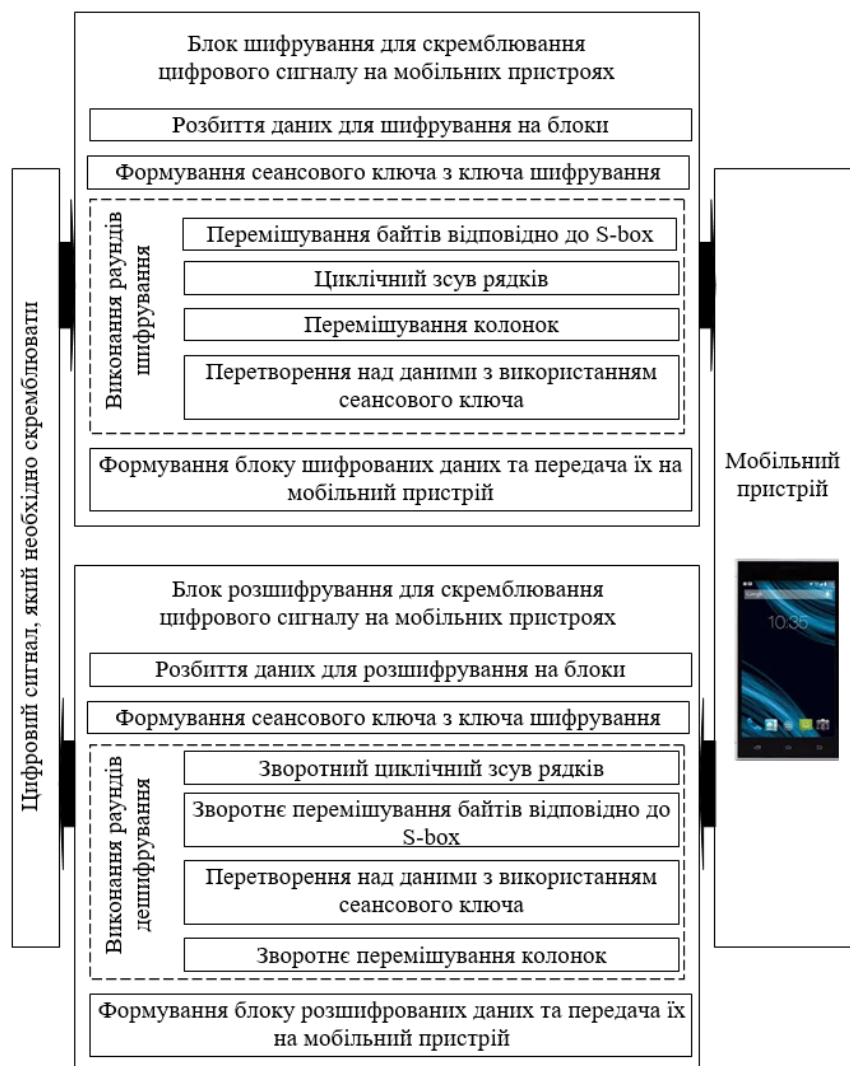


Рисунок 1 – Структурна схема системи

У даній роботі, для системи скремблювання цифрового сигналу на мобільних пристроях використовується алгоритм AES.

Структурна схема наведена на рисунку 1. З неї ми бачимо, що розроблена система складається з наступних структурних блоків.

- Дані, які передаються між мобільними пристроями.

- Блок шифрування за допомогою алгоритму AES для скремблювання цифрового сигналу на мобільних пристроях.
 - Блок розшифрування за допомогою алгоритму AES для скремблювання цифрового сигналу на мобільних пристроях.
 - Мобільний пристрій, на який надходять зашифровані сигнали.
- Основним блок системи є блок шифрування AES.

Випереджайте кіберзагрози за допомогою безпеки мобільних пристроїв

Зі зміною ландшафту загроз, актуальні заходи безпеки є надзвичайно важливими. Це включає регулярний перегляд та оновлення політик безпеки, інформування про нові загрози та відповідну адаптацію стратегій безпеки.

ІТ-менеджерам слід підписатися на розсилку новин про безпеку мобільних пристроїв та заохочувати всіх співробітників ділитися будь-якими відповідними новинами щодо пристроїв або програмних послуг, які вони використовують.

Проактивні заходи для безпеки мобільних пристроїв

Ефективна безпека мобільних пристроїв вимагає постійного моніторингу та швидкого реагування на інциденти безпеки. Аналіз після інциденту має вирішальне значення для навчання та вдосконалення в майбутньому.

Програмне забезпечення для управління корпоративною мобільністю надає важливі дані бізнес-аналітики для підтримки надійної стратегії безпеки пристроїв. Крім того, організаціям слід дотримуватися наведених вище найкращих практик безпеки мобільних пристроїв для захисту конфіденційних даних, зменшення ризиків та захисту від потенційних загроз.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів скремблювання цифрового сигналу на мобільних пристроях. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем скремблювання цифрового сигналу на мобільних пристроях.
- Досліджена система скремблювання цифрового сигналу на мобільних пристроях.
- На основі отриманих результатів досліджень створена програмна реалізація системи скремблювання цифрового сигналу на мобільних пристроях. Розроблені алгоритми дозволяють успішно вирішувати завдання скремблювання цифрового сигналу на мобільних пристроях. 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., Bebeshko, 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., 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., Prisyazhnyy, 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., Yenchov, 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., Chubaievskiy, V., Khorolska, K., Bebeshko, 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., Neskorodieva, T., Fedorov, E., Rudakov, K., Neskorodieva, 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.
 32. 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.

УДК 004

П.Арсієвич, магістр гр. КІ-24М,

Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ВІДЕОНАГЛЯДУ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ HD-SDI

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

відеонагляд, HD-SDI

Постановка проблеми. Новим напрямком у системах відеоспостереження й відеомоніторингу стало впровадження технології й стандарту HD-SDI, що добре відомо в HDTV – телебаченні високої чіткості. HD-SDI (на англ. High Definition Serial Digital Interface) – цифровий послідовний інтерфейс із можливістю передачі сигналу з високим дозволом. Даний стандарт підтримує дозволи – 720p, 1080i, 1080p. Ця технологія об'єднала в собі переваги аналогових і цифрових систем. Вона дозволяє, не використовуючи режим стиску (компресії) зображення, передавати високоякісне відео з дозволом 1920 X 1080p і зі швидкістю порядку 1,2 – 1,5 Гбіт/сек по звичайному коаксіальному кабелі типу RG6, RG11 або RG59. Довжина кабелю що дозволяє передавати зображення без втрат становить 120 – 150 метрів. Для передачі відеосигналу на більші відстані варто застосовувати оптоволоконний кабель, а при використанні коаксіала, через кожні 150 – 200 метрів необхідно ставити повторювачі. У цьому випадку довжину лінії можна продовжити до 1 км.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи відеонагляду з використанням технології HD-SDI.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи відеонагляду з використанням технології HD-SDI.

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

- Огляд існуючих систем відеонагляду з використанням технології HD-SDI.
- Дослідження системи відеонагляду з використанням технології HD-SDI.
- Програмна реалізація системи відеонагляду з використанням технології HD-SDI.

Об'єктом дослідження є процес відеонагляду з використанням технології HD-SDI.

Предметом дослідження є методи відеонагляду з використанням технології HD-SDI.

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

Виклад основного матеріалу. Монітори SDI (послідовний цифровий інтерфейс) створені для отримання нестиснених відеосигналів безпосередньо з камер або

відеореєстраторів із підтримкою SDI через коаксіальні кабелі. На відміну від IP-моніторів, вони не потребують налаштування мережі, забезпечують наднизьку затримку та є надзвичайно стабільними.

Основні переваги:

- Нестиснене відео для чіткішої деталізації та точного відтворення.
- Майже нульова затримка – необхідна для моніторингу в реальному часі.
- Налаштування "підключи та працюй" за допомогою роз'ємів BNC.
- Відсутність залежності від локальних мереж або Інтернету – забезпечує надійну роботу в середовищах з обмеженим доступом до мережі

Але не кожен SDI-монітор побудований однаково. Вибір правильного означає розуміння вашого середовища, інфраструктури та технічних вимог.

Ключовий висновок: Для більшості сучасних випадків спостереження ідеально підходять HD-SDI або 3G-SDI. Вони забезпечують чіткість високої чіткості та плавне відтворення в режимі реального часу без додаткової обробки.

Коли варто використовувати HD-SDI-монітор?

Якщо ви переходите з аналогового відеоспостереження або працюєте в критично важливому середовищі, монітори HD-SDI пропонують кілька експлуатаційних переваг.

Використовуйте монітор HD-SDI, коли:

- У вас є існуюча коаксіальна інфраструктура. SDI-монітори можна підключати безпосередньо до застарілих кабелів (RG59/RG6), що дозволяє уникнути необхідності дорогої перепрокладки.

- Вам потрібна видимість відео в режимі реального часу. HD-SDI ідеально підходить для постів охорони, диспетчерських та виявлення загроз у реальному часі, пропонує кадрово-точне відтворення без затримки.

- Налаштування мережі не є життєздатним або безпечним. У лікарнях, урядових будівлях або захищених зонах SDI повністю обходить мережу, зменшуючи ризики та необхідність конфігурації IT.

Найкращі програми для HD-SDI-моніторів:

- Віддалені або тимчасові сайти без IP-інфраструктури.
- Банки та урядові будівлі зі суворою сегментацією мережі.
- Лікарні та входи до відділень екстреної допомоги, яким потрібна візуалізація в режимі реального часу.

Які характеристики важливі при порівнянні SDI-моніторів?

Щоб зробити правильний вибір, не обмежуйтеся лише характеристиками роздільної здатності. Ось контрольний список того, що слід оцінити, – кожен фактор пояснюється практичними порадами:

1. Підтримувані формати (HD-SDI, 3G-SDI). Оберіть монітор, який підтримує як HD-SDI, так і 3G-SDI. Це гарантує сумісність з новішими камерами, що забезпечують 60 кадрів/с, і дозволяє проводити майбутні оновлення без заміни всієї системи відображення.

2. Вихід відео (BNC-вихід). Монітори з наскрізним SDI-з'єднанням дозволяють підключити одне відеоджерело до кількох дисплеїв або до системи запису. Це надзвичайно важливо для систем з кількома станціями перегляду або для поєднання локального моніторингу з віддаленим архівуванням.

3. Захист від вигорання. Під час відеоспостереження статичні зображення (наприклад, зображення з коридору) можуть залишатися на екрані годинами. Шукайте монітори із вбудованою функцією Anti-Burn-in™ або захистом від залишкового зображення, щоб запобігти появі ореолів та продовжити термін служби екрана.

4. Довговічність життя. Ваш монітор, ймовірно, працюватиме цілодобово в громадському або промисловому середовищі. Надайте перевагу моделям з:

- Металевий корпус для стійкості до ударів.

- Оптичні скляні екрани для захисту від подряпин.
- Посилення внутрішніх компонентів від пилу та вібрації.

Вони забезпечують надійну роботу протягом тривалого часу, навіть у складних умовах.

5. Гнучкість встановлення. Кімнати керування та кіоски відеоспостереження відрізняються за плануванням. Виберіть монітор із:

- Різноманітні варіанти входу (HDMI, SDI, VGA за потреби).
- Сумісність кріплень VESA.
- Широку кути огляду.

Це дозволяє вам налаштовувати установки без додаткових кронштейнів або перетворювачів.

Де монітори HD-SDI мають стратегічне значення

Зони спостереження високого ризику

У правоохоронних органах, ювелірних магазинах або казино можливість моніторингу подій у режимі реального часу – без затримки чи буферизації – є критично важливою. Монітори SDI пропонують безпечний перегляд без затримок.

Розширений судово-медичний огляд

Якщо ваша команда використовує записи з камер спостереження для аналізу після події, ключовим є збільшення масштабу без спотворень або артефактів стиснення. Монітори SDI забезпечують природну чіткість зображення для деталей та точності масштабування.

Встановлення на великі відстані

З коаксіальним кабелем RG6 відстані передачі SDI можуть перевищувати 100–300 метрів. Додайте оптоволоконні перетворювачі, і дальність ще більше збільшиться – без шкоди для цілісності сигналу.

Перегляд на кількох моніторах

Використовуючи монітор із наскрізним SDI-виходом, зображення з однієї камери може одночасно відображатися на кількох моніторах або записуючих пристроях. Це важливо для постів охорони або багаторівневих зон спостереження.

Типові помилки, яких слід уникати під час вибору SDI-монітора

Навіть досвідчені монтажники можуть не помітити критичні фактори. Ось деякі поширені помилки та способи їх уникнути:

– Якщо припустити, що всі SDI-монітори підтримують 3G-SDI: Не кожна модель це робить. Завжди перевіряйте вхідні характеристики, особливо якщо використовуються камери з високою частотою кадрів.

– Ігнорування ризику вигорання: відеоспостереження передбачає надмірне використання статичної електрики. Без захисту від вигорання залишкове зображення може з часом пошкодити дисплей.

– Нехтування міцністю корпусу: монітори споживчого класу можуть бути дешевшими, але вони не витримують цілодобового перебування в запиленіх, промислових або інтенсивних середовищах.

– Невідповідність роз'ємів або кабелів: SDI вимагає 75-омного BNC-кабелю. Використання неправильної специфікації (наприклад, RG58) може призвести до втрати сигналу або нестабільності.

Вибір правильного SDI-монітора – це не лише питання технічних характеристик, а й забезпечення продуктивності вашої системи спостереження, коли це найбільше потрібно.

Підсумовуючи, зверніть увагу на:

- Гнучкість формату (HD-SDI, 3G-SDI).
- Можливість виходу з ланцюжка.
- Відео в реальному часі без затримки.
- Цілодобова довговічність.

- Захист від вигорання.
- Сумісність з вашою кабельною системою та плануванням об'єкта.

Завдяки правильному SDI-монітору ваша система спостереження може забезпечити високу чіткість зображення з низькою затримкою, що дозволяє швидше приймати рішення та отримувати кращі результати.

HD-SDI

Донедавна дозвіл Full HD (1920x1080) було нерозривно зв'язаний тільки з IP-системами. На сьогоднішній день технології дають можливість передавати по аналоговому кабелю незжаті зображення найвищої якості. При цьому ціна HD-SDI камер істотно нижче IP-аналогів.

На відміну від аналогових відеокамер, HD SDI відеокамери дозволяють охоплювати набагато більшу територію. Завдяки цьому стає можливим охопити ту ж територію меншою кількістю камер.

HD SDI відеореєстратори дають можливість одержувати більше деталізовану картинку, що дозволяє без проблем розглянути номер автомобіля або особу людини на відстані більш ніж 200 метрів.

Сучасні технології дозволяють модернізувати звичну аналогову систему й на її основі впровадити нову, набагато могутнішу HD-SDI. Найпривабливішим моментом є можливість використовувати стару систему комутації на базі коаксіальних кабелів. Таким чином, необхідна лише модернізація, щоб одержати повністю нову систему відеоспостереження, без складностей в експлуатації й яка забезпечує високу якість зображення.

Монтаж і подальша робота з HD-SDI системами не вимагають перенавчання. Конструктивна схожість дозволять будь-якому технікові, що хоч раз установлював аналогові камери без проблем упоратися й з новим форматом.

Одна з головних переваг HD-SDI – мінімальна втрата дані картини, відсутність затримки при перегляді. На таких об'єктах як аеропорти, вокзали, банки це є однією з основних умов при виборі системи відеоспостереження.

Дальність передачі відеосигналу безпосередньо пов'язана з якістю використовуваних коаксіальних проводів. Як показує досвід, передача HD картини може вестися на 100 м-150м без додаткових пристроїв.

Типи й характеристики HD-SDI камер

Сучасні HD-SDI камери мають максимальний дозвіл 1920x1080, тобто є 2,1 Мп камерами й підтримують передачу по аналоговому кабелі незжатого й не пакетизованого зображення Full HD (1080P). Існують і бюджетні моделі з максимальним дозволом 720p.

Стандартна чутливість 0, 1-0,01 люкса, а так само існують моделі з можливістю працювати аж до 0,000006 люкса із застосуванням ІЧ-фільтра, ІЧ-підсвітлення й сучасних чипів обробки відеосигналу. Модельні лінійки й конструктивне виконання схоже на аналогові лінійки. Отут є й вуличні з ІЧ і без ІЧ-підсвічування, у металевих антивандальних куполах, боксові камери під об'єктив (використовуються такі ж мегапіксельні як і на IP-камерах), внутрішньої й зовнішньої поворотні PTZ-камери, камери з убудованими трансфокаторами з автофокусом.

Відеореєстратори HD-SDI

Тип і зовнішній вигляд реєстраторів HD-SDI багато в чому повторює аналогові DVR. Деякі виробники випускають HD моделі в тих же корпусах, що й стандартні. Функціонал, меню, налаштування – практично ідентичні. Простіше перелічити основні відмінності:

1. Дозвіл запису – аж до 1080p. Залежно від займаної цінової ніші в даному дозволі можлива швидкість запису 5, 15 або 30 к/с на кожний канал. Можливий одночасний запис у різних дозволах.

2. Оперативний перегляд каналів здійснюється в реальному часі з будь-яким дозволом. Для перегляду рекомендується широкоформатний монітор не менш 24" з дозволом FullHD. Сигнал на монітор подається по HDMI кабелі (стандартне оснащення для HD-SDI реєстраторів).

3. Віщання в мережу відеопотоку аж до 1280*720. У багатьох виробників ПЗ сумісно як з аналоговим устаткуванням, так і з HD устаткуванням, що дозволяє створювати гібридні системи або переходити на новий рівень відеобезпеки поступово. Також можна відзначити наявність гібридних моделей, що дозволяють працювати одночасно як із цифровим, так і з аналоговим відеопотоком. Системи відеоаналітики й роботи з архівами повторюють аналогові моделі.

IP і HD-SDI

У порівнянні з IP-системами в технології HD-SDI є як плюси, так і мінуси.

Монтаж системи повністю нагадує створення аналогової системи відеоспостереження. Камера-кабель-реєстратор із з'єднанням розніманнями BNC. При наявності готової системи на базі аналога із установленим якісним кабелем модернізація системи складається тільки в заміні кінцевого встаткування й не вимагає витрат на побудову нової інфраструктури на базі IP. Не потрібне навчання персоналу для монтажу нового обладнання.

Вартість устаткування порівнянна з устаткуванням IP з відповідним дозволом, але при цьому можна заощадити на створенні інфраструктури (не потрібні комутатори, дорогі сервери й комп'ютери для оперативного спостереження), не використовується дороге ПЗ для IP-спостереження. Кожна камера HD-SDI підключена по власному кабелі (каналу), що повністю забирає можливість зниження якості сигналу або швидкості кадрів, які можуть виникнути у зв'язку з навантаженням на комп'ютерну мережу, до якої підключена IP-камера.

HD-SDI відеоспостереження є цифровим інтерфейсом послідовного типу, що забезпечує високий дозвіл зображення. Дана система являє собою стандарт устаткування цифрового формату для запису й реєстрації зображень у високому дозволі 1920x1080 пікс. або 1280x720 пікс. Передача даних від камер до пристрою, що реєструє, здійснюється в цифровому форматі через звичайний кабель RG-6. HD-SDI дає можливість експлуатації, як як автономна система, так і в складі складних систем безпеки й відеоспостереження. Одна з особливостей всіх камер HD-SDI полягає в тому, що вони мають додатковий аналоговий вихід.

Структурна схема системи зображена на рисунку 1.



Рисунок 1 – Структурна схема системи

Саме новий стандарт відео HDcctv сполучить у собі надійність і безвідмовність аналогових систем і високоякісного цифрового відео. HDcctv базується на технології, розробленої для використання у високоякісних віщальних ТБ-системах і на відміну від аналогових технологій відеокамери HD-SDI дозволяють охоплювати в 3-4 рази більше контрольованої площі. Використання коаксіальних кабелів і рознімань BNC, однакова ідеологія побудови систем і аналогічний користувальницький інтерфейс в DVR – все це

робить HDcctv досить перспективним напрямком в області безпеки. Ще раз відзначимо, що мова йде про закриті проекти з максимальною захищеністю, найбільшою надійністю й найкращим зображенням, простими в налаштуванні й експлуатації, інтегровальними з іншими компонентами системи безпеки.

Переваги

Що ми маємо у випадку застосування систем безпеки стандарту HDcctv:

1. Камери мегапіксельного дозволу – дозволяють мати відео з високим рівнем деталізації.
2. HD-SDI-камери – більше високий рівень захищеності від знімання й підміни відеосигналу в порівнянні з аналоговими й IP-камерами.
3. Максимальний рівень захисту відеоданих – відео архівується (записується) у власному кодованому форматі, недоступному звичайним медіаплеєрам.
4. Широке й гнучке використання технічних можливостей апаратних DVR – тривожні входи й виходи, інтелектуальні детектори руху й пошук в архіві по обраних зонах.
5. Апаратну обробку й запис відео – свідомо саму надійну з існуючих.
6. Можливість використання комбінованих рішень – аналог + HD-SDI. Гібридні системи дозволяють замінити частину найбільш важливих камер, а другорядні – залишити без зміни або поліпшити в рамках стандарту (700 ТВЛ).
7. Можливість застосування програмних рішень, що поєднують всі блокову й віддалені DVR у єдину мережу моніторингу й адміністрування, – при розширенні системи (особливо важливо для розгалуженої мережі філій).
8. Застосування клієнтського універсального ПЗ – дозволяє додати до внутрібанківських систем банкоматну й автотранспортну мережу, включаючи живе відео й доступ до локальних архівів.
9. Використання клієнтського універсального ПЗ – дозволяє настроїти дублювання (дзеркалювання) відеоданих і журналу подій на віддалені мережні сховища (внутрібанківська закрита мережа).

Дозвіл

Повний розмір кадру становить 1920x1088 пікс. – це дозволяє одержати набагато більше зображення з високою деталізацією в порівнянні з дозволом D1 (720x576). Зовсім очевидно, що для досягнення високодеталізованого зображення в D1 необхідно винятково оптичне збільшення, тобто звуження кута огляду шляхом збільшення фокусної відстані об'єктива. А для мегапіксельної камери така деталізація досяжна на кутах об'єктива майже втричі більше. Вивід – мегапіксельні відеокамери HD і FullHD дозволяють бачити деталізоване зображення на широкому куті захвата сцени.

Саме широкий кут огляду дозволяє контролювати максимальну площу сцени, а у випадку довгофокусного наведення мегапіксельної камери – розглядати дрібні деталі й елементи зображення, наприклад вид, колір і достоїнство грошових знаків, чіткі особи відвідувачів, особливості одягу, кольору волосся і т.д. Як показує кримінальна статистика, саме такі "дріб'язки" є головною ланкою й надійною ідентифікацією в більшості розслідувань.

Захищеність

Одним із самих головних вимог до систем безпеки в банках є захищеність і конфіденційність даних. У цей час найпоширеніший спосіб розмежування (захисту) доступу – однофакторна автентифікація. Найчастіше це парольний захист. Двофакторна автентифікація з використанням додаткового бар'єра, наприклад USB-ключа або Smart-карти з PIN-кодом, набагато надійніше.

У системах відеоспостереження, побудованих на IP-технологіях (IP-камери, комутатори, серверне встаткування), застосовуються новітні методи 128-бітного шифрування самого мережного трафіку з використанням протоколу IPv6 (IPSec). Але проте захист доступу до контенту через безпосередній вхід на сервер або клієнтську програму за рідкісним винятком залишається однофакторним. Рівно так само, як здійснюється доступ до

адміністрування й архіву в аналоговій та HDcctv-системах. Тому говорити про перевагу IP-системи в плані захищеності в порівнянні з іншими не доводиться. І якщо пряме перехоплення й підміна відеопотоку в аналогових системах – справа технічно не дуже складне (прикладів тому багато, включаючи голлівудські посібники для зломщиків), то підмінити або навіть продублювати для несанкціонованого запису відеопотік із цифровим сигналом HD-SDI набагато складніше.

Зрозуміло, для віддаленого й розподіленого адміністрування будь-яких систем не обійтися без мережних технологій – закриті або відкриті локальні мережі на сьогодні найшвидший і максимально функціональний спосіб одержати доступ до необхідних даних – будь тої бази даних різного роду, платіжні операції, документообіг або відео/аудіоархів. Напевно, не потрібно зайвий раз говорити про те, що різнонаправлені за призначенням локальні мережі обов'язково повинні бути фізично незалежними. Така побудова продиктована в першу чергу вимогами до безпеки, а також міркуваннями технічного плану. Трафік з відеоданими в тисячі й сотні тисяч разів перевищує максимальні мережні навантаження будь-якої установи, отже, і умови (середовище) обслуговування таких різних завантажень повинна бути різним.

Очевидно, що стосовно до стаціонарних HDcctv-відеореєстраторам мережний захист стане актуальною у випадку створення власної локальної мережі, яка організується винятково для швидкого віддаленого моніторингу, адміністрування або резервного копіювання відеоданих. Проектуючи подібні структури, замовникові (властиво, службі безпеки установи) необхідно мати чітке подання про те, які конкретні завдання покликане вирішувати створювана ЛОМ, можливості мережних сервісів і програмних додатків. Захист мережі вирішується також, як і у випадку з IP-системами – шифруванням IPv6. У цьому випадку будуть потрібні комутатори з підтримкою цього типу шифрування з відповідним включенням даного протоколу на всіх дозволених віддалених клієнтах (ПК).

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів відеонагляду з використанням технології HD-SDI. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем відеонагляду з використанням технології HD-SDI.
- Досліджена система відеонагляду з використанням технології HD-SDI.
- На основі отриманих результатів досліджень створена програмна реалізація системи відеонагляду з використанням технології HD-SDI. Розроблені алгоритми дозволяють успішно вирішувати завдання відеонагляду з використанням технології HD-SDI.

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

С.Батрак, магістр гр. КІ-24М,

Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ПРОАКТИВНОГО МОНІТОРИНГУ МЕРЕЖЕВОГО ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

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

проактивний моніторинг, мережевий електронний документообіг

Постановка проблеми. Багато глобальних організацій узгодили свою стратегію та діяльність за допомогою структури інтегрованої системи управління (ІСУ) на основі ISO, яка дозволяє їм об'єднувати системи управління якістю, навколишнім середовищем, охороною здоров'я та безпекою. У такому контексті наявність надійної системи електронного управління документами (СЕД) є важливою, особливо на глобальних підприємствах, де велика кількість документів, що генеруються процесами, проходить через різні робочі культури. Однак, не існує універсального рішення для СЕД, оскільки воно залежить від потреб, розміру та розподілу ресурсів організацій.

У цій роботі розглядається взаємозв'язок між СЕД та ІСУ, щоб запропонувати найкращу практику. Дана робота методологічно базується на якісному, інтерпретативному, позовжньому емпіричному дослідженні на заводі вітрових турбін.

Удосконалення та ефективність ІСУ ігнорують СЕД як ключовий фактор у встановленні належної технологічної підтримки процесів ІСУ. Правильне застосування СЕД може додатково сприяти організаційному навчанню, точності документації та міжорганізаційній співпраці.

Теоретизація щодо ІСУ потребує глибшого розуміння технологічних обмежень та потенціалу базування ІСУ на СЕД.

ІСУ – це складні системи, що включають велику кількість адміністративних функцій. СЕД забезпечує формальне представлення з потенціалом автоматизації, що підвищує та забезпечує достовірність документів. ІСУ, як правило, залишається у професіоналів, наприклад, лінійних менеджерів та фахівців з контролю якості/якості/якісного менеджменту (QA/QMS). Напрямок обговорення СЕД передбачає ширше охоплення. Дослідження ІСУ як технологічної реалізації забезпечує кращу платформу для узгодження ІСУ з іншими бізнес-процесами та наближає ІСУ до операційної діяльності в межах підприємства.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи проактивного моніторингу мережевого електронного документообігу.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи проактивного моніторингу мережевого електронного документообігу.

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

- Огляд існуючих систем проактивного моніторингу мережевого електронного документообігу.
- Дослідження системи проактивного моніторингу мережевого електронного документообігу.
- Програмна реалізація системи проактивного моніторингу мережевого електронного документообігу.

Об'єктом дослідження є процес проактивного моніторингу мережевого електронного документообігу.

Предметом дослідження є методи проактивного моніторингу мережевого електронного документообігу.

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

Виклад основного матеріалу. Сьогодні нам кажуть, що простого моніторингу недостатньо. Щоб досягти справжньої оптимізації продуктивності та надійності, потрібно проводити моніторинг проактивно. Тому багато компаній звертаються до проактивного моніторингу.

На перший погляд, це цілком очевидно. Не потрібно бути досвідченим інженером з надійності сайтів (SRE), щоб знати, що краще застосовувати проактивний підхід до моніторингу, ніж чекати, поки щось піде не так, перш ніж виправляти це.

Але справжнє питання полягає в тому, як насправді здійснювати проактивний моніторинг. Легко говорити про важливість проактивного моніторингу, але важче підійти до нього на практиці.

Що таке проактивний моніторинг?

Проактивний моніторинг – це стратегія моніторингу, за якої команди прагнуть виявляти та вирішувати проблеми до того, як вони перетворюються на критичні збої.

Він відрізняється від звичайного реактивного моніторингу тим, що замість того, щоб чекати, поки щось піде не так, перш ніж вживати заходів для її вирішення, проактивний моніторинг зосереджується на використанні інформації з моніторингу для прогнозування проблем, що виникають, та придушення їх у зародку, перш ніж вони перетворяться на реальні проблеми.

Іншими словами, замість того, щоб чекати, поки сервер вийде з ладу або програма буде перевантажена трафіком, перш ніж вживати заходів щодо виправлення ситуації, проактивний моніторинг передбачає вжиття превентивних заходів для запобігання збоєм сервера або запуску іншого екземпляра програми, щоб уникнути збою.

Проактивний моніторинг – це автоматизований процес у режимі реального часу, який безперервно відстежує продуктивність системи, мережеву інфраструктуру та ключові показники для виявлення та запобігання потенційним проблемам, перш ніж вони спричинять простой або збої. Використовуючи прогнозу діагностику та виявлення аномалій, проактивний моніторинг виявляє проблеми на ранній стадії, сповіщає команди про необхідність негайного вжиття заходів та забезпечує ефективну та надійну роботу системи.

Такий підхід допомагає запобігти збоєм серверів, оптимізувати продуктивність та захистити інфраструктуру, забезпечуючи масштабовані, інтегровані рішення для підприємств будь-якого розміру. Завдяки проактивному моніторингу проблеми вирішуються до їх загострення, мінімізуючи перебої та підтримуючи безперебійну роботу.

Знову ж таки, переваги проактивного моніторингу мають бути досить очевидними. Коли ви запобігаєте проблемам проактивно, ваші користувачі стикаються з меншою кількістю збоїв. Ви забезпечуєте набагато кращий клієнтський досвід – і, в свою чергу, збільшуєте бізнес-цінність – коли повністю уникаєте серйозних збоїв.

За допомогою реактивного моніторингу найкраще, на що ви можете сподіватися, це швидке вирішення проблем із збоями після того, як вони вже сталися. Це не ідеально з точки зору клієнтського досвіду чи бізнесу.

Проактивний проти реактивного моніторингу

Проактивний моніторинг передбачає використання загальносистемних процедур моніторингу для виявлення та вирішення основних проблем, *перш ніж* вони призведуть до збоїв. Реактивний моніторинг здійснюється лише *у відповідь на* проблему, яка вже виникла. Процедури реактивного моніторингу, по суті, слугують розслідуванням першопричини проблеми, тоді як проактивний моніторинг служить запобіжним заходом.

Хоча проактивний моніторинг часто передбачає «реагування» адміністраторів на невідповідності в продуктивності, ці дії все ще вважаються превентивними, оскільки кінцевий користувач ще не постраждав.

Чому проактивний моніторинг кращий за синтетичний моніторинг

Синтетичний моніторинг включає моделювання поведінки кінцевого користувача для тестування функціональності та виявлення проблем продуктивності та несправностей. Результати цих тестів використовуються для виявлення та усунення будь-яких збоїв, виявлених на шляхах користувача.

За своєю природою, синтетичний моніторинг можна вважати розширенням реактивного моніторингу, оскільки він спирається на вивчення досвіду кінцевого користувача і тому не може виявляти та діагностувати проблеми проактивно. Крім того, синтетичний моніторинг розглядає дані лише епізодично та не може протестувати весь набір можливих шляхів користувачів, що часто призводить до пропущених збоїв та проблем. Проактивний моніторинг, за визначенням, використовує цілісний підхід до ІТ-моніторингу та випереджає проблеми, шукаючи ранні індикатори.

Приклади проактивного моніторингу + ранні індикатори

Проблеми неможливо діагностувати, оцінюючи окремі ІТ-метрики. Однак, коли збираються історичні дані та встановлюється базовий рівень продуктивності, тенденції цих показників слугують ранніми індикаторами справжньої проблеми. Деякі приклади проактивного моніторингу ранніх індикаторів включають:

Приклад 1: Значна втрата пакетів

Пакет вважається «втраченим», коли він не досягає місця призначення після передачі. Системи покладаються на передачу пакетів для всієї інтернет-діяльності. У разі значної втрати пакетів кінцевий користувач може зіткнутися з повним перебоєм у роботі сервісу або повільним мережевим з'єднанням. Відсоток втрати пакетів необхідно контролювати, щоб переконатися, що на сервіс не впливають збої мережевого обладнання, несправності програмного забезпечення або порушення безпеки.

Приклад 2: Аномалії часу відгуку та тенденції до зниження

Забезпечення стабільної продуктивності передбачає встановлення базового рівня часу відгуку та визначення точок даних, які відрізняються від нього щонайменше на 100% або більше. Відхилення такого значного ступеня вимагає розслідування потенційних основних причин. Звідси мережеві адміністратори можуть дослідити розбіжність та вирішити будь-які проблеми, що перешкоджають продуктивності. Аномалія не завжди є показником серйознішої проблеми, проте закономірність низького або погіршеного часу відгуку, виявлена за допомогою проактивного моніторингу мережі, майже завжди є такою.

Приклад 3: Фактори навколишнього середовища

Визначення проактивного моніторингу виходить за рамки базових ІТ-метрик, таких як втрата пакетів та час відгуку. Навіть фактори навколишнього середовища, такі як температура в комп'ютерній кімнаті, підпадають під поняття проактивного моніторингу. Якщо ваша комп'ютерна кімната або центр обробки даних перегріється, ваше обладнання може зазнати величезних пошкоджень та можливого виходу з ладу. Такої події можна уникнути, просто встановивши датчики навколишнього середовища у вашому комп'ютері, які сповіщають вас про порушення певних температурних порогів.

Приклад 4: Проблеми з конфігурацією

Щось таке просте, як проблема з конфігурацією, може призвести до серйозного збою. Наприклад, інтерфейсне з'єднання на вашому маршрутизаторі відповідає за обробку інтернет-трафіку. Якщо це з'єднання перестає реагувати, це призводить до збоїв у роботі таких служб, як перегляд веб-сторінок та зовнішній трафік. Інші поширені помилки конфігурації включають незбереження конфігурації, випадкову зміну конфігурації пристрою або просто неправильне введення команд. Точні та функціональні конфігурації мають вирішальне значення для щоденної роботи вашої компанії, і успішні організації повинні мати можливість проводити проактивний моніторинг програм, щоб виявляти проблеми, пов'язані з неправильними конфігураціями, перш ніж вони вплинуть на кінцевого користувача.

Найкращі практики для проактивного ІТ-моніторингу**Створіть карту своїх ІТ-активів**

Щоб контролювати свої пристрої, вам спочатку потрібно знати, де вони знаходяться відносно свого оточення. Збір цієї інформації та її відображення на проактивній карті моніторингу мережі не лише допоможе вам візуалізувати структуру вашої мережі, але й точно визначити, де виникають проблеми. Наявність процедур автоматичного виявлення та зіставлення пристроїв допоможе вам підтримувати актуальну картину вашого середовища.

Встановлення базових показників

Встановлення базових показників продуктивності на основі історичних даних пристроїв є основою для будь-якого проактивного моніторингу. Без базового рівня немає точки відліку для позначення точок даних як аномалій, запуску функцій сповіщень та сповіщень або спостереження за тенденціями. Базові показники слід визначати шляхом поєднання аналізу історичних даних та цільових показників, встановлених найкращими практиками.

Увімкнути сповіщення та сповіщення

Ваше програмне забезпечення для моніторингу повинно мати можливість проактивно попереджати ІТ-менеджерів, коли ресурс знаходиться на межі досягнення критичного порогу. Такі показники, як високий трафік на мережевому комутаторі або зменшення ресурсів на сервері, що підтримує критично важливі для бізнесу програми, необхідно враховувати якомога швидше. Менеджери повинні мати можливість налаштувати проактивні сповіщення, коли пристрій перебуває в стані тривоги, щоб вони могли усунути проблему, перш ніж це вплине на кінцевого користувача.

Майте інтелектуальний план потужностей

Наявність інтелектуального плану управління потужностями необхідна для забезпечення безперебійного взаємодії з кінцевим користувачем. Щоб випередити дефіцит або надлишок обчислювальних ресурсів, потрібен інтелектуальний та адаптивний план, що базується на поглибленому аналізі історичних даних. Організації повинні мати механізми для прогнозування своїх потреб у потужностях та проактивного моніторингу програм та інших активів на предмет будь-яких потенційних проблем із потужностями у найближчому майбутньому.

Оповіщення про тенденції, а не про порогові значення

Підхід до сповіщень за замовчуванням зазвичай полягає в налаштуванні сповіщень, які спрацьовують, коли показники перевищують певний поріг. Ви налаштовуєте свої інструменти так, щоб вони повідомляли вас, коли використання процесора сервера перевищує 80 відсотків, наприклад, або коли середній час відгуку програми перевищує 5 секунд.

Проблема з цими сповіщеннями на основі порогових значень полягає в тому, що вони, як правило, не повідомляють про проблеми, доки вони вже не перетворяться на збої. Якщо ваш сервер вже майже повністю завантажений процесором, може бути занадто пізно вирішувати проблему, перш ніж вона вийде з ладу.

Кращою стратегією є налаштування інструментів моніторингу таким чином, щоб вони сповіщали вас про відповідні тенденції, такі як стабільне збільшення використання

процесора або часу відгуку протягом фіксованого періоду часу. Таким чином, ви будете знати раніше, коли починає проявлятися проблемна тенденція, що збільшує ваші шанси на реагування до того, як щось дійсно станеться не так.

Розтин

Розбір інформації після збою, тобто огляди або звіти, які команди готують після збою, щоб оцінити, що пішло не так, є чудовим способом запобігти повторенню подібних проблем у майбутньому.

Вони також корисні для застосування проактивного підходу до моніторингу, оскільки дозволяють вашій команді бути в курсі тенденцій та даних, пов'язаних з перебоями в минулому. Ретельно оцінюючи минулі проблеми, ваші інженери мають кращі можливості для розпізнавання нових проблем у даних моніторингу в режимі реального часу.

Посібники реагування для проактивного моніторингу

Для фахівців з реагування на інциденти та ІТ-інженерів є поширеною практикою розробляти методичні посібники з реагування на інциденти, які допомагають їм вирішувати певні типи інцидентів. Однак, методичні посібники часто призначені для усунення проблем після того, як вони вже перетворилися на інциденти, а не для проактивного вирішення потенційних проблем на ранніх стадіях.

Ось чому варто інвестувати в посібники, які також враховують потреби раннього, проактивного вирішення проблем. Не обмежуйте свої посібники реагуванням на серйозні інциденти.

Зіставлення показників з впливом на бізнес

Не всі потенційні проблеми, які виявляють ваші інструменти моніторингу, матимуть однаковий вплив на бізнес. Іноді сервер може вийти з ладу або програма може вийти з ладу, фактично не порушуючи роботу користувачів, оскільки є резервні ресурси.

З цієї причини розумно класифікувати сповіщення залежно від рівня їхнього впливу на бізнес. Це допоможе вашій команді зрозуміти, на які проблеми, що виникають, слід звернути найбільшу увагу, а які можна відкласти, доки не збереться більше даних. В іншому випадку вони можуть витратити час на спроби вирішити некритичні проблеми проактивно, що ускладнить вирішення справді проблемних.

Як впровадити проактивний моніторинг

Крок 1: Визначте та під'єднайте своє обладнання

Скільки у вас маршрутизаторів і комутаторів? Скільки кінцевих точок? Окрім загального переліку пристроїв, вам потрібно знати, де розташований кожен з них і як він підключається до решти вашої мережі. Проактивні рішення для моніторингу з можливостями картографування дозволяють візуалізувати весь ваш ІТ-ландшафт, автоматично додавати та видаляти обладнання, а також відстежувати дані про стан пристроїв у режимі реального часу.

Крок 2: Визначте свої найважливіші активи

На цьому етапі ви повинні визначити, яка інформація є найважливішою для моніторингу та збору. ІТ-середовища можуть мати десятки тисяч кінцевих точок та пристроїв, тому важливо точно визначити, які з них мають найбільший вплив на успіх вашої організації. Пристрої в цій категорії зазвичай включають комутатори, маршрутизатори, брандмауери та сервери. Після визначення ви повинні визначити, які показники потрібно відстежувати, щоб забезпечити оптимальну роботу пристрою, і чи можете ви ділитися цими даними зі своїми серверами.

Крок 3: Впровадження проактивного рішення для моніторингу

Щойно ви отримаєте уявлення про свою ІТ-систему та чітко визначите структуру пріоритетів, ви зможете впровадити програмне забезпечення для моніторингу, яке автоматично записуватиме та аналізуватиме дані про пристрої та інфраструктуру всієї організації. На цьому етапі вам буде запропоновано налаштувати базові рівні та порогові значення продуктивності.

Після встановлення цих параметрів та запису історичних даних програмне забезпечення, ймовірно, зможе звітувати про показники пристрою, робити прогнози та

виявляти будь-які тенденції, які вимагатимуть розслідування потенційних причин. Це також сприятливий час для налаштування сповіщень на основі винятків для елементів та подій, які ви вважаєте критичними.

Крок 4: Підтримуйте свою інфраструктуру в належному стані

Ви повинні постійно переконатися, що основні комутатори, маршрутизатори та брандмауери, на яких базується ваша мережа, підтримують сучасні протоколи моніторингу продуктивності. Якщо ні, то ви будете обмежені в типі даних про продуктивність, які можете збирати, що значно ускладнить вам своєчасний моніторинг та вирішення будь-яких проблем.

Крок 5: Додайте кібербезпеку, автоматизацію та аналітику

Після впровадження основи вашої стратегії проактивного моніторингу ви можете додавати рівні для підвищення ефективності та заповнення прогалин у безпеці. Наприклад, автоматизацію можна інтегрувати для розгортання процедур усунення недоліків, щоб у разі перевищення або падіння показників нижче певного порогу заздалегідь запрограмована послідовність вирішувала проблему або передавала її відповідному персоналу.

Функції кібербезпеки, такі як виявлення та запобігання вторгненням, можуть використовувати вашу інфраструктуру моніторингу та зібрані нею дані для виявлення шкідливої поведінки у ваших системах. Автоматизовану аналітичну звітність можна налаштувати для генерування та надання зацікавленим сторонам зворотного зв'язку щодо ключових тенденцій і закономірностей у даних, що дозволить вашій організації постійно підвищувати продуктивність.

Електронне управління документами (СЕД) працює за допомогою інтелектуального захоплення та автоматизованого індексування, перетворюючи неструктуровані дані на стратегічні цифрові активи. У провідних системах СЕД оптичне розпізнавання символів (OCR) працює на базі штучного інтелекту (ШІ) для вилучення даних, метаданих та контексту зі сканованих файлів, електронних листів або форм.

Тим часом, алгоритми машинного навчання можуть класифікувати документи на основі змісту, призначення або нормативних вимог.

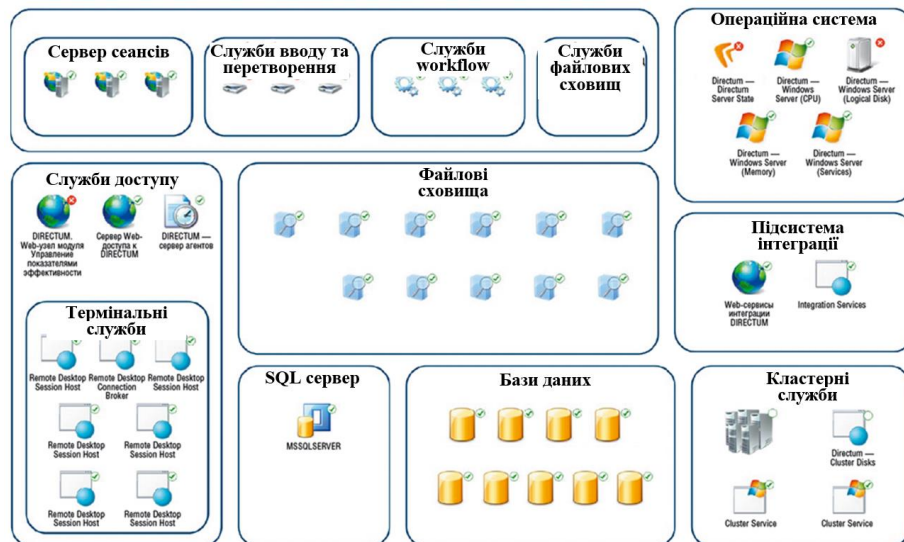


Рисунок 1 – Структурна схема системи

Після оцифрування документи зберігаються в централізованому хмарному сховищі, що забезпечує їх миттєвий пошук. Основні методи категоризації включають:

- Тегування метаданих (наприклад, ідентифікатор клієнта, назва проекту, термін дії).
- Повнотекстовий пошук на базі обробки природної мови (NLP).
- Контроль версій з відстеженням редагувань та затверджень.
- Автоматизовані правила зберігання для забезпечення відповідності нормативним вимогам.

Автоматизація робочих процесів спрощує операції: попередньо визначені правила направляють документи на перевірку, отримання електронних підписів або архівування.

Водночас, інструменти для співпраці в режимі реального часу дозволяють кільком користувачам одночасно редагувати, коментувати або затверджувати файли. Це усуває конфлікти версій та пришвидшує такі процеси, як укладення договору чи відповіді на аудит.

Зрештою, розширена аналітика та інтеграція перетворюють документи на стратегічні інструменти: штучний інтелект визначає тенденції або аномалії у використанні документів, а API-інтерфейси з'єднують систему СЕД з платформами ERP, CRM або відповідності. Варіанти перевірки на основі блокчейну можуть забезпечити захист від несанкціонованого доступу, а автоматизовані зашифровані резервні копії можуть захистити документи протягом усього їхнього життєвого циклу.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів проактивного моніторингу мережевого електронного документообігу. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем проактивного моніторингу мережевого електронного документообігу.
- Досліджена система проактивного моніторингу мережевого електронного документообігу.
- На основі отриманих результатів досліджень створена програмна реалізація системи проактивного моніторингу мережевого електронного документообігу. Розроблені алгоритми дозволяють успішно вирішувати завдання проактивного моніторингу мережевого електронного документообігу. 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., 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. 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 ґешування 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 ґешування 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

Д.Бобровський, магістр гр. КІ-24М,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ЗАХИСТУ ДАНИХ GPRS-МЕРЕЖІ, РОЗГОРНУТОЇ НА ПРИСТРОЯХ, ЯКІ ПРАЦЮЮТЬ ПІД ОС ANDROID

У статті розроблено програмне забезпечення, яке призначено для системи захисту даних GPRS-мережі, розгорнутої на пристроях, які працюють під ОС Android. Метою розробки є дослідження та принципи побудови системи захисту даних GPRS-мережі, розгорнутої на пристроях, які працюють під ОС Android. Об'єктом дослідження є процес захисту даних GPRS-мережі, розгорнутої на пристроях, які працюють під ОС Android. Предметом дослідження є методи захисту даних GPRS-мережі, розгорнутої на пристроях, які працюють під ОС Android. Методи дослідження базуються на методах захисту інформації у мережі, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи захисту даних GPRS-мережі, розгорнутої на пристроях, які працюють під ОС Android. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

системи захисту даних, GPRS-мережа, Android

Постановка проблеми. Щоб можна було скористатися перевагами GSM мереж, їх необхідно захистити. Незахищені бездротові мережі відкривають практично необмежений доступ до корпоративної мережі для хакерів і інших зловмисників, які нерідко прагнуть лише одержати безкоштовний доступ в Internet. Відповідно, дані, які передаються по GPRS, потребують захисту.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи захисту даних GPRS-мережі, розгорнутої на пристроях, які працюють під ОС Android.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи захисту даних GPRS-мережі, розгорнутої на пристроях, які працюють під ОС Android.

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

- Огляд існуючих систем захисту даних GPRS-мережі, розгорнутої на пристроях, які працюють під ОС Android.
- Дослідження системи захисту даних GPRS-мережі, розгорнутої на пристроях, які працюють під ОС Android.
- Програмна реалізація системи захисту даних GPRS-мережі, розгорнутої на пристроях, які працюють під ОС Android.

Об'єктом дослідження є процес захисту даних GPRS-мережі, розгорнутої на пристроях, які працюють під ОС Android.

Предметом дослідження є методи захисту даних GPRS-мережі, розгорнутої на пристроях, які працюють під ОС Android.

Методи дослідження базуються на методах захисту інформації у мережі, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Безпека мобільних даних є критично важливим пріоритетом у 2025 році, оскільки компанії стикаються зі зростанням кіберзагроз,

спрямованих на смартфони, планшети та інші підключені пристрої. Зростання мобільних кіберзагроз, витоків даних та атак шкідливого програмного забезпечення вимагає надійних заходів безпеки. Такі фактори, як віддалена робота, політика BYOD (Bring Your Own Device) та хмарні мобільні сервіси, ще більше ускладнюють проблеми безпеки. Організації повинні впроваджувати рішення для безпеки мобільних даних, щоб запобігти несанкціонованому доступу, витокам даних та фішинговим атакам.

Розуміння безпеки мобільних даних

Безпека мобільних даних передбачає захист конфіденційних даних на мобільних пристроях за допомогою шифрування, автентифікації та методів зменшення загроз.

Забезпечення безпеки мобільних даних має вирішальне значення для запобігання:

- Несанкціонований доступ та витоки даних.
- Атаки програм-вимагачів та шкідливих програм.
- Внутрішні загрози та спроби фітінгу.

Як розвивається ландшафт мобільних загроз

Кібератаки продовжують зростати як за частотою, так і за винахідливістю, і нещодавні звіти лідерів галузі, таких як Verizon та IBM, відзначають стабільне зростання з року в рік. Сьогоднішні зловмисники не просто закидають широкі сітки – вони використовують складні методи, спеціально спрямовані на мобільні пристрої та їхніх користувачів.

Нові та постійні тенденції у сфері мобільних загроз включають:

- Розширене шкідливе програмне забезпечення та фішинг: Шкідливі програми та оманливі посилання можуть проникнути на ваш пристрій, видаючи себе за легітимні завантаження або повідомлення. Зловмисники використовують дедалі переконливіші тактики соціальної інженерії, щоб обманом змусити користувачів відмовитися від облікових даних або встановити шкідливе програмне забезпечення.

- Атаки типу «людина посередині»: пристрої в незахищених мережах вразливі до перехоплення зловмисниками їхніх повідомлень. Цей метод може призвести до витоку конфіденційних даних під час чогось такого простого, як перевірка електронної пошти в громадському Wi-Fi.

- Компрометація пристрою: Зловмисники використовують такі методи, як джейлбрейк та рутінг, для обходу обмежень безпеки, що надає їм глибший доступ до пристрою та його даних. Сучасні загрози здатні маскувати їхню активність, що ще більше ускладнює виявлення.

- Вразливості ОС: Зловмисники швидко використовують нещодавно виявлені вразливості в мобільних операційних системах (відстежуються як CVE), іноді швидше, ніж встигають випустити патчі.

- Контроль доступу до корпоративних ресурсів: Організації спостерігають дедалі більше спроб заражених пристроїв підключитися до внутрішніх мереж, що підвищує ризик витоку даних та несанкціонованого доступу до критично важливих для бізнесу активів.

Щоб випередити ці загрози, потрібні багаторівневі захисні рішення та постійне навчання, що гарантує готовність як пристроїв, так і користувачів до будь-яких загроз, які підкине їм ландшафт мобільних загроз, що розвивається.

Ключові проблеми безпеки в мобільних середовищах:

- Ризики незахищеного Wi-Fi: публічні мережі наражають користувачів мобільних телефонів на кіберзагрози.

- Шкідливі програми та мобільне програмне забезпечення: Зловмисники атакують пристрої через неперевірені програми.

- Ризики втрати та витоку даних: втрачені/викрадені пристрої можуть поставити під загрозу конфіденційні дані.

- Прогалини в безпеці BYOD та корпоративних пристроїв: балансування безпеки з продуктивністю користувачів.

Виявлення та запобігання розширеному джейлбрейку та рутингу

Надійні рішення для мобільної безпеки використовують низку стратегій для виявлення та протидії складним спробам джейлбрейка (iOS) та рутування (Android) пристроїв. Ці інструменти постійно контролюють цілісність пристроїв шляхом:

- Сканування на наявність незвичайних модифікацій системи або несанкціонованих змін у файлах ОС.
- Виявлення наявності сторонніх інструментів керування, які часто використовуються для джейлбрейка/рутингу.
- Використання поведінкової аналітики для позначення підозрілої активності та підвищення привілеїв.
- Забезпечення автоматичного виконання дій відповідності, таких як обмеження доступу до пристроїв або запуск віддаленого стирання, у разі виявлення потенційної компрометації.

Провідні платформи, такі як Lookout, Zimperium та Symantec, інтегрують ці заходи виявлення загроз, щоб забезпечити доступ до конфіденційних бізнес-ресурсів лише безпечним пристроям, що відповідають політикам.

Вплив генеративного штучного інтелекту на мобільну безпеку

Генеративний штучний інтелект швидко трансформує ландшафт мобільних загроз, впроваджуючи нові та складні методи атак, які вимагають нашої уваги. Від переконливих фішингових повідомлень, що генеруються на льоту, до автоматизованих атак соціальної інженерії, загрози на базі штучного інтелекту тепер можуть обходити традиційні засоби захисту з безпрецедентною швидкістю та тонкістю.

Щоб випереджати ці ризики, що змінюються, організаціям слід:

- Впроваджуйте виявлення загроз на основі штучного інтелекту: використовуйте інструменти безпеки від таких постачальників, як Palo Alto Networks та Symantec, які використовують машинне навчання для виявлення незвичайної поведінки та нових загроз.
- Навчайте користувачів шахрайству на основі штучного інтелекту: регулярно навчайте співробітників та користувачів мобільних пристроїв розпізнавати дипфейкові дзвінки, голосовий фішинг (вішинг) та ретельно розроблені шкідливі повідомлення.
- Впроваджуйте безперервне сканування програм: використовуйте рішення, які відстежують шкідливі програми та код, створений або розроблений за допомогою методів генеративного штучного інтелекту.
- Посилення контролю автентифікації: поєднання біометричної автентифікації та адаптивної багатофакторної автентифікації (MFA) для мінімізації ризику підробки облікових даних за допомогою штучного інтелекту або видання себе за іншу особу.

Інвестування в рішення, що розвиваються разом із загрозами, спричиненими штучним інтелектом, може бути вирішальним фактором між реагуванням на порушення та його запобіганням. Проактивна адаптація зараз є важливою для сучасної мобільної безпеки.

Як виявляються та управляються вразливості операційної системи

Програмне забезпечення для захисту мобільних даних проактивно сканує пристрої на наявність вразливостей операційної системи, постійно відстежуючи нові виявлені CVE (поширені вразливості та ризики). Провідні рішення використовують оцінку ризиків у режимі реального часу, регулярно перевіряючи налаштування пристроїв, конфігурації системи та дозволи. Розширені інструменти від таких постачальників, як Symantec та Lookout, сповіщають адміністраторів щоразу, коли вони виявляють ознаки компрометації, несанкціоновані зміни конфігурації або спроби рутування чи джейлбрейка пристрою.

Ці рішення допомагають ІТ-командам випереджати загрози завдяки:

- Виявлення та позначення невивірених вразливостей і ризикованих конфігурацій.
- Надання автоматизованих інструкцій або опцій віддаленого виправлення.
- Блокування спроб компрометації до того, як відбудеться експлуатація.

Підтримуючи постійний контроль за станом операційної системи та забезпечуючи дотримання надійних конфігурацій, організації можуть значно знизити ризик успішних мобільних атак або витоків даних.

Ключові характеристики, які слід шукати в програмному забезпеченні для безпеки мобільних даних

- Розширений захист від мобільних загроз (MTD): виявлення фішингу, шкідливого програмного забезпечення та загроз нульового дня на основі штучного інтелекту.

- Наскрізне шифрування: Безпечний мобільний зв'язок, електронна пошта та обмін файлами.

- Безпечна контейнеризація: ізоляція бізнес-даних та особистих даних на одному пристрої.

- Можливості віддаленого стирання та блокування: запобігання втраті даних у разі крадіжки або компрометації пристрою.

- Багатофакторна автентифікація (MFA) та біометричний захист: забезпечення безпечного входу.

- Запобігання втраті даних (DLP): обмеження несанкціонованого доступу до даних та їх передачі.

- Мобільний VPN та мережева безпека: захист даних у публічних та корпоративних мережах.

- Хмарне керування мобільною безпекою: керування політиками безпеки для віддалених користувачів.

Інфраструктура мережевої безпеки: попередження нових загроз

Інфраструктура безпеки мобільних мереж відіграє ключову роль у допомозі підприємствам проактивно захищатися від нових і постійно зростаючих загроз. Використовуючи передові засоби захисту на пристроях, подібні до тих, що містяться в провідних пакетах безпеки для настільних комп'ютерів, організації можуть забезпечити безпеку мобільних кінцевих точок, навіть коли користувачі підключаються через незахищені мережі Wi-Fi або стільникового зв'язку.

Деякі ключові переваги включають:

- Виявлення загроз у режимі реального часу: Розширена система безпеки на рівні мережі постійно відстежує шкідливу активність, включаючи спроби фішингу, підозрілий трафік та атаки типу «людина посередник», зупиняючи загрози до того, як вони вплинуть на пристрої або конфіденційні дані.

- Безшовна інтеграція: Ці рішення працюють разом з існуючими політиками безпеки підприємства, поширюючи на мобільні пристрої той самий надійний захист, який уже діє для традиційних кінцевих точок.

- Захист з будь-якого місця: Співробітники часто підключаються з аеропортів, готелів або кав'ярень. Надійний рівень мережевої безпеки гарантує захист конфіденційних бізнес-даних незалежно від місцезнаходження.

Впроваджуючи комплексні стратегії мережевої безпеки від таких постачальників, як Lookout, Zimperium та Symantec, організації можуть значно зменшити свій вплив як відомих, так і нових кіберзагроз на мобільних платформах.

Блокування заражених пристроїв з корпоративних ресурсів

Провідні платформи безпеки використовують комбінацію моніторингу стану пристроїв у режимі реального часу та динамічного контролю доступу, щоб захистити конфіденційні дані компанії від скомпрометованих пристроїв. Коли виявляються загрози – будь то шкідливе програмне забезпечення, фішингові атаки чи неавторизовані програми – програмне забезпечення автоматично скасовує або обмежує доступ до корпоративних мереж, хмарних сервісів та критично важливих для бізнесу програм.

Наприклад, такі рішення, як Lookout та Zimpregium, використовують оцінки ризиків на основі штучного інтелекту для постійного сканування пристроїв. Якщо виявлено загрозу, платформа може:

- Миттєво ізолюйте пристрій від корпоративних VPN, електронної пошти та інструментів для співпраці.
- Застосування політик умовного доступу через інтеграцію з постачальниками ідентифікаційних даних (таких як Okta або Microsoft Entra).
- За потреби активувати протоколи віддаленого стирання.

Поєднуючи автоматичне виявлення, забезпечення дотримання політик та сегментацію на рівні мережі, ці платформи допомагають забезпечити доступ до ресурсів вашої організації лише справних пристроїв, що відповідають вимогам.

Переваги єдиного захисту кінцевих точок в одному клієнті

Керування безпекою мобільних даних для сучасних віддалених працівників може швидко перетворитися на жонглювання десятками інструментів, кожен з яких має свої особливості та портали. Саме тут на допомогу приходить універсальний клієнт захисту кінцевих точок, який поєднує платформи захисту кінцевих точок (EPP), засоби виявлення та реагування на кінцеві точки (EDR) та розширене виявлення та реагування (XDR) в одному оптимізованому пакеті.

Чому варто об'єднати кошти до одного клієнта:

- Спрощене керування безпекою: маючи все під одним дахом, IT-команди можуть контролювати, налаштовувати та застосовувати політики з централізованої панелі інструментів, що зменшує адміністративні труднощі.
- Зменшення складності та покращення продуктивності: Запуск кількох агентів безпеки часто призводить до уповільнення роботи системи та проблем сумісності. Уніфікований клієнт потребує менше ресурсів та зменшує ризик конфліктів.
- Комплексна видимість загроз: інтеграція EPP, EDR та XDR забезпечує швидше виявлення загроз та реагування на них на кінцевих точках, у мережах та хмарних середовищах, чого важко досягти за допомогою об'єднаних інструментів.
- Стабільне покриття: Від програм-вимагачів до шкідливих програм нульового дня, єдине консолідоване рішення гарантує відсутність прогалин у безпеці між непов'язаними інструментами.
- Спрощені оновлення та виправлення: Замість того, щоб витрачати час на оновлення для кількох окремих програм, єдиний клієнт дозволяє розгортати найновіші засоби захисту одночасно, забезпечуючи стійкість усіх кінцевих точок до нових загроз.

Примітно, що провідні постачальники рішень безпеки, такі як CrowdStrike, SentinelOne та Sophos, застосували цей підхід, зробивши надійну комплексну безпеку кінцевих точок новим стандартом для гнучких та безпечних мобільних працівників.

Найкращі практики для посилення мобільної безпеки:

- Впроваджуйте стратегію захисту від мобільних загроз (MTD) – захищайтеся від шкідливого програмного забезпечення, фішингу та мережевих загроз.
- Забезпечте надійне мобільне шифрування та автентифікацію – використовуйте біометричні дані для входу та багатофакторну автентифікацію.
- Розгортання політик безпеки мобільних пристроїв підприємства – визначення правил безпечного використання програм і доступу до даних.
- Моніторинг та усунення ризиків мобільної безпеки – постійне відстеження вразливостей та неправильних конфігурацій.
- Увімкніть безпечний перегляд мобільних веб-сторінок та захист електронної пошти – запобігайте фішинговим атакам та атакам типу «людина посередині» (MITM).
- Забезпечте запобігання втраті даних (DLP) на мобільних пристроях – контролюйте обмін файлами та обмеження доступу.

Як забезпечити душевний спокій під час вибору програмного забезпечення для мобільної безпеки

Вибір правильного програмного забезпечення для мобільної безпеки має вирішальне значення для захисту ваших особистих даних та забезпечення душевного спокою. Ось як споживачі можуть прийняти обґрунтоване рішення:

1. Широко дослідіть: почніть з вивчення різних варіантів на ринку. Шукайте відгуки та експертні оцінки на надійних технологічних веб-сайтах. Ці дані можуть виявити сильні та слабкі сторони програмного забезпечення.

2. Порівняння функцій: Визначте основні функції, такі як захист від шкідливого програмного забезпечення, можливості захисту від фішингу та запобігання крадіжкам. Порівняйте продукти, щоб побачити, який з них пропонує повне покриття.

3. Перевірте незалежні тести: Шукайте програмне забезпечення, яке пройшло незалежне тестування у відомих лабораторіях кібербезпеки. Сертифікати від сторонніх організацій можуть гарантувати надійність та ефективність.

4. Відгуки користувачів: Відгуки користувачів безцінні. Перегляньте онлайн-форуми та магазини додатків, щоб дізнатися про реальний досвід, який може виявити потенційні проблеми або видатні функції.

5. Пробні версії: оберіть програмне забезпечення, яке пропонує безкоштовний пробний період. Це дозволить вам безпосередньо випробувати функціональність та оцінити зручність використання без початкових витрат.

6. Підтримка клієнтів: Надійна служба підтримки клієнтів може стати справжнім порятунком у разі технічних проблем. Перевірте, чи пропонує компанія доступні та оперативні варіанти підтримки.

Ретельно досліджуючи та оцінюючи рішення для мобільної безпеки на основі цих факторів, споживачі можуть вибрати продукт, який не лише відповідає їхнім потребам, але й забезпечує душевний спокій.

Розуміння переваг тестування програмного забезпечення для мобільної безпеки

У сучасну цифрову епоху забезпечення безпеки вашого мобільного пристрою є надзвичайно важливим. Але яку користь вам як споживачеві насправді приносить процес тестування та оцінки програмного забезпечення для мобільної безпеки? Давайте розглянемо це детальніше.

Обґрунтоване прийняття рішень

Коли експерти тестують та оцінюють варіанти мобільної безпеки, вони надають вам важливу інформацію про їхню продуктивність та ефективність. Замість того, щоб сліпо вибирати програмне забезпечення, ви маєте доступ до:

— Детальні звіти порівняння: Подивіться, як різні продукти порівнюються один з одним з точки зору функцій та рівнів захисту.

— Показники продуктивності: Зрозумійте, яке програмне забезпечення пропонує найкращий захист без шкоди для продуктивності вашого пристрою.

Посилена гарантія безпеки

Не все програмне забезпечення для мобільної безпеки однакове. Завдяки ретельному тестуванню:

1. Перевірка ефективності: Ви дізнаєтесь, які рішення є найефективнішими для блокування таких загроз, як шкідливе програмне забезпечення, спроби фішингу та підозрілі програми.

2. Оновлений захист: гарантує, що програмне забезпечення може адаптуватися до найновіших загроз безпеці, забезпечуючи безпеку ваших даних.

Ефективність витрат

Інвестування в правильне програмне забезпечення для мобільної безпеки означає розумні витрати. Огляди тестування можуть виділити:

– Співвідношення ціни та якості: Визначте продукти, які пропонують найкращі характеристики за розумною ціною.

– Уникнення помилок: заощаджуйте гроші, уникаючи неякісного програмного забезпечення, яке не забезпечує належного захисту.

Аналітика користувацького досвіду

Окрім безпеки, критично важливим є те, як програма взаємодіє з користувачами. Тестування показує:

– Простота використання: Дізнайтеся, яке програмне забезпечення має зручні інтерфейси, що роблять навігацію легкою.

– Підтримка клієнтів: Зрозумійте рівні підтримки, що пропонуються, якщо у вас виникнуть будь-які проблеми або вам знадобиться допомога.

Перетворюючи комплексне тестування на чіткі, практичні висновки, споживачі краще підготовлені до вибору програмного забезпечення для мобільної безпеки, яке не лише відповідає їхнім потребам, але й забезпечує душевний спокій у цифровому світі.

Для високих вимог безпеки галузі ми повинні забезпечити безпеку передачі даних. Які способи гарантують безпеку даних під час використання GPRS-модемів? Існує наступний спосіб вирішення проблеми: оператори APN або VPDN впроваджують технологію тунелювання VPDN, що передбачає інкапсуляцію даних у корпоративній мережі для передачі в тунелі. Основний процес тунелювання полягає в тому, що на інтерфейсі між вихідною локальною мережею (LAN) та загальнодоступною мережею дані упаковуються в контейнер у форматі передачі даних загальнодоступної мережі. На інтерфейсі з загальнодоступною мережею LAN цільове рішення інкапсулює дані та знімає навантаження.

Логічний шлях – це інкапсульовані пакети, що передаються через Інтернет, що називається «тунелюванням». Для забезпечення плавної інкапсуляції, передачі та декапсуляції даних використовується протокол зв'язку, який забезпечує безперебійну роботу ядра. Може використовуватися для міжрегіональної групової інтрамережі, спеціалізованої мережі постачальників професійних інформаційних послуг, магістральних мереж, фінансових державних послуг, банківських та інших послуг для доступу до бізнес-мереж. У практичному застосуванні операторам необхідно відкрити відповідний бізнес-проект, а для його реалізації – прокласти власну лінію зв'язку. Недоліком є громіздкість бізнес-процедур, висока вартість використання та непридатність для загальних проектів. Якщо ви не можете подати заявку на спеціальні мережеві послуги, чи є інші способи забезпечити безпеку даних? Це може бути забезпечено лише апаратним забезпеченням.

У галузі GPRS-модемів зазвичай немає такої функції. У Сямень комунікаційні компанії протягом багатьох років досліджували бездротове термінальне обладнання для передачі даних, і останній продукт компанії – WCTU. Підтримка шифрування даних, підтримка шифрування для DES, 3DES, AES. Під час налаштування WCTU лише запусить відповідні налаштування. Коли дані WCTU пакетуються, вони використовують шифрування DES, 3DES та AES. Такі дані не турбуються про безпеку в Інтернеті. Ця функція зручна та проста у використанні, її слід популяризувати.

Щоб ефективно керувати своєю мережею та приймати обґрунтовані рішення, вам потрібно збирати інформацію про моделі мережевого трафіку. Якщо у вас виникли проблеми, пов'язані з підключенням або безпекою, вам потрібно мати змогу виявляти зміни в трафіку. Carrier Security надає набір інструментів, що відповідають особливим потребам стільникових мереж.

Журнали та сповіщення відстеження GTP

Служба безпеки оператора записує інформацію про активність сигналізації GTP, що стосується стільникового зв'язку, включаючи APN, IMSI, режим вибору, адреси GSN тощо. Інформація, записана в цих журналах, може допомогти вам визначити, чому певний трафік GTP може бути відхилений або заблокований, а також вирішити, чи слід налаштувати Політику безпеки для прийняття цього трафіку.

Шлюз перевірки GTP Carrier Security генерує широкий спектр детальних сповіщень безпеки у разі порушень протоколу та політики безпеки, включаючи деталі PDU, інформацію про мережу та тип порушення протоколу. Carrier Security також надає сповіщення, специфічні для GTP, про неправильно сформовані пакети та шкідливу активність.

Запис даних GTP з незрівнянних PDU

Carrier Security може записувати GTP-трафік, який не відповідає правилу GTP у базі правил. Зазвичай трафік, який не відповідає правилу, реєструється в загальному журналі як простий Drop. Carrier Security надає інструмент для збору цих даних за допомогою спеціальних полів, пов'язаних із GTP, які можуть допомогти виявити причину цих падінь.

Бухгалтерський облік GTP

Встановивши правило трафіку користувача GTP на Log, Carrier Security створює запис у журналі для кожного завершеного контексту PDP, який відповідає правилу. У журналі записується загальна кількість користувацьких пакетів (n_pdu) та байтів (n_byte), переданих у площині користувача під час контексту PDP. Carrier Security створює журнали для таких подій:

- Видалення контексту/сеансу PDP.
- Закінчення терміну дії тунелю.
- Відпочинок у тунелі.
- Активний шлюз не працює (у режимі високої доступності).

Захист від надмірних журналів

Через малу кількість пакетів стільникового зв'язку, Carrier Security щодня записує величезну кількість даних, набагато більше, ніж типовий брандмауер Check Point. Цей збір даних є важливим для точної діагностики стану мережі та усунення помилок мережі.

Така інтенсивна активність ведення журналу може зробити деякі системи більш вразливими до атак типу «відмова в обслуговуванні» (DoS). Carrier Security захищає від цього типу атаки, встановлюючи similar logging поріг, вище якого аналогічні журнали не генеруються. Цю функцію можна налаштувати.

За замовчуванням – кожні 10 секунд.

Режим лише монітора

Режим лише моніторингу відстежує певний несанкціонований трафік, не блокуючи його. У цьому режимі брандмауер продовжує перевіряти трафік GTP, але не застосовує жодних засобів захисту, пов'язаних з GTP. Він продовжує застосовувати правила безпеки, пов'язані з GTP, реєструвати активність, пов'язану з GTP, а також створювати журнали помилок і сповіщення GTP. Режим лише моніторингу дозволяє операторам переглядати результати змін глобальних властивостей і налаштувань, що стосуються перевірки GTP. Цей режим корисний для запобігання непередбачуваним поведінці під час першого впровадження безпеки оператора, а також щоразу, коли в глобальні властивості вносяться зміни.

Після ретельного перегляду журналів та переконання, що зміни не перешкоджають легітимному стільниковому трафіку, оператор стільникового зв'язку може вимкнути режим «Тільки моніторинг», а брандмауер може почати блокувати шкідливий GTP-трафік.

Carrier Security слідкує за тунелями GTP та зберігає їх statetак, як це було б у звичайному режимі роботи. Таким чином, ви можете плавно вмикати та вимикати режим лише моніторингу – вся інформація про тунель продовжує існувати в обох режимах, і жодні тунелі не втрачаються під час переходу.

Налаштування моніторингу

– Створювати розширений журнал для незбіганих PDU. Реєструє GTP-пакети, які не збігаються з попередніми правилами, за допомогою розширених полів журналу, пов'язаних з GTP, Carrier Security. Ці журнали мають коричневий колір, а їхній атрибут Action порожній. Значення за замовчуванням – checked.

– Опція відстеження порушення протоколу дозволяє встановити відповідну опцію відстеження або сповіщення, яка використовуватиметься у разі виявлення порушення протоколу (спотвореного пакета). Налаштування за замовчуванням – Log.

GPRS-мережа має зв'язку з великою кількістю зовнішніх мереж (інтернет, роумінг-партнери, корпоративні клієнти, провайдери GRX (GPRS Roaming Exchange), і т.д.). Таке сусідство й партнерські відносини ставлять перед мобільними операторами підвищені вимоги по забезпеченню безпеки переданих даних. Так як зв'язок з партнерами й доступ в інтернет здійснюється по протоколі IP, а усередині GPRS-магістралі дані інкапсулюються в небезпечні тунелі GTP, те границю GPRS-мережі необхідно надійно захищати.

Основну погрозу представляють напрямки Gi і Gp, так як використовуючи протокол IP, будь-який користувач може посилати довільні пакети в GPRS-мережу. Оскільки оператори не обмежують типи користувальницького трафіку, користувачі мобільних терміналів перебувають повністю відкритими для всіх недуг інтернету (віруси, хробаки, трояни, DoS і т.д.). Відповідно, не захищені й користувальницькі дані, які відправляються в зовнішні мережі. Також більшість атак можуть бути спрямовані на саму GPRS-інфраструктуру (Gn), викликаючи відмову або некоректну роботу устаткування.

Типи атак на потенційно небезпечних GPRS-інтерфейсах:

1.Gp-інтерфейс:

- паразитний трафік роумінг-партнера;
- DNS флуд;
- GTP флуд;
- довільне видалення PDP- контекстів користувачів;
- некоректна BGP-інформація;
- підміна DNS-відповідей;
- підміна запитів Create/Update PDP Context;
- overbilling attacks.

2.Gi-інтерфейс:

- DoS-атаки;
- флуд з IP-адрес мобільних станцій;
- влучення в корпоративну мережу іншого клієнта.

3.Gn-інтерфейс:

- підміна GGSN/SGSN;
- підміна запиту видалення PDP-контекстів користувачів;
- атаки мобільних користувачів друг проти друга.

Завдання захисту Gn і Gp інтерфейсів ускладнює особливість комунікацій, які ведуться там по засобом протоколу GTP.

Принцип роботи GTP кардинально відрізняється від інших IP-протоколів: GTP-тунель може бути розподілений по декількох IP-сесіях, і навпаки – одна IP-сесія може містити трохи GTP-тунелів. Такий принцип роботи робить практично марним застосування класичних IP-Firewall для фільтрації GTP-трафіку. Виходячи з того, що звітка IP-трафік на інтерфейсах Gn і Gp інкапсульован в GTP, на даних інтерфейсах необхідний GTP Firewall для перевірки коректності функціонування GTP.

Безліч атак функціонує на більше високих рівнях подання даних (Layer 5-7), ніж ті, з якими працює фаєрвол (Layer 2-4). Тому, як другий ешелон захисту від атак рівня додатків, потрібна система запобігання вторгнень. Аналізуючи легітимний трафік, що пройшов через Firewall на Layer 2-4 дана система проведе високорівневий аналіз і зможе виявити й запобігти атакам, що ховаються в трафіку додатків. Стосовно до GPRS-мережі, такий підхід вибудовування системи захисту особливо ефективний у точці підключення до мережі інтернет (інтерфейс Gi).

Пропонується використовувати ефективне рішення для операторів зв'язку, що здатно забезпечувати безпека трафіку в будь-якій точці GPRS-мережі. Мова йде про лінійку високопродуктивних шлюзів безпеки Juniper High-End SRX з підтримкою GTP. Пристрою

Juniper HE SRX – це універсальна модульна платформа, що поєднує функціонал різних пристроїв (firewall, маршрутизатор, комутатор, UTM, IDP) в одному шасі. Всі пристрої працюють під керуванням надійної платформи JunOS, що успішно зарекомендувала себе в сегменті магістральних рішень. Модульна архітектура SRX дозволяє гнучко масштабувати продуктивність для виконання необхідного функціоналу. Підтримка протоколу GTP робить їхнім незамінним рішенням питань безпеки для мобільних GPRS-операторів зв'язку, що легко інтегрується з технологією GPRS Tunneling Protocol.

Впровадження Juniper HE SRX у на найнебезпечніших ділянках GPRS-мережі, а саме, на інтерфейсах Gn і Gp, забезпечить перевірку коректності роботи протоколу GTP і контроль інформаційних потоків між PLMN. А наявність убудованої системи запобігання вторгнень (Juniper IDP) дозволяє High-End SRX забезпечувати фільтрацію трафіку й високоінтелектуальний захист від атак одночасно. Дана особливість оптимально підходить для захисту Gi інтерфейсу GPRS-мережі, що забезпечує взаємодію з небезпечним Інтернетом.

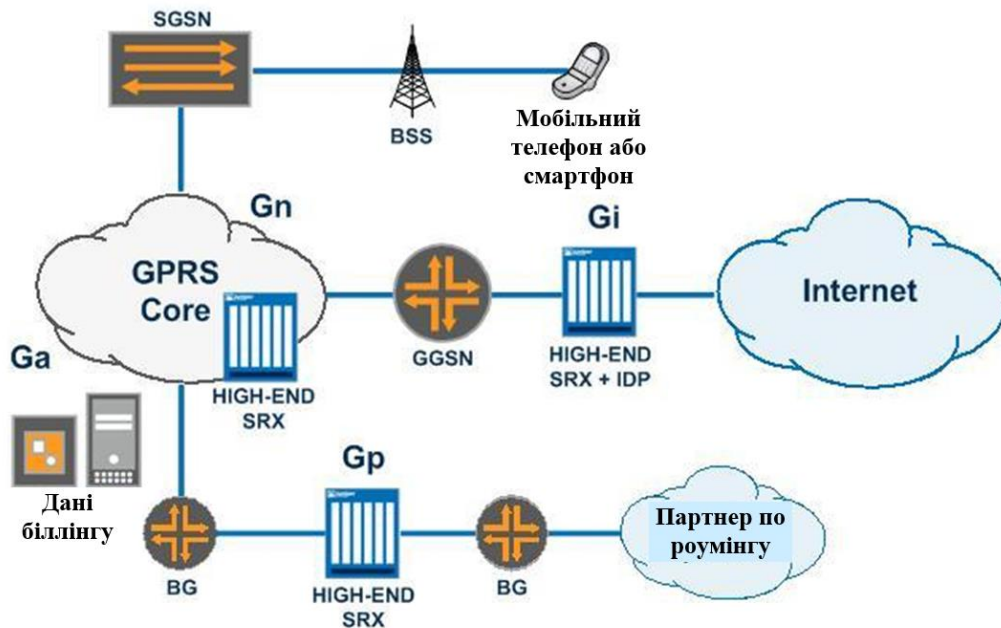


Рисунок 1 – Структурна схема системи

При впровадженні SRX важливо враховувати місце в топології GPRS-мережі.

Інтерфейс Gp

У даній точці важливо виділити сервіси, необхідні для взаємодії з роумінг-партнерами прямо або через GRX. У загальному випадку для підключення роумінг-абонента, необхідно забезпечити зв'язок локального SGSN і GGSN його оператора. Для встановлення такого підключення використовується GTP. Крім цього, між PLMN різних операторів повинні функціонувати мережні протоколи BGP і DNS (перетворення імен APN). Основні погрози на Gp інтерфейсі пов'язані з функціонуванням GTP. Для зменшення даних ризиків рекомендовано вживати наступних заходів:

- фільтрація вхідних/вихідних пакетів: запобігає обміну даними з невідомим роумінг-операторами (при підключенні до GRX) і можливість спуфінг-атак від імені локальної PLMN;
- stateful-фільтрація GTP-пакетів: фільтрація GTP-сесій з невідомими PLMN для запобігання атак і розвантаження локальних GSN;
- обмеження смуги GTP: запобігання DoS-атак, виділення достатньої смуги для роботи GTP, BGP, DNS;
- установа IPsec-тунелів з роумінгами-партнерами: забезпечення автентифікації й конфіденційності переданих даних;

– запобігання overbilling-атак: повідомлення Gi Firewall про “завислі” сесії для запобігання переплати абонента.

Інтерфейс Gn

Погрози можуть виходити як зсередини мережі оператора, так і бути спрямованими на устаткування мережі. Залежно від інтенсивності атаки можливий варіант тимчасового виводу з ладу устаткування мережі. Це у свою чергу виливається в простоту, втрату сервісу, прибутки й невдоволення абонентів. Для усунення даних ризиків рекомендується використовувати політики розмежування доступу й фільтрацію пакетів на основі стану GTP-сесій. Наприклад, у випадку атаки із застосуванням підміни адреси GGSN, запит GTP PDP Context Delete буде відкинутий якщо перед цим не було GTP PDP Context Create повідомлення.

Інтерфейс Gi

Становить особливу небезпеку, хоч і не вимагає декапсуляції й контролю GTP. Основні механізми захисту включають:

- поділ логічних тунелів для підключення корпоративних клієнтів і впровадження IPSec у випадку використання каналів Інтернет;
- пріоритезація трафіку корпоративних користувачів і IPSec для недопущення можливості відмови каналів абонентів;
- інспектування пакетів з урахуванням стану сесій – використання політик розв'язне тільки ініціювання підключень із боку мобільних станцій;
- фільтрація вхідних/вихідних пакетів – запобігає можливість пересилання даних від IP-адрес мобільної станції, отриманих для виходу в Інтернет, на іншу мобільну станцію;
- запобігання overbilling-атак.

Також загальним підходом при реалізації механізмів безпеки в GPRS-мережах є використання часток IP-адрес для внутрішніх елементів інфраструктури мережі.

Функціонал для безпеки GTP включає:

1. GTP packet sanity check (перевірка заголовка кожного пакета GTP/UDP на відповідність стандарту).
2. GTP stateful inspection (перевірка GTP пакетів на відповідність поточному стану GTP-тунелю в контексті передачі попередніх пакетів; при одержанні пакета не приналежному поточному стану GTP обміну, пристрій відкидає пакет).
3. GGSN redirection (функція перенапряму запиту GTP PDP Context Create; у запиті вказуються IP-адреси інших GGSN, після чого GTP-U і GTP-C повідомлення посиляють зазначеним IP).
4. Policy-based GTP inspection (обмеження доступу між різними PLMN на основі визначення політик безпеки шляхом асоціації PLMN із зонами безпеки).
5. GTP message length filtering (фільтрація GTP-пакетів, що не відповідають мінімальній або максимальній довжині GTP-повідомлення).
6. GTP message type screening (фільтрація GTP-пакетів певного типу).
7. GTP IMSI prefix and APN filtering (фільтрація GTP-пакетів від невідомих PLMN на основі ідентифікатора мережі абонента (IMSI) і шляхи доступу абонента (APN)).
8. Removal of IEs of GTP R6 (функція видалення специфічних атрибутів 3GPP заголовки пакета GTP при наступній передачі в мережі 2GPP).
9. GSN rate limiting (зниження навантаження на GSN за допомогою обмеження швидкості обробки GTP-C пакетів).
10. GTP sequence number validation (функція перевірки порядкових номерів повідомлень G-PDU під час PDP-активації контексту).
11. Cleanup of hanging GTP tunnel (автоматичне видалення “висячих” GTP-тунелів).
12. GTP traffic logging (функція протоколювання GTP-пакетів на основі статусу (forwarded, prohibited, rate-limited, state-invalid, tunnel-limited))
13. GTP tunnel failover for high availability (функція підтримки активних GTP-сесій у режимі відказостійкості).

Переваги:

1. Модульна архітектура.
2. Можливість гнучкого масштабування.
3. Функціонал повноцінного маршрутизатора, фаєрволу, системи запобігання вторгнень і UTM (антивірус, антиспам, веб-фільтр, контент-фільтр).
4. Повна підтримка GTP і механізмів забезпечення його безпеки.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів захисту даних GPRS-мережі, розгорнутої на пристроях, які працюють під ОС Android. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем захисту даних GPRS-мережі, розгорнутої на пристроях, які працюють під ОС Android.
- Досліджена система захисту даних GPRS-мережі, розгорнутої на пристроях, які працюють під ОС Android.
- На основі отриманих результатів досліджень створена програмна реалізація системи захисту даних GPRS-мережі, розгорнутої на пристроях, які працюють під ОС Android. Розроблені алгоритми дозволяють успішно вирішувати завдання захисту даних GPRS-мережі, розгорнутої на пристроях, які працюють під ОС Android. 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. 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.
2. 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.
3. Усїк, 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
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. 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. 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.
9. 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.
10. 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.
11. 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.
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. 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.
15. 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.
16. Akhalaia, G., Iavich, M., Iashvili, G., Prysiazhnyy, D., Smirnova, T. «Secure Encrypted Connection on Georgian Website». CEUR Workshop Proceedings, 2023, 3550, pp. 313-320.
17. 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
18. 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.
19. 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.
20. Smirnov, O., Lakhno, V., Akhmetov, B., Chubaievskiy, V., Khorolska, K., Bebashko, 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.
21. 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.
22. 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.
23. 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.
24. 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.
25. 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.
26. Smirnov, O., Neskoriy, T., Fedorov, E., Rudakov, K., Neskoriy, A. «Method Detection Audit Data Anomalies on Basis Restricted Cauchy Machine» CEUR Workshop Proceedings, Volume 3187, 2022,
27. 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.
28. 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.
29. 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.
30. 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.
31. 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.

УДК 004

О.Бойко, магістр гр. КІ-24М,*Центральноукраїнський національний технічний університет*

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ КЛІЄНТА ВКЗ ЗА ДОПОМОГОЮ ТЕХНОЛОГІЇ WEBRTC

У статті розроблено програмне забезпечення, яке призначено для системи клієнта ВКЗ за допомогою технології WebRTC. Метою розробки є дослідження та принципи побудови системи клієнта ВКЗ за допомогою технології WebRTC. Об'єктом дослідження є процес клієнта ВКЗ за допомогою технології WebRTC. Предметом дослідження є методи клієнта ВКЗ за допомогою технології WebRTC. Методи дослідження базуються на методах обробки інформації у комп'ютерній мережі, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи клієнта ВКЗ за допомогою технології WebRTC. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

відео-конференц-зв'язок, WebRTC

Постановка проблеми. Визначальний вплив на розвиток загальносвітового ринку ВКЗ в останні кілька років роблять підвищення мобільності користувачів і потребу в простих й зручних у використанні рішеннях. При виборі продукту все частіше перевага віддається пристроям з інтуїтивно зрозумілим інтерфейсом, які легко включаються й не вимагають докладних інструкцій для експлуатації. По усьому світі люди прагнуть до максимальної мобільності й воліють якнайменше часу проводити прив'язаними до свого робочого місця. Тому для сучасних працівників надто важливо поза залежністю від місцезнаходження одержувати всі ті ж функції, що й в офісі, у тому числі можливість взаємодіяти зі своїми колегами з використанням високоякісного відео.

Ці тенденції проявляються й на українському ринку, хоча попит на мобільні рішення багато в чому залежить від рівня розвитку міської інфраструктури й часу, що людям доводиться витрачати на дорогу до роботи. Сучасний мегаполіс, такий як Київ, змушує жителів щодня проводити в пробках по кілька годин. На щастя, якісне інтернет-підключення доступно в столиці практично повсюдно й при наявності відповідних інструментів дозволяє працювати з будинку без втрати функціональності. Головними драйверами розвитку ВКЗ є представники покоління Y (люди, що народилися з 1980 по 2000 рік). Вони прекрасно орієнтуються в технологічних новинках, активно користуються відеозв'язком, різними месенджерами й соціальними мережами. Таким чином, і нові ВКЗ-рішення повинні бути настільки ж мобільними, інтуїтивно зрозумілими й гнучкими, як технології соціальної взаємодії.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи клієнта ВКЗ за допомогою технології WebRTC.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи клієнта ВКЗ за допомогою технології WebRTC.

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

- Огляд існуючих систем клієнта ВКЗ за допомогою технології WebRTC.
- Дослідження системи клієнта ВКЗ за допомогою технології WebRTC.

– Програмна реалізація системи клієнта ВКЗ за допомогою технології WebRTC.

Об'єктом дослідження є процес клієнта ВКЗ за допомогою технології WebRTC.

Предметом дослідження є методи клієнта ВКЗ за допомогою технології WebRTC.

Методи дослідження базуються на методах обробки інформації у комп'ютерній мережі, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Основні тенденції ринку ВКЗ:

– Підвищення мобільності користувачів.

– Ріст потреби в рішеннях із простим, інтуїтивно зрозумілим інтерфейсом.

– Можливість підключення до ВКЗ без якого-небудь програмного клієнта – просто через браузер завдяки технології WebRTC.

– Інтеграція з іншими системами, у першу чергу Skype for Business і системою корпоративної телефонії.

– Зниження цін за рахунок посилення конкуренції, поширення нових моделей (хмари), зміни схем ліцензування та ін.

Термінали: групові й/або персональні

Багаторічні дослідження показують, що частка замовників, що використовують групові термінали ВКЗ, не знижується. Різкого росту числа компаній, що застосовують персональні термінали, також не спостерігається. Хоча, звичайно, загальне число індивідуальних засобів відеозв'язку росте швидше, ніж число групових систем.

Грунтуючись на статистику продажів, відзначимо, що динаміка продажів групових систем у цілому треба за ринком: при погіршенні економічної ситуації в країні попит на них падає, при поліпшенні – збільшується. Тоді як продажу настільних відеосистем від стану ринку не залежать і рік у рік перебувають практично на одному рівні. Імовірно, це обумовлено тим, що в нас у країні настільний відеотелефон так і не став інструментом рядових співробітників компаній і позиціонується як засіб зв'язку керівника.

Тому що наші основні замовники – це великі корпорації й державні організації, найбільше продається групових терміналів. Відзначимо також ріст попиту на ПЗ зв'язкове сполучення відео-конференц-зв'язку для мобільних пристроїв і ПК, що пов'язане з ростом числа мобільних співробітників і розвитком концепції віддаленої роботи в Україні.

Поява нового стандарту WebRTC з підтримкою SVC здатна зробити революцію, схожу з тією, що викликали програмні рішення.

Для задоволення поточний бізнес-потреб часом вигідніше побудувати якийсь переговорний кластер для організації внутрішніх і зовнішніх комунікацій.

Недавно проведені дослідження показали, що, хоча традиційні конференц-зали як і раніше використовуються досить широко, перевага віддається більше гнучкому середовищу, що сприяє більш відкритому й ефективному співробітництву. Це виражається в рості популярності так званих huddle rooms – невеликих кімнат або ізольованих просторів усередині офісу, технічно оснащених для цілей спільної роботи. Експерти Polysom вважають, що надійних рішень для таких завдань із адекватною вартістю на ринку недостатньо, тому компанія випустила ряд націлених на таке застосування новинок: RealPresence Debut і Trio.

Cisco

Головна новинка року від Cisco – сервер Cisco Meeting Server. Він працює з устаткуванням і ПЗ різних виробників, підтримує специфічні для них механізми кодування голосу й відео з якістю до 1080p60 і поєднує в поділюваних робочих просторах різні типи комунікацій – чат, голос, Web-конференції й відео, а також надає кошти для гнучкого керування ними. Якщо в користувача немає спеціального устаткування зв'язку, то сервер дозволяє підключитися до конференцій із браузера з використанням технології WebRTC (без необхідності установки додаткових програмних модулів).

Інші нововведення стосуються термінального встаткування. Cisco змінила дизайн інтерфейсів і розробила нове ПЗ для персональних відеосистем, уніфікувавши його для всієї лінійки продуктів. При цьому «розумні» камери вийшли на новий рівень: до режиму

автоматичного наведення на мовця доданий працюючий паралельно з ним режим виявлення й супроводу лектора.

Компанія реалізувала просте й інтуїтивне керування конференцією прямо із сенсорного пульта (технології ActiveControl). А завдяки новому функціоналові InRoom Control користувачі можуть управляти із цього ж пульта будь-яким стороннім устаткуванням.

ClearOne

Хмарний сервіс Spontania 3.0 дозволяє розгорнути віртуальну переговорну, у якій комфортно переглядати й обговорювати презентації й інші файли, завантажені із пристрою користувачів. Сервіс пропонується як по моделі SaaS, так і по моделі PaaS. У другому випадку замовник одержує свою хмару з необмеженим доступом до таких сервісів, як миттєвий обмін повідомленнями (чат), відеовиклики й спільна робота над документами.

Безкоштовна річна передплата на Spontania надається разом з більшістю ВКЗ-продуктів ClearOne. У їхнє число входить компактний апаратний кодек Collaborate Pro 300 для малих і середніх приміщень, у комплект поставки якого включені камера з 12-кратним зумом і спікерфон. Кодек Collaborate Pro 600 поставляється із двома з'єднаними в ланцюжок мікрофонними масивами й убудованим сервером MCU. У комплекті Collaborate Pro 900 – мікрофонний масив Beamforming з мікшерним пультом Converge DSP. Крім того, даний комплект підтримує запис і віщання відео.

Huawei

Одна із самих цікавих новинок в області ВКЗ – Huawei TE10, компактний термінал з камерою із сенсором 2 Мпікс, розв'язною здатністю 1080p FHD і п'ятикратним оптичним збільшенням. Як відзначають в Huawei, TE10 являє собою пристрій для роботи з корпоративними й хмарними рішеннями ВКЗ; відрізняється адаптивністю, простими налаштуваннями, ефективністю й захищеністю корпоративного класу; позиціонується як рішення для персонального використання або для малих приміщень. Термінал наділений всім необхідним для надання повноцінного функціонала ВКЗ, забезпечує ультраширокий кут огляду камери й ультраширокий сектор захвата звуку.

Термінал TE10 простий у використанні, а на його розгортання, по даним Huawei, потрібно тільки 1 хв. Він важить усього 500 г і має невелике енергоспоживання (8 Вт). Компактність, простота й багатий функціонал дозволяють використовувати термінал TE10 у різних сценаріях, починаючи з організації зручного спілкування для компаній будь-якого розміру до систем телемедицини, дистанційного утворення й ін.

Як відзначають в Huawei, TE10 привносить у лінійку продуктів ВКЗ цієї компанії принципово новий інтерфейс, орієнтований на простоту використання. Такий же інтерфейс має й інша новинка Huawei – груповий термінал TE20, призначений для малих і середніх конференц-кімнат.

Крім того, в Huawei звертають увагу на оновлений персональний термінал для керівника DP300 з 27-дюймовим сенсорним екраном FHD IPS, а також на новий груповий термінал TX50 і камеру VPC800, першого представника ери ВКЗ із розв'язною здатністю 4К.

Grandstream

Представники компанії виділили два групових термінали ВКЗ: GVC3200 і GVC3202. Це рішення на базі Android з убудованим сервером MCU. Модель GVC3200 підтримує до дев'яти учасників відеоконференції (до чотирьох у режимі Full HD), а модель GVC3202 – до трьох учасників HD-відеоконференції (або Full HD у режимі «точка – точка»). На GVC3200 або GVC3202 установлені керовані камери з 12- і 9-кратним оптичним збільшенням відповідно.

Термінали Grandstream підтримують взаємодія по Bluetooth і Wi-Fi. До них підключається до трьох моніторів (вхід VGA/HDMI), можливий запис відеоконференцій. Рішення побудовані на базі SIP-архітектури з підтримкою хмарної платформи IPVideoTalk.

Сервіс аудіо-, відео- і Web-конференцій IPVideoTalk дозволяє організувати трансляцію конференції на 100 учасників. Для участі потрібні тільки ноутбук і Web-браузер.

Logitech

Представники Logitech виділили дві новинки для систем ВКЗ: відеокамери Group і C925E.

Камера Logitech Group призначена для конференц-кімнат: її базових можливостей досить для проведення наради за участю до 14 чоловік в одній кімнаті, а при використанні додаткових виносних мікрофонів – до 20. Завдяки тому, що камера підтримує USB-підключення за технологією Plug-and-Play, для початку сеансу ВКЗ пристрій досить підключити до ноутбука. Logitech Group підтримує запис відео високої чіткості 1080p із частотою 30 кадрів у секунду. Варті уваги також підтримка стиску відео по стандарті H.264 і десятикратний зум. Як затверджують у компанії, камера сумісна з кожним ПЗ для проведення відеоконференцій.

У комплект Logitech Group входять також пульт дистанційного керування й пристрій голосного зв'язку. Останнє підтримує функції луна- і шумозаглушення, що гарантує природну звукопередачу й у той же час зменшує реверберацію й фоновий шум.

Web-камера Logitech C925e також підтримує відео Full HD (1080p) із частотою 30 кадрів у секунду. Поле огляду камери становить 78° – цього досить для її використання невеликими групами або однією людиною. Модель C925e підтримує технологію RightLight 2 і здатна робити інтелектуальне підстроювання для поліпшення якості зображення при недостатнім висвітленні або наявності заднього підсвічування. Камера підключається за принципом Plug-and-Play і сумісна практично з усіма додатками ВКЗ, включаючи Skype for Business, Lync, Cisco Jabber і WebEx.

Polycom

Доступна українським замовникам з 2025 року універсальна система Polycom RealPresence Clariti являє собою повнофункціональну інфраструктуру для спільної роботи, здатну забезпечити висока якість аудіо- і відеозв'язку, обмін контентом, підтримку мобільних користувачів, інтеграцію з Microsoft Lync/Skype for Business і багато чого іншого. Розгортання інфраструктури Clariti може бути здійснене як на базі апаратних серверів Polycom, так і з використанням ПЗ для популярних платформ віртуалізації.

Ряд новинок Polycom випустила для так званих huddle rooms – невеликих кімнат або ізольованих просторів усередині офісу, призначених для спільної роботи. Одна з них – RealPresence Debut. Вона проста як у розгортанні, так і у використанні й, як затверджують у компанії, не має аналогів по співвідношенню якості й ціни. Рішення пропонує HD-відео з високою частотою кадрів, можливість обміну контентом з розв'язною здатністю аж до 1080p, а також оснащено аудіоінноваціями Polycom, включаючи технологію NoiseBlock, що усуває зайві шуми.

Ще одне рішення – RealPresence Trio – являє собою перший інтелектуальний центр, що трансформувалася звичний усім трикутний телефон-жабу для сполучення-конференц-зв'язку в потужну систему для спільної роботи. Рішення підтримує технології придушення шуму, передачі аудіо-, відео- і HD-контенту.

TrueConf

Фахівці компанії відзначають, що останнім часом початку активно розвиватися інтеграція ВКЗ із різним устаткуванням і системами. Тому TrueConf відкрила стороннім розроблювачам доступ до комплекту бібліотек SDK для створення мобільних систем ВКЗ. Оскільки SDK можуть використовувати тільки кваліфіковані фахівці, вирішено було також запропонувати більш простий інструмент для інтеграції відеозв'язку. У результаті з'явилися різні набори інструментів для організації програмувальної взаємодії із продуктами TrueConf через інтерфейси API.

TrueConf планує надати користувачам у переговорних кімнатах такі ж гнучкість і функціональність, які вони звикли бачити на своїх робочих місцях. Для цього розроблений перший безкоштовний програмний ВКЗ-термінал – TrueConf Terminal 2.0. Система встановлюється на ПК під керуванням ОС Windows, а користувач може управляти терміналом з будь-якого пристрою через Web-браузер.

В 2025 році з'явилися повноцінні 3D-камери, які мають два високоякісних сенсори (по 1080р кожний), автофокус, USB-інтерфейс. Одночасно виник і попит на 3D-ВКЗ. Формально розробку 3D-ВКЗ TrueConf не можна вважати новинкою, однак тільки зараз вона стала затребувана: з'явилися перші серйозні проекти, в основному в області телемедицини.

Yealink

Компанія, що представляє в Україні системи вкЗ, Yealink як новинки вказала не тільки окремі продукти, але й інтеграційні рішення.

Перше передбачає інтеграцію різного встаткування (кодеки Yealink, матричні відеоконфутатори Kramer, засобу керування Crestron, AMX) для побудови складних систем для залів сполучення відео-конференц-зв'язку, де потрібні «просунуті» аудіовізуальні засоби й комплексне керування.

Друге рішення представники Yealink характеризують як «усе з однієї коробки». У його состав входять і апаратний сервер, і програмний MCU, і апаратні кодеки в складі стійки з телевізорами. Що важливо: до трьох чвертей у вартості такого рішення доводиться на зроблені в Україні продукти.

Нарешті, третя новинка, що повинна з'явитися до кінця 2025 року, – це двокамерне рішення «усе в одному» без додавання складних елементів. Все керування буде здійснюватися з пульта або конференц-телефону.

Разом з тим ряд компаній указують на збільшення частки персональних відеотерміналів. Воно відбувається головним чином за рахунок програмних клієнтів. «Сьогодні практично в кожному проекті, крім відеотерміналів для переговорних кімнат, передбачаються програмні відеоклієнти для співробітників, – говорить вона. Тенденція така, що кожному співробітникові повинен бути доступний такий сервіс для оперативної роботи».

Якщо замовник готовий купити апаратний кодек, то найчастіше він здобуває саме груповий кодек. Також відзначимо істотний ріст частки «тонкого кодеку», коли замовник замість класичного апаратного кодеку вибирає рішення на базі ПК або неттопа.

Однієї із причин росту попиту на програмні персональні термінали ВКЗ – підвищення якості відеокамер ноутбуків. При цьому підкреслимо, що якісні й недорогі персональні пристрої ВКЗ теж розвиваються й непогано затребувані.

Інфраструктура: апаратна або програмна

Дані свідчать про те, що замовники досить швидко оцінили переваги програмних серверів MCU – в 2025 році їх використовують уже порядку 30% всіх компаній, що мають системи ВКЗ. Але більшість – 55% – поки віддають перевагу апаратним MCU.

Світові тенденції в ІТ, яким треба Cisco, зложилися на користь не просто програмних систем, а програмних систем, що розгортаються на базі розповсюджених рішень віртуалізації (VMware і Microsoft). Віртуалізовані рішення мають масу переваг перед апаратними серверами. Їх простіше обслуговувати, при виході з ладу апаратної частини їх можна перенести в інший ЦОД або відновити з резервної копії практично миттєво, тоді як при поломці апаратного сервера зроблені в нього інвестиції, швидше за все, виявляться загублені. При необхідності нарощування ємності або продуктивності можна просто виділити віртуальній машині більше ресурсів, а у випадку апаратного рішення прийде здобувати новий сервер. Більше того, необов'язково здобувати апаратну платформу у виробника ПЗ – можна використовувати наявну й відповідну ІТ-стандартам підприємства. І це далеко не повний список переваг віртуалізації, містить експерт Cisco.

В ідеальній з погляду Cisco ситуації виконання відеоз'єднання для користувача не повинне нічим відрізнятися від дзвінка по мобільному телефоні

Класичні апаратні пристрої уступають своє місце програмним серверам відео-конференц-зв'язку. Сучасна інфраструктура ВКЗ являє собою не набір «заліза», а комплекс віртуальних машин у ЦОДі.

Софтверизація є важливою тенденцією ринку ВКЗ, а програмні рішення по своїй функціональності вже практично не уступають апаратним. І ми спостерігаємо появу в замовників інтересу до програмних рішень. Правда, з одним важливим застереженням, що

такі рішення здобуваються назавжди – по сценарії «вічного володіння». Але, як показує практика, українські замовники все-таки як і раніше тяжіють до класичних апаратних платформ, а використання програмних інфраструктур, скоріше, доля окремих передових компаній з високим рівнем зрілості ІТ.

На нинішньому етапі розвитку ринку ВКЗ практично вже не важливий тип сервера (програмний або апаратний) – на перше місце виходять питання архітектури системи, вартість підключення одного абонента, наявність підтримки масштабованого кодування відео (SVC). Поява нового стандарту WebRTC з підтримкою SVC змусить багатьох гравців кардинально переглянути політикові ліцензування своїх інфраструктурних рішень. Це здатно зробити революцію, схожу з тої, що викликали програмні рішення.

Модель розгортання: «все своє» або хмари

Дані однозначно свідчать: на українському ринку домінує модель «все своє» – їй віддають перевагу більше 65% замовників.

Для великого бізнесу важливо мати можливість контролю, а також застосовувати специфічні вимоги до зберігання даних, наприклад в області захисту інформації. Хмарні сервіси, як правило безкоштовні (Skype, Viber і інші), використовують переважно дрібні компанії, а також стартапи.

Традиційно переважає модель «все своє», проекти з переходом у хмару можна перерахувати по пальцях однієї руки, і те в половині з них використовуються власні хмари. Зв'язує він це з тим, що часто системи ВКЗ використовуються для обговорення конфіденційних питань, а поки замовники випробовують недовіру до безпеки хмарних технологій.

Перевага моделі «все своє» пояснюється тим, що багато керівників не довіряють хмарам, вважаючи їх небезпечними. При цьому сама СТІ однієї з перші початки пропонувати в Україні хмарну послугу «ВКЗ по запиті». Забезпечується високий рівень захисту хмари, . При цьому враховуються рекомендації виробників і власний досвід в області безпеки.

У нашій країні хмарні сервіси ВКЗ не одержали значимого розвитку, у тому числі й тому, що придбання відповідної інфраструктури затратно для провайдеру, а законодавча база обмежує використання закордонних сервісів.

Проте в Україні чимало й прихильників хмарної моделі. Хто б що не говорив, малий і середній бізнес буде користуватися хмарними рішеннями. Це факт, що відбулось, у Західній Європі й США, до цього все йде й в Україні. Вітчизняні компанії стрімко беруть на озброєння хмарні сервіси.

Малий і середній бізнес як і раніше гостро має потребу в засобах уніфікованих комунікацій. Апаратні системи ВКЗ надають їх, але залишаються дорогими й недоступними для масового користувача, по суті, будучи долею великих корпорацій. На зміну їм поступово приходять більше доступні хмарні сервіси, незаперечним плюсом яких стала можливість підключення до багатоточечному сеансу не тільки групових ВКЗ-кодеків, але й персональних пристроїв: ноутбуків, планшетів і навіть смартфонів.

Багато експертів відзначають ріст інтересу замовників до гібридних моделей, що передбачають масштабування приватної інфраструктури або розширення набору функцій за рахунок хмарних сервісів. Виробники прагнуть відповідати цій тенденції. Так, Polycom із середини 2017 року пропонує в Україні своє гібридне рішення RealPresence Clariti. Популярні сервіси Web-конференцій Cisco WebEx також можуть бути використані для побудови гібридного рішення для масштабування корпоративного сервісу ВКЗ до сотень учасників. До нарад у віртуальних переговорних кімнатах WebEx CMR можуть підключатися учасники з будь-якого зручного для них пристрою: стандартної відеосистеми, ПК, мобільного пристрою, телефону, браузера або програмних клієнтів Lync (Skype for Business).

Поки в порівнянні із загальносвітовими показниками проникнення хмарних сервісів в Україні ще не так значно. Але інтерес до цих сервісів очевидний, і гібридні рішення можуть стати гарним варіантом для багатьох замовників.

Тенденція до зниження вартості систем ВКЗ очевидна. Схеми ліцензування міняються, ціни стають більше демократичними, а ВКЗ – більше доступною.

Мало того, що замовники прагнуть заощаджувати, вони хочуть за менші гроші придбати більше функцій. Як відзначає Владислав Перегудів, на ринку з'явилися нові моделі, які можна віднести до низькобюджетного сегмента, але вони відповідають сучасним вимогам до ВКЗ, а в ряді випадків надають розширені функції. У першу чергу, це рішення «усе в одному», коли, наприклад, у корпус камери вже убудований термінал. Завдяки привабливій ціні й універсальному функціоналові попит на них досить стабільний.

Якщо раніше вартість оснащення переговорної кімнати системою ВКЗ становила мінімум 500 тис. гривень, то зараз вхідний поріг став нижче, починаючись від 150 тис., – далі все залежить від розміру кімнати й переваг замовника. Така ситуація змушує виробників з «великої трійки» (Cisco, Polycom, Huawei) випускати бюджетні термінали.

Змінюються схеми ліцензування, ціни стають більше демократичними, а ВКЗ – більше доступної.

Питання економії знову приводить багатьох до хмар. У період кризи усе більше компаній урізують бюджет на ВКЗ, і найбільш доступним рішенням виявляється послуга SaaS. Вартість рішення Spontania порівнянна з витратами на офісні потреби – від покупок скріпок до заправлення картриджів (та й то на 26 доларів на місяць особливо не розгуляєшся). При цьому замовник одержує можливість проведення нарад і конференцій цілодобово.

Ще одна тенденція – бажання замовників здобувати встаткування в оренду. Причина тому – нестабільна економічна ситуація: клієнти не хочуть вкладати гроші прямо зараз, прагнучи перенести витрати на OPEX. Але така модель продажів становить інтерес не для всіх учасників ринку

У цілому ситуація на українському ринку ВКЗ характеризується появою нових гравців і посиленням конкуренції, що, безумовно, сприяє зниженню цін. Якщо до цього додати підривний ріст числа потенційних терміналів ВКЗ (у першу чергу завдяки росту популярності Skype for Business і розвитку технології WebRTC), то перешкод на шляху масового використання відеозв'язку стає усе менше. Якщо виходити з кількості проданого класичного встаткування ВКЗ, то в результаті може створитися враження, що ринок «просів», але насправді проникнення відео в корпоративне середовище «розширюється» і «заглиблюється». Просто не завжди нові застосування підпадають під класичне поняття ВКЗ.

Давайте розглянемо, як працює технологія WebRTC, використовуючи приклад peer-to-peer виклику на основі браузера:

- користувач відкриває сторінку WebRTC.

- Браузер може запитувати доступ до веб-камери та мікрофона. У цьому випадку користувачеві потрібно надати дозвіл застосунку WebRTC на доступ до своїх пристроїв. Також є випадки, коли цей дозвіл не потрібен, наприклад, під час перегляду прямої трансляції.

- Пакет SDP (Session Description Protocol) генерується в браузері, який ініціює з'єднання. Фактично, це текстовий файл, який містить важливі деталі з'єднання, наприклад, тип медіаданих (аудіо, відео чи контент), кодеки, які параметри підтримуються браузером тощо.

- Залежно від того, як реалізована технологія, ініціатор з'єднання передає цей пакет іншим учасникам. Для цієї мети часто використовується сигнальний сервер та протокол WebSocket.

- На стороні приймача браузер отримує SDP-пакет, а потім генерує аналогічний, який також приймає дані з першого пакета. Другий пакет надсилається назад стороні ініціатора. Тепер обидва клієнти вже певним чином познайомилися один з одним.

- Залежно від його реалізації, стан мережевого з'єднання аналізується разом з попередніми кроками. Клієнтам надається адреса STUN-сервера, яка використовується для визначення зовнішньої IP-адреси пристрою. Потім вона порівнюється з внутрішньою IP-

адресою, щоб визначити, чи використовується NAT для з'єднання, і якщо так, то як маршрутизуються UDP-пакети. У складніших випадках, наприклад, коли використовується подвійний NAT, розробники використовують TURN-сервери. Вони, по суті, є ретрансляторами, що перетворюють P2P-з'єднання на клієнт-сервер-клієнт.

- Після успішного виконання цих кроків з'єднання встановлюється. Подія `onicescandidate` періодично викликається для передачі інформації про IP-адреси, налаштування NAT та спроби з'єднання між клієнтами.

Переваги:

- Встановлення програмного забезпечення не потрібне.
- Високоякісний зв'язок завдяки:
 - o Сучасні відео- та аудіокодеки.
 - o Автоматичне налаштування якості.
 - o Вбудоване придушення луни та шуму.
 - o Автоматичне регулювання підсилення (АПП).

Сильний акцент на безпеці: усі з'єднання захищені та шифруються за протоколами DTLS та SRTP. Водночас WebRTC працює лише за протоколом HTTPS, тоді як вебсайт, що використовує цю технологію, повинен мати підписаний сертифікат.

- Підтримка SVC додана в рамках реалізації кодеків VP9 та AV1. Незважаючи на те, що браузері ще не підтримують SVC, TrueConf дозволяє використовувати SVC у клієнтських браузерах.

- Вбудована функція спільного доступу до робочого столу.
- Інтерфейси керування на основі HTML5 та JavaScript.
- Проєкт з відкритим кодом, який можна вбудувати у ваш продукт або послугу.
- Кросплатформність: WebRTC-додаток однаково добре працює з будь-якою операційною системою – настільною чи мобільною – якщо браузер підтримує WebRTC. Це значно економить ресурси розробки програмного забезпечення.

Недоліки:

- Рішення WebRTC несумісні одне з одним, оскільки стандарт описує лише методи передачі відео- та аудіоданих, дозволяючи розробникам вирішувати питання щодо методів адресації, параметрів відстеження стану, обміну повідомленнями та файлами, планування тощо. Іншими словами, ви не можете здійснювати дзвінки з однієї програми WebRTC до іншої.

- Користувачі, які піклуються про безпеку, будуть розчаровані, дізнавшись, що WebRTC визначає їхні справжні IP-адреси. Водночас ні проксі, ні мережа Tor не допоможуть зберегти анонімність. Ви можете приховати свою IP-адресу за допомогою різних VPN-сервісів та сервера TURN. За потреби WebRTC можна вимкнути.

- WebRTC не підтримує керування віддаленим робочим столом. Звичайно, ви можете транслювати те, що відбувається на екрані вашого пристрою, але це односторонній відеопотік, як зображення, що передається з камери, при цьому немає можливості взаємодіяти з джерелом потоку. Це зроблено з міркувань безпеки: код Javascript не може керувати нічим поза межами поточного вікна браузера. Ви можете отримати більше функцій, включаючи керування віддаленим робочим столом, використовуючи клієнтські програми, налаштовані постачальниками відеоконференцій.

Кодеки WebRTC

Кодеки WebRTC можна розділити на обов'язкові (браузері, що реалізують цю технологію, повинні підтримувати ці кодеки) та додаткові (нестандартні, хоча деякі браузери їх підтримують).

Аудіокодеки

Для стиснення аудіотрафіку WebRTC використовує обов'язкові (Opus та G.711) та додаткові кодеки (G.722, iLBC, iSAC).

Opus – це аудіокодек з низькою затримкою (від 2,5 мс до 60 мс), підтримкою змінного бітрейту та високим рівнем стиснення, що ідеально підходить для потокової передачі аудіо в

мережах зі змінною пропускною здатністю. Opus – основний аудіокодек для WebRTC. Це гібридне рішення, яке поєднує найкращі можливості кодеків SILK (стиснення голосу та покращення людської мови) та CELT (кодування аудіо). Кодек є відкритим та повністю безкоштовним. Безсумнівно, Opus перевершує інші аудіокодеки за багатьма параметрами. За кількістю параметрів він перевершує досить популярні кодеки з низьким бітрейтом, такі як MP3, Vorbis та AAC LC. Порівняно з AMR-WB та Speex, Opus відновлює аудіоструктуру, яка є найближчою до оригіналу.

G.711 – це застарілий високошвидкісний (64 кбіт/с) мовний кодек, розроблений для використання в традиційних VoIP-системах. Головною перевагою є мінімальне обчислювальне навантаження завдяки легким алгоритмам стиснення. Кодек має низький рівень стиснення аудіосигналів і не збільшує затримку аудіо під час зв'язку між користувачами.

G.711 підтримується багатьма пристроями. Системи, що використовують цей кодек, простіші у використанні, ніж ті, що базуються на інших аудіокодеках, таких як G.723, G.726, G.728 тощо. Що стосується якості, G.711 отримав 4,2 бала в тестуванні MOS (бал 4–5 є найвищим і означає хорошу якість, подібну до якості голосового трафіку в ISDN і навіть вищу).

G.722 – це стандарт ITU-T, прийнятий у 1988 році, який не вимагає сплати роялті. Він може працювати зі швидкістю 48, 56 та 64 кбіт/с, забезпечуючи якість звуку, еквівалентну G.711. Подібно до G.711, він є застарілим, але все ще підтримується Chrome, Safari та Firefox.

iLBC (інтернет-кодек з низьким бітрейтом) – це вузькосмуговий мовний кодек з відкритим кодом, що підтримується Chrome та Safari. Через високий рівень стиснення потоку цей кодек збільшує навантаження на процесор.

iSAC (інтернет-звуковий кодек для мовлення) – це раніше власний широкосмуговий аудіокодек для мовлення, який тепер є частиною проекту WebRTC. Однак він не є обов'язковим, але підтримується Chrome та Safari. У випадку WebRTC він використовує адаптивний бітрейт від 10 до 52 кбіт/с із частотою дискретизації 32 кГц.

Відеокодеки

Який відеокодек обрати для WebRTC? Розробникам довелося думати над цим кілька років, і відповідь – VP8 та H.264. Також є додаткові відеокодеки (H.265, VP9 та AV1).

VP8 – це безкоштовний відкритий відеокодек, що характеризується високою швидкістю декодування відео та покращеною стійкістю до втрати кадрів. Кодек багатофункціональний: його легко інтегрувати в апаратні платформи, тому постачальники послуг відеоконференцій часто використовують його у своїх продуктах. Він сумісний з Chrome, Edge, Firefox та Safari (12.1+).

Платний відеокодек H.264 став відомий набагато раніше за свого аналога. Цей кодек пропонує високий коефіцієнт стиснення відеопотоків, зберігаючи при цьому високу якість відео. Широко використовується в апаратних системах відеоконференцій, він ідеально підходить для WebRTC. Він сумісний з Chrome (52+), Edge, Firefox (більше не підтримується у версіях 68+ для Android) та Safari.

VP9 – це відкритий та безкоштовний стандарт стиснення відео, розроблений Google у 2012 році. Згодом розширений в рамках AV1It, він є результатом ідей, що лежать в основі VP8. Цей кодек сумісний з Chrome (48+) та Firefox.

H.265 – це платний відеокодек, який розглядається як наступник H.264 та забезпечує таку ж візуальну якість при вдвічі меншому бітрейті. Це можливо завдяки ефективнішим алгоритмам стиснення. Наразі цей кодек конкурує з безкоштовним AV1.

AV1 – це кодек стиснення відео з відкритим кодом, спеціально розроблений для передачі відео через Інтернет. Він підтримується Chrome (70+) та Firefox (67+).

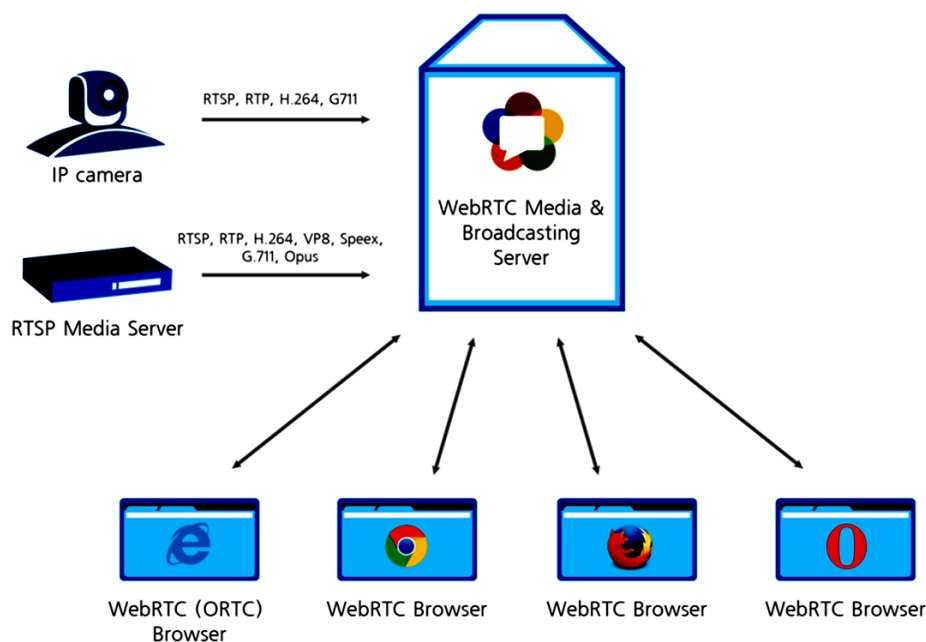


Рисунок 1 – Структурна схема системи

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів клієнта ВКЗ за допомогою технології WebRTC. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем клієнта ВКЗ за допомогою технології WebRTC.
- Досліджена система клієнта ВКЗ за допомогою технології WebRTC.
- На основі отриманих результатів досліджень створена програмна реалізація системи клієнта ВКЗ за допомогою технології WebRTC. Розроблені алгоритми дозволяють успішно вирішувати завдання клієнта ВКЗ за допомогою технології WebRTC. 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. 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,
6. 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.
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 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.
 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., 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. Дресв, 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.

УДК 004

Л.Буханенко, магістр гр. КІ-24М,
 Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ МЕРЕЖЕВОЇ БЕЗПЕКИ ПОБУДОВАНОЇ НА ОСНОВІ РІШЕНЬ AXIS

У статті розроблено програмне забезпечення, яке призначено для системи мережевої безпеки побудованої на основі рішень Axis. Метою розробки є дослідження та принципи побудови системи мережевої безпеки побудованої на основі рішень Axis. Об'єктом дослідження є процес мережевої безпеки побудованої на основі рішень Axis. Предметом дослідження є методи мережевої безпеки побудованої на основі рішень Axis. Методи дослідження базуються на методах захисту інформації у комп'ютерній мережі, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи мережевої безпеки побудованої на основі рішень Axis. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

мережева безпека, Axis

Постановка проблеми. Axis пропонує низку комплексних рішень для відеоспостереження, які працюватимуть для вас сьогодні та завтра, дозволяючи вам бути спокійними. Захистіть себе від зловмисників, проникнення зі зломом, вандалізму чи будь-чого іншого, що може статися, завдяки рішенням для відеоспостереження Axis. Незалежно від потреб вашого бізнесу, ваше життя стане набагато простішим завдяки кільком розумним способам.

Комплексні рішення – це комплексні системи безпеки, адаптовані та перевірені відповідно до ваших конкретних потреб. Axis може запропонувати все: від системи керування відео Axis, такої як Axis Companion або Axis Camera Station, до всіх підключених пристроїв. Кожне рішення буде індивідуальним для потреб бізнесу та може варіюватися від однієї камери на вході до сотні камер та інших пристроїв безпеки, які стежать за кожним сантиметром вашого приміщення.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи мережевої безпеки побудованої на основі рішень axis.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи мережевої безпеки побудованої на основі рішень Axis.

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

- Огляд існуючих систем мережевої безпеки побудованої на основі рішень Axis.
- Дослідження системи мережевої безпеки побудованої на основі рішень Axis.
- Програмна реалізація системи мережевої безпеки побудованої на основі рішень

Axis.

Об'єктом дослідження є процес мережевої безпеки побудованої на основі рішень Axis.

Предметом дослідження є методи мережевої безпеки побудованої на основі рішень Axis.

Методи дослідження базуються на методах захисту інформації у комп'ютерній мережі, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Axis пропонує інструмент Designer, який спростить проектування вашого комплексного рішення для відеоспостереження. Він також надасть вам корисну документацію з встановлення та можливість експортувати конфігурації, щоб уникнути помилок під час встановлення. Цей інтуїтивно зрозумілий інструмент спрощує робочий процес проектування та складання кошторисів, роблячи проекти швидшими та простішими для створення, редагування або впровадження.

Лінійка відеореєстраторів Axis – це чудовий спосіб розпочати створення комплексного рішення. Це готові до використання рішення, які забезпечують надійне відеоспостереження високої чіткості. Попередньо завантажені всім необхідним програмним забезпеченням і ліцензіями для вашої системи, ці рішення для запису можуть задовольнити вимоги широкого кола бізнес-потреб і галузей. Якщо вам потрібне безпечне та надійне відеоспостереження, це ідеальне рішення для вас.

Axis Companion – це просте та зручне програмне забезпечення для керування відео, яке інтегрується з камерами, домофонами та аудіопродукцією Axis. Це ідеальний вибір для підприємств з невеликими об'єктами, яким потрібна проста у використанні система, наприклад, роздрібні магазини.

Axis Camera Station – це потужна та проста у використанні, повнофункціональна система керування відео, яка легко інтегрується з іншими продуктами Axis. Пропонує повну, гнучку, безпечну та надійну систему, що ідеально підходить для великих підприємств, таких як школи, роздрібна торгівля та виробництво.

Купуючи комплект для відеоспостереження, легко зосередитися на кількості камер або роздільній здатності. Але у 2025 році розумний захист означає глибший пошук, особливо якщо вам потрібна надійність, швидкість та моніторинг без використання рук. Ось що дійсно важливо.

Роздільна здатність та якість камери

Розумна система відеоспостереження повинна забезпечувати більше, ніж просто HD. У 2025 році базовим стандартом буде 4K. Звертайте увагу на широкий динамічний діапазон, гібридний зум та кольорове нічне бачення, щоб чітко фіксувати обличчя, номерні знаки та критичні події в режимі реального часу.

Кількість каналів

Масштабованість має значення. Система відеоспостереження NVR з 8 або 16 каналами дозволяє розширити покриття пізніше – ідеально підходить для зростаючих домогосподарств або підприємств зі складними периметрами.

Місткість та можливості розширення

Найкраща система безпеки NVR повинна пропонувати щонайменше 2 ТБ локального сховища, бажано з можливістю розширення до 16 ТБ. Завдяки цілодобовому запису та відео високої роздільної здатності ємність швидко вичерпується. Локальне сховище також зменшує залежність від хмари.

Інтеграція мобільних додатків та віддалений перегляд

Кожна система з цього списку підтримує інтеграцію з мобільними додатками. Ви отримуватимете миттєві сповіщення, історію подій та прямі трансляції безпосередньо на свій телефон – з будь-якого місця. Бонусні бали за системи з графічним інтерфейсом на основі браузера та без абонентської плати.

Виявлення руху та сповіщення штучного інтелекту

Розумний штучний інтелект допомагає фільтрувати рух – не кожна тінь чи гілка повинна спрацьовувати тривога. Сучасні системи виявляють людей, домашніх тварин та транспортні засоби, а деякі пропонують сповіщення на основі облич або розпізнавання незнайомих для більшої точності.

Нічне бачення та розумне ІЧ-підсвічування

Інфрачервоне підсвічування входить до стандартної комплектації. Чудовою системою є кольорове нічне бачення, інтелектуальна адаптація ІЧ-підсвічування та система

відлякування на основі прожектора. Чітке нічне відео означає, що ви не пропустите те, що відбувається після настання темряви.

Розумний пошук відео

Одним з найбільших проривів 2025 року є пошук відео на основі штучного інтелекту. Фільтрація за обличчям, об'єктом, рухом, часом або навіть певними зонами. Це скорочує час розгляду інциденту з годин до хвилин.

PoE проти бездротової інфраструктури

Системи відеоспостереження PoE NVR забезпечують швидкість та надійність завдяки одному кабелю. Бездротові комплекти пропонують гнучке розміщення, але можуть страждати від перешкод або перебоїв з'єднання. Оберіть PoE для критично важливих установок, Wi-Fi для гнучкості.

Локальне та хмарне сховище

Багато систем пропонують обидва варіанти. Деякі забезпечують гібридне сховище з кліпами подій у хмарі та повними записами локально. Ми ж віддаємо перевагу системам з локальним сховищем насамперед – для швидкості, конфіденційності та доступу офлайн.

Штучний інтелект та відстеження Cross-Cam

Високоякісні системи відеоспостереження NVR тепер включають крос-камерний штучний інтелект, що дозволяє відстежувати один об'єкт від камери до камери. Це революційно впливає на периметри бізнесу та об'єкти з широким кутом огляду.

Налаштування та екосистема програм

Простота налаштування має значення. Підключення через PoE або бездротове з'єднання за принципом «підключи та працюй», зрозумілі інтерфейси додатків, інтелектуальне керування зонами та швидке оновлення прошивки – все це додає довгострокової цінності.

Співвідношення ціни та якості

Зрештою, комплект відеокамери має окупати інвестиції. Важлива не лише початкова вартість, а й те, як довго він служить, наскільки добре захищає та наскільки ним легко користуватися.

Програмне забезпечення мережевої безпеки побудованої на основі рішень Axis – це програмна платформа для керування, моніторингу та обслуговування рішень для відеоспостереження на основі мережевих камер та IP-пристроїв Axis. Зручність для системних інтеграторів та клієнтів лежить в основі програмного забезпечення мережевої безпеки побудованої на основі рішень Axis: воно проста в установці, просте у використанні та спрощує обслуговування комплексного рішення для відеоспостереження. Регулярний потік удосконалень означає, що програмне забезпечення мережевої безпеки побудованої на основі рішень Axis йде в ногу з інноваціями в технологіях, як у самому програмному забезпеченні для керування відео, так і у зв'язку зі зростанням кількості та типу пристроїв, підключених до систем спостереження.

Програмне забезпечення мережевої безпеки побудованої на основі рішень Axis забезпечує основу для створення перевіреного комплексного рішення на основі технологій Axis. Воно ідеально відповідає повному портфолію IP-продуктів та функцій Axis, пропонуючи клієнтам повну, гнучку та надійну систему. Програмне забезпечення мережевої безпеки побудованої на основі рішень Axis легко встановлюється, а завдяки своєму інтуїтивно зрозумілому інтерфейсу користувача вона проста у використанні.

Програмне забезпечення для керування відео на основі рішень Axis є основою комплексного рішення Axis. Комплексне рішення складається з:

- Клієнтське та серверне програмне забезпечення: обробляє весь зв'язок з камерами та допоміжними пристроями в системі, керує правами користувачів та забезпечує взаємодію з відео в реальному часі та записаними відео, а також керування системою, функції обслуговування та журнали.

- Безпечний вхід: вбудований у програмне забезпечення Програмне забезпечення мережевої безпеки побудованої на основі рішень Axis та забезпечує функції контролю доступу при додаванні контролерів дверей AXIS A1601
- Мережеві відеореєстратори: прості в установці та надійні рішення для запису, ідеально адаптовані до широкого спектру мережевих продуктів Axis
- Мобільний додаток для перегляду: забезпечує дистанційний перегляд відео та записів у реальному часі, а також живий зв'язок з відвідувачами та керування дверима на мобільних пристроях
- Підтримка повного портфоліо IP-підключених продуктів Axis, включаючи відеокамери, натільні камери, аудіопристрої, домофони та контролери дверей, радары
- Доступ до потужних аналітичних програм для покращення рішення для відеоспостереження, включаючи AXIS License Plate Verifier, AXIS Guard Suite, AXIS Perimeter Defender, AXIS Object Analytics та інші.

Для системних інтеграторів пакет Програмне забезпечення мережевої безпеки побудованої на основі рішень Axis Integrator Suite – це набір інструментів, які допомагають інтеграторам проектувати, розгортати та обслуговувати рішення Програмне забезпечення мережевої безпеки побудованої на основі рішень Axis, і включає AXIS Site Designer, AXIS Installation Verifier та Програмне забезпечення мережевої безпеки побудованої на основі рішень Axis System Health Monitoring.

У широкому сенсі, можливості програмного забезпечення мережевої безпеки побудованої на основі рішень Axis стосуються перегляду відео в реальному часі, відтворення та пошуку відео, аудіо, контролю доступу, а також управління системами та користувачами.

Перегляд відео в реальному часі

Програмне забезпечення мережевої безпеки побудованої на основі рішень Axis дозволяє створювати налаштований робочий простір з миттєвим доступом до зображень і камер у системі, а також інтеграцією планів поверхів і зовнішніх веб-сторінок. Ключовим фактором є максимальна гнучкість, що відповідає потребам будь-якого оператора. Підтримка кількох моніторів (наприклад, для поєднання перегляду в реальному часі та записаного зображення), визначені користувачем кнопки дій і програмовані гарячі клавіші вбудовані як стандартні функції. Також у стандартну комплектацію входять інтерактивні карти, екранні елементи керування для функцій камер, таких як керування склоочисниками PTZ-камери, і профілі відеопотоку, вибрані оператором.

Щоб забезпечити перегляд відео найвищої якості, програмне забезпечення мережевої безпеки побудованої на основі рішень Axis дозволяє одночасно синхронізувати відео в реальному часі з різних серверів та/або сайтів, а також, за наявності відповідного клієнта та дисплея, підтримує камери високої роздільної здатності UltraHD 4K для чіткої ідентифікації інцидентів.

Кілька функцій, зокрема виправлення спотворень на 360 градусів, формат коридору Axis та багатосенсорне зшивання зображень, забезпечують повний огляд без сліпих зон. Оператори можуть визначати цифрові попередньо встановлені позиції зон інтересу, гнучко налаштовувати зображення, поєднуючи карти, веб-сторінки, камери тощо, а також створювати віртуальні обходи охоронців для автоматичного огляду будь-якої ділянки.

Сигналізація та сповіщення можуть бути налаштовані таким чином, щоб негайно привертати увагу операторів до певних сцен і автоматично запускати відеозапис і аудіооголошення. Сповіщення можна надсилати в мобільний додаток Програмне забезпечення мережевої безпеки побудованої на основі рішень Axis, що дозволяє операторам реагувати на інциденти та розслідувати їх у режимі реального часу, а також вживати необхідних заходів з будь-якого місця.

Покращене відтворення та пошук

Програмне забезпечення мережевої безпеки побудованої на основі рішень Axis також надає багатий функціонал для відтворення відео. Це включає синхронізоване, одночасне відтворення з кількох камер та різних серверів, а також перемикання відео, швидке

відтворення та покадровий перехід, що дозволяє операторам швидко та точно знаходити ділянки відео, що мають певний інтерес.

Це ще більше покращується завдяки функції Smart Search 2, яка дозволяє операторам швидко шукати у відеоматеріалах людей та транспортні засоби, що цікавлять їх. Smart Search 2 працює на основі даних про рух об'єктів з камери Axis, які можна додатково обробляти за допомогою методів машинного та глибокого навчання для швидкої класифікації об'єктів, таких як люди, автомобілі, вантажівки та велосипеди.

Окремі розділи відео, що становлять особливий інтерес, можна анотувати за допомогою закладок, коментарів і нотаток, а також експортувати для сприяння розслідуванню та побудові справ. Справи можна упакувати в захищену паролем zip-папку, а випадки спостереження можна ділитися з іншими завдяки вбудованому файловому плеєру, що полегшує одержувачу перегляд результатів.

Для захисту конфіденційності третіх осіб, знятих на відеоматеріалах, у Програмне забезпечення мережевої безпеки побудованої на основі рішень Axis передбачено редагування відео, яке пропонує можливості маскувати людей та об'єкти на відео перед експортом.

Підтримка мережевого аудіо Axis

Програмне забезпечення мережевої безпеки побудованої на основі рішень Axis дозволяє керувати всім портфоліо IP-продуктів Axis, яке включає зростаючу кількість мережевих аудіопристроїв. Підтримуються як аудіовхід, так і аудіовихід: мікрофони, підключені до камер, дозволяють операторам прослуховувати живі сцени, а також забезпечувати аудіозаписи, тоді як живі розмови та попередньо записані повідомлення можна відтворювати або запускати через мережеві динаміки, що дозволяє оператору проактивно запобігати небажаний поведінці, а також звертатися до людей на об'єкті.

AXIS Cameras Station має інтуїтивно зрозуміле керування звуком з можливістю регулювання гучності або вимкнення вхідного звуку. Оператори можуть прослуховувати кілька джерел звуку та керувати підключеними динаміками для забезпечення живого спілкування.

Для камер Axis із вбудованими динаміками та динаміками Axis функція «натисни і говори» дозволяє операторам отримувати аудіо та надає можливість спілкуватися в режимі реального часу. Після ввімкнення динаміка для будь-якої камери в режимі реального часу відображається кнопка голосового зв'язку.

Інтегрований контроль доступу

Функція контролю доступу вмикається в AXIS Cameras Station після додавання контролерів дверей AXIS A1601. Завдяки зручному інтерфейсу Програмне забезпечення мережевої безпеки побудованої на основі рішень Axis оператори можуть легко налаштовувати контролери дверей та керувати власниками карток.

Об'єднання відео та контролю доступу дозволяє перевірити вхід за допомогою відео та миттєво надсилати тривоги контролю доступу співробітникам системи спостереження. Це також спрощує розслідування, дозволяючи шукати події контролю доступу за допомогою синхронізованого відео.

Налаштування автоматизованих ланцюжків дій

Програмне забезпечення мережевої безпеки побудованої на основі рішень Axis має потужний та простий у використанні механізм правил дій. Оператори можуть вибирати з різних тригерів та дій, що дозволяє налаштовувати автоматизовані дії. Автоматизовані ланцюжки дій допомагають у багатьох відношеннях, розвантажуючи оператора від виснажливої роботи перед екраном, дозволяючи йому проактивно втручатися лише за потреби.

Його також можна використовувати для покращення спостереження та загальної ефективності бізнесу. Наприклад, активація розтяжки від AXIS Fence Guard може ініціювати запис з кількох камер, перемістити PTZ-камеру в певне попередньо встановлене положення, а також потенційно ініціювати аудіоповідомлення на динаміку, вихід для ввімкнення освітлення та сповіщення оператора.

Управління системою та користувачами

За допомогою Програмне забезпечення мережевої безпеки побудованої на основі рішень Axis можна легко керувати камерами та підключеними IP-пристроями у великих системах та на кількох об'єктах, а також обліковими даними операторів, яким потрібно використовувати та керувати системою. Microsoft Active Directory можна використовувати для полегшення адміністрування користувачів, груп та прав доступу до пристроїв.

Клієнти можуть підключатися до кількох серверів одночасно, щоб отримати повний огляд системи, незалежно від того, чи знаходиться вона на одному чи кількох сайтах. Адміністратори можуть підключатися до кількох сайтів/серверів та налаштовувати параметри будь-якого пристрою, підключеного до системи, включаючи оновлення прошивки пристрою.

Axis Secure Remote Access спрощує доступ до віддалених систем спостереження, усуваючи необхідність ручного переадресації портів та налаштування маршрутизатора. Технологія використовує кілька рівнів автентифікації для встановлення безпечного, зашифрованого зв'язку між клієнтом та системою спостереження.

Програмне забезпечення мережевої безпеки побудованої на основі рішень Axis також підтримує покращений захист пристроїв, автоматично генеруючи безпечний випадковий пароль максимальної довжини, що підтримується вибраним(и) пристроєм(ами).

Систему можна масштабувати та підвищувати продуктивність, додаючи більше серверів для підтримки більшої кількості підключених пристроїв та збільшення вимог до сховища.

Крім того, можна використовувати кілька підходів до оптимізації сховища. До них належать керування бітрейтом за допомогою Zipstream, AXIS Average Bitrate – складний метод контролю бітрейту за допомогою стиснення відео, адаптований для забезпечення постійного виконання вимог щодо часу зберігання, – та визначення часу зберігання відео для кожної окремої камери.

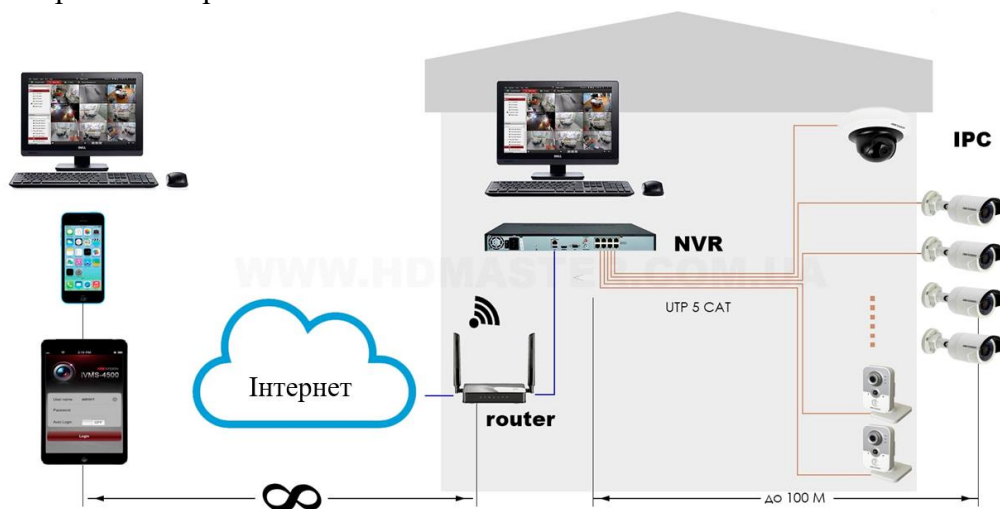


Рисунок 1 – Структурна схема системи

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів мережевої безпеки побудованої на основі рішень Axis. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем мережевої безпеки побудованої на основі рішень Axis.
- Досліджена система мережевої безпеки побудованої на основі рішень Axis.
- На основі отриманих результатів досліджень створена програмна реалізація системи мережевої безпеки побудованої на основі рішень Axis. Розроблені алгоритми дозволяють успішно вирішувати завдання мережевої безпеки побудованої на основі рішень Axis. 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., 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.
2. 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.
3. 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.
4. 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,
5. Smirnov O., Smirnova T., Anas M. Al-Oraiqat, Drieiev O., Polishchuk L., Sherov 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.
6. 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>
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., 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.
10. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
11. 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.
12. 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.
13. 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.
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., 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., Gorbacheva, L., Babenko, V., «Hiding data in images using a pseudo-random sequence», CEUR Workshop Proceedings Volume 2608, 2020, Pages 646-660.
19. 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.
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., 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., 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. 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.
29. Т.В. Смірнова, О.М. Дресєв, 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.
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. 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.
32. Смірнов О.А., Дресєва Г.М., Дресєв О.М., Смірнова Т.В. «Фрактальний аналіз генератора самоподібного трафіку на основі ланцюга Маркова». Центральньоукраїнський науковий вісник. Технічні науки. № 2(33). с. 161-172, 2019.

УДК 004

К.Василенко, магістр гр. КІ-24М,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У МЕРЕЖЕВИХ CLOUD-СИСТЕМАХ

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

захист персональних даних, Cloud-система

Постановка проблеми. Стандартизація необхідна для ефективного функціонування будь-якої галузі, і ринок хмарних послуг не є виключенням. Його повноцінний розвиток неможливо без стандартів захисту інформації, переносимості даних і додатків, оцінки рівня надаваного сервісу й т.д. Причому їхній вплив може бути настільки ж великий, як і законодавчих вимог і норм. Проте забезпечення належної відповідності їм, а також сертифікація залишаються комерційною справою кожного провайдеру, якщо немає відповідної вимоги регулятора. Ключову роль у прийнятті необхідних стандартів і розвитку ринку може грати уряд – потенційно найбільш великий споживач хмарних сервісів. Підтримка хмарних обчислень припускає прийняття безлічі різних стандартів, що – з урахуванням наявності десятків органів по стандартизації – чревате їхньою фрагментарністю, непогодженістю й взаємним дублюванням. У свій час Європейська комісія навіть виразила заклопотаність із цього приводу, назвавши «мішанину стандартів» головною перешкодою на шляху переходу до хмар, що гальмує розвиток ринку. Найбільше побоювання викликало те, що галузь не зможе прийти до згоди відносно інтероперабельності сервісів і переносимості даних. Кожний великий гравець прагне до домінування на ринку, а тому, на думку комісії, не зацікавлений у стандартизації. У результаті замовники можуть виявитися прив'язаними до конкретного провайдеру, не маючи можливості його переміняти. Крім того, комісія виразила тривогу із приводу відсутності стандартів для забезпечення безпеки даних, відповідно до яких можна було б сертифікувати провайдерів хмарних послуг, їхню інфраструктуру й сервіси, що дозволило б гарантувати схоронність користувальницьких даних і допомогло галузі розвиватися.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи захисту персональних даних у мережеских cloud-системах.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи захисту персональних даних у мережеских Cloud-системах.

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

- Огляд існуючих систем захисту персональних даних у мережеских Cloud-системах.

- Дослідження системи захисту персональних даних у мережевих Cloud-системах.
- Програмна реалізація системи захисту персональних даних у мережевих Cloud-системах.

Об'єктом дослідження є процес захисту персональних даних у мережевих Cloud-системах.

Предметом дослідження є методи захисту персональних даних у мережевих Cloud-системах.

Методи дослідження базуються на методах захисту інформації у мережі, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Релевантними для провайдерів стандартами ISO із групи 27000 є ISO 27002 на методи й засоби інформаційної безпеки й ISO 27005 на керування ризиками в області інформаційної безпеки. У першому більш докладно розглядаються засоби керування, що перераховуються в додатку до ISO 27001. Обидва стандарти (27002 і 27005) є рекомендаційними, сертифікація на відповідність їм не передбачається. Проте провайдер може замовити незалежну оцінку, щоб перевірити, якою мірою дотримуються запропоновані рекомендації. Деякі замовники запитують таку оцінку замість сертифікації по 27001. Всі три стандарти не є специфічними для провайдерів. Тим часом улітку 2014 року ISO опублікувала стандарт ISO 27018:2015 про захист персональних даних у хмарі, а наприкінці 2015 року – ISO 27017:2015 про засоби контролю інформаційної безпеки для хмарних рішень.

В ISO 27017 передбачаються додаткові елементи безпеки для хмари, відсутні в ISO 27002. Повна офіційна назва цього стандарту: «Звід правил для засобів керування інформаційною безпекою на базі ISO/IEC 27002 для хмарних сервісів» («Code of practice for information security controls based on ISO/IEC 27002 for cloud services»). Незважаючи на те що його фінальна редакція була опублікована лише 30 листопада 2015 року, Amazon Web Services уже має відповідний сертифікат, отриманий ще в жовтні 2015-го. Тим часом, будучи доповненням до ISO 27002, новий стандарт не припускає сертифікації, однак через його популярність багато органів сертифікації планують це робити: імовірно, будуть видавати «свідчення про відповідність». У всякому разі, на дане питання ще немає ясної відповіді.

Конкретні рекомендації стосовно до хмарних сервісів даються до 37 з більш ніж сотні засобів керування безпекою, які визначені в ISO 27002. Вони адресовані не тільки провайдерам хмарних послуг, але й замовникам, чим підкреслюється їхня взаємна відповідальність за безпеку сервісів: замовник повинен розробити політику використання хмарних сервісів, а провайдер – надати йому необхідну інформацію. Найбільші зміни стосуються розділу, присвяченого контролю доступу: розглядаються реєстрація й вихід користувача, надання доступу, керування привілейованим доступом, обмеження доступу до інформації й використання привілейованих службових програм. Крім того, вводяться сім нових елементів керування:

- загальні ролі й відповідальність у хмарному середовищі;
- видалення й повернення активів клієнта хмарних сервісів;
- сегрегація у віртуальних обчислювальних середовищах;
- посилення віртуальних машин;
- операційна безпека адміністратора;
- моніторинг хмарних сервісів;
- узгодження керування безпекою для віртуальних і фізичних середовищ.

Звичайно, це далеко не всі стандарти, навіть якщо обмежитися тільки інформаційною безпекою. Чим їх більше, тим суужніше в них розібратися. Як би те не було, ISO 27001 представляється найкращим базовим стандартом для всіх компаній, що бажають захистити свою інформацію (і єдиним із серії стандартів інформаційної безпеки ISO, на який видається реальний сертифікат). Залишаючи осторонь питання про захист персональних даних (ISO 27018 і/або 152-ФЗ), можна сказати, що реалізований постачальником хмарних послуг комплекс рекомендацій ISO 20001 і 20017 є необхідним «джентльменським набором» в

області інформаційної безпеки, якщо провайдер хоче розсіяти сумніву замовника в безпеці хмарних сервісів.

Однак, як впливає з ISO 20017, навіть проходження провайдером його рекомендаціям не знімає відповідальності із клієнта, що повинен виконати свою частину домашнього завдання й також ретельно дотримуватися рекомендацій стандарту. Наприклад, відповідно до вимог контролю доступу A.9.4.1, він повинен обмежити доступ до інформації в хмарі у відповідності зі своєю корпоративною політикою.

Стандарти можуть робити настільки ж значний вплив на ринкову ситуацію, як і введення законодавчих вимог і норм. Проте при відсутності офіційних вимог забезпечення відповідності тим або іншим стандартам, а також сертифікація – це комерційна справа кожного провайдеру. У більшості країн діяльність хмарних провайдерів державою ніяк спеціальним образом не регулюється. Донедавна в жодній країні миру не було окремих законів, присвячених хмарам. Торік першопрохідником на цьому шляху стала Південна Корея.

До кінця 2017 року були прийняті необхідні правові акти по врегулюванню використання хмарних технологій при здійсненні державного керування. Однак на даний момент спеціальні нормативно-правові акти, де б установлювалися правила надання хмарних послуг, відсутні. Проте в Україні дуже багато законів, у яких і до замовників, і до постачальників послуг пред'являються досить специфічні й детальні вимоги. Головні з них – Цивільний кодекс (ГК), а також закони про інформацію й персональні дані.

Основні обмеження в частині обробки інформації стосуються персональних даних (ПДн). З юридичної точки зору у відносинах, що формуються у зв'язку з використанням хмарних послуг, беруть участь три сторони: суб'єкти даних, замовники й провайдери, – причому замовник є також оператором даних для тих суб'єктів даних, інформацію про які він збирає й потім передає в хмару. При буквальному читанні закону про персональні дані провайдер може класифікуватися як оператор ПДн залежно від обсягу надаваної хмарної послуги. У такому випадку виникає необхідність відповісти величезній кількості критеріїв, у числі яких – реєстрація в спеціальному реєстрі регулятора й відповідальність перед суб'єктом персональних даних, що перебувають у хмарі, що збільшує навантаження на провайдеру і його витрати.

Щоб уникнути цієї ситуації радимо провайдерам скористатися особливим режимом обробки даних – обробкою з доручення. Він рятує від необхідності діставати згоду на обробку ПДн у суб'єктів і дозволяє уникнути відповідальності безпосередньо перед ними: відносини провайдеру із приводу дотримання законодавства про ПДн будуть обмежені його контрактом із замовником – розбиратися з тими або іншими претензіями конкретних суб'єктів даних буде сам замовник, він же оператор даних. Для цього в договорі із провайдером повинні бути прописані наступні умови:

- перелік дій по обробці ПДн, які будуть відбуватися провайдером, а також мети обробки;
- зобов'язання провайдеру дотримувати конфіденційності ПДн і забезпечити їхню безпеку в ході обробки;
- перелік вимог до провайдеру по захисту оброблюваних ПДн.

При відсутності в договорі цих умов провайдер ризикує порушити безліч статей закону про ПДн, а при їхній наявності він хоча й звільняється від безпосередньої відповідальності перед суб'єктом даних, але відповідає за недотримання передбачених договором заходів щодо захисту ПДн.

Багато питань викликало вимогу закону про локалізацію, що вказує на те, що персональні дані українських громадян повинні оброблятися з використанням баз даних, що перебувають в Україні, і – згідно «твердому трактуванню» – винятково на вітчизняних серверах. Однак у підсумку вибрали більше м'який варіант: обробка даних українських громадян можлива й на закордонних серверах, якщо ці дані втримуються також у базах даних, розташованих на території України, при цьому не допускається наявності за межами

країни Пдн, які відсутні в українській базі даних. Як відзначає Микола Феоктистов, дане роз'яснення не відповідає на цілий ряд питань, наприклад: якщо нові дані створюються за рубежем і вони доступні користувачеві в Україні, те чи належні вони відразу реплікуватися в українську базу даних і яка відповідальність провайдеру в той період часу, поки ця реплікація відбувається?

Послуги хмарних обчислень – послуги з надання обчислювальних потужностей, включаючи технічні засоби й права використання програм для електронних обчислювальних машин з метою обробки й зберігання інформації органів державної влади, органів місцевого самоврядування, органів керування державними позабюджетними фондами з використанням технічних засобів, взаємодіючих через інформаційно-телекомунікаційні мережі.

Фактично в цьому визначенні хмарні сервіси розглядалися як послуги винятково для державних структур, тому після обговорення експертів згадування про органи державної влади й іже з ними було виключено (до слова, було подано всього одна пропозиція по внесенню зміни, текст якого, на жаль, недоступний; наскільки можна судити по приводяться адресам, що, електронної пошти, текст виправлень розсилався на експертизу в основному представникам бізнес-співтовариства): «Послуги хмарних обчислень – послуги з надання обчислювальних потужностей, включаючи технічні засоби й права використання програм для електронних обчислювальних машин з метою обробки й зберігання інформації з використанням технічних засобів, взаємодіючих через інформаційно-телекомунікаційні мережі».

Однак поточне формулювання як і раніше носить занадто загальний характер (наприклад, під дане визначення підходять послуги аутсорсингу обчислювальної інфраструктури, коли оператор не тільки обслуговує відомчу мережу, але й надає в оренду встаткування. Крім того, вона не відбиває специфіки хмарних сервісів: оперативне одержання послуг при мінімальній участі провайдеру, оплату за фактичне використання й інші особливості. Далі, не тільки не проводиться явного розходження між різними моделями надання хмарних сервісів («інфраструктура як сервіс» і «ПЗ як сервіс»), але вони фактично змішуються – «надання обчислювальних потужностей (IaaS), включаючи...права використання програм (SaaS)». (І нарешті, винятково редакторське зауваження – після «обчислювальних машин» необхідна кома, інакше виходить нелегкотравна фраза про «технічні засоби ... з використанням технічних засобів».)

У виправленнях даються визначення не тільки хмарних сервісів, але також хмарної інфраструктури й постачальника послуг хмарних обчислень, які по суті носять тавтологічний характер: хмарна інфраструктура – це інфраструктура для надання хмарних сервісів. Втім, якщо підходити формально, з визначення не цілком ясно, чи входять у неї мережі доступу або тільки мережі усередині ЦОДа, оскільки передача інформації (надання її клієнтові) не згадується в числі операцій з даними: «хмарна інфраструктура – сукупність програмно-технічних засобів і інформаційно-телекомунікаційних мереж, що забезпечують обробку й зберігання інформації з метою надання послуг хмарних обчислень».

Як провайдери можуть виступати як юридичні особи, так і індивідуальні підприємці. До них пред'являються три основних вимоги: постачальник повинен забезпечити доступність інформації й програмного забезпечення, можливість обробки даних (включаючи повне видалення) і, нарешті, захист інформації (відповідно до вимог ст. 16 з 5-й частини закону про інформацію). Окремо обмовляється, що постачальник не має ніяких прав на інформацію (не є її власником). Здійснювати поставку хмарних послуг державним і муніципальним органам можуть тільки українські компанії (і навіть індивідуальні підприємці), а їхня хмарна інфраструктура повинна перебувати на території України. Провайдерам необхідно буде одержати акредитацію. Крім того, міністерство зобов'язане розробити вимоги до контрактів і договорів на надання хмарних послуг. Порядок надання послуг визначить уряд України.

Перший закон про хмари був прийнятий у Південній Кореї. Його повна назва – «Закон про розвиток хмарних обчислень і захисту користувачів» («Act on the Development of Cloud Computing and Protection of Users», скорочено – Korean Cloud Act). Держава зважилася на

дерегулювання галузі, оскільки Південна Корея була однією з деяких країн, де суспільним інститутам заборонялося орендувати хмарні сервери в приватних провайдерів. Головною причиною заборони було побоювання щодо можливих погроз інформаційної безпеки, який, як виявляється з назви, у законі приділяється особлива увага.

На розробку й прийняття цього документа пішло біля півтора років (постанова уряду бути схвалено у вересні 2013 року, а закон прийнятий у березні 2015-го й набув чинності у вересні того ж року). Причому спочатку комітет з науки, ІКТ, майбутньому плануванню й комунікаціям не квапився з його розглядом, вважаючи більше важливим рішення інших завдань, зокрема прийняття закону про віщання.

Закон поширюється на всі суспільні інститути – центральний уряд, громадські організації, установи охорони здоров'я й утворення – і покликаний стимулювати першочергове використання хмарних сервісів для підвищення продуктивності й конкурентоспроможності.

Місцевий ринок хмарних обчислень відносно невеликий і нерозвинений у порівнянні з локальним ІТ-ринком, щодо цього він схожий з українським. По оцінках інституту економічних досліджень Digiesco, в 2014 році його обсяг склав 863 млн доларів, що порівнянно з розміром українського хмарного ринку (до знецінення гривни). Як очікується, його щорічний ріст повинен скласти 30% за рахунок наступних мір:

- нарощування інвестицій у розвиток хмарного ринку й розширення підтримки, насамперед з боку уряду;
- дозвіл і заохочення повсюдного використання хмарних сервісів, включаючи публічні сервіси;
- введення мер по забезпеченню безпеки з боку провайдерів хмарних послуг.

Корейське Міністерство науки, ІТ і перспективного планування надає й ряд стимулюючих преференцій, адресованих насамперед невеликим розроблювачам хмарного програмного забезпечення: податкові відрахування й технічна допомога. Крім того, такі компанії одержать пріоритет при проведенні державних тендерів на реалізацію науково-дослідних проектів у сфері хмарних технологій.

Вся відповідальність за захист даних переноситься із клієнта на провайдера хмарних сервісів. Як затверджується, це зроблено для того, щоб компаніям без досвіду роботи в ІТ не доводилося додатково витрачатися на безпеку, і тоді хмарні сервіси стануть для них більше привабливими. Власники даних повинні підписати угоду із провайдером і вказати, яка збережена в хмарі інформація може бути розкрита, а яка немає.

Спочатку передбачалося, що контроль за відповідністю вимогам безпеки стане здійснювати Національне агентство розвідки (НАР). Зокрема, провайдери повинні були б повідомляти НАР про всі інциденти безпеки із хмарними сервісами. Однак побоювання у відношенні того, що НАР одержить необмежений контроль за хмарними сервісами й персональними даними, привело до суспільних протестів, і ця стаття була вилучена з підсумкового тексту. Відповідно до закону про інциденти провайдер повинен повідомляти про підозрілі випадки в галузеве міністерство, і саме воно буде ініціювати перевірку.

Вимоги до хмарних провайдерів

При виборі провайдера клієнти повинні з'ясувати його відповідність вимогам закону про хмари. Відповідно до нового південнокорейського законодавства, на провайдерів хмарних послуг покладає ряд зобов'язань:

- провайдер зобов'язаний повідомити про факт витоку інформації, якщо такий мав місце, своїм клієнтам і в профільне міністерство; останнє може провести розслідування інциденту;
- провайдер не повинен надавати приналежним клієнтам інформацію третій стороні або використовувати неї для інших, відмінних від застережених, цілей без згоди клієнта;
- провайдер повинен повернути або видалити дані клієнта після закінчення строку контракту про надання хмарних послуг;

- при розміщенні інформації за межами Південної Кореї клієнт може зажадати від провайдеру розкрити її місцезнаходження;
- якщо клієнт поніс втрати внаслідок навмисних дій провайдеру або через його недбалість і порушення закону про хмари, то клієнт може зажадати відшкодування від провайдеру, що повинен сам доводити свою невинність;
- підзаконними актами міністерства будуть деталізовані вимоги до якості/функціональності хмарних сервісів і належних рівнів обслуговування, а також стандарти для захисту інформації;
- крім цього, планується введення системи сертифікації хмарних сервісів і стандартизованих контрактів на використання хмарних сервісів.

У законі про хмари поки немає якої-небудь прив'язки до міжнародних стандартів. У ряді країн для оцінки провайдеру хмарних послуг регулювальні органи орієнтуються, наприклад, на рекомендації ISO/IEC 27001 і ISO/IEC 27018. Передбачені останнім інструменти контролю відповідають багатьом положенням південнокорейського закону (і навіть пред'являють більше тверді вимоги), тому в тих провайдерів, які вже забезпечили відповідність ISO/IEC 27018, не повинне виникати яких-небудь проблем з його виконанням.

Як сподіваються в Південній Кореї, прийняття цього закону, з одного боку, активізує розвиток суміжних галузей, а з іншої, буде мотивувати недержавні компанії до використання хмарних сервісів. Розвиток необхідної інфраструктури для надання хмарних сервісів повинне сприяти росту таких зв'язаних галузей, як телемедицина, фінансові послуги й Інтернет речей. А як показує досвід Китаю, що у цьому випадку є прикладом, впровадження хмарних послуг у державному секторі сприяє їхній популяризації в приватному секторі.

Розуміння основ комп'ютерної безпеки ще ніколи не було таким важливим. З огляду на те, що наше життя дедалі більше перебуває в Інтернеті, захист вашої особистої інформації є ключем до збереження вашої конфіденційності та запобігання крадіжці особистих даних.

Комп'ютерна безпека охоплює широкий спектр практик, протоколів і технологій, спрямованих на захист ІТ-систем від несанкціонованого доступу, витоків даних та кіберзагроз. Вона передбачає впровадження різних заходів безпеки, включаючи брандмауери, антивірусний захист, персональний брандмауер та інструменти шифрування, всі з яких розроблені для захисту конфіденційної інформації від зловмисників.

Перш ніж ми поговоримо про послуги комп'ютерної безпеки, давайте розглянемо визначення комп'ютерної безпеки. Комп'ютерна безпека включає захисні заходи та практики, які ви впроваджуєте для запобігання несанкціонованому доступу до ІТ-систем. Водночас вона забезпечує цілісність, конфіденційність та доступність ваших даних та цифрової інформації.

Якщо ви хочете досягти надійної комп'ютерної безпеки, потрібен багатогранний підхід, який включає різні компоненти. Зазвичай це включає шифрування даних для захисту конфіденційної інформації, гарантуючи, що навіть у разі перехоплення дані залишатимуться нечитабельними без відповідних ключів розшифрування. Стандарти шифрування також відіграють значну роль у забезпеченні безпеки ваших даних.

Контроль доступу є життєво важливим для обмеження дозволів користувачів та доступу до системи лише уповноваженими особами, тим самим мінімізуючи потенційні вразливості. Методи автентифікації, такі як захист паролем, біометричне сканування та багатофакторна автентифікація, забезпечують додаткові рівні безпеки, перевіряючи особу користувачів.

Разом ці елементи створюють комплексну систему, необхідну для захисту ваших цифрових активів від потенційних загроз та порушень.

Важливість комп'ютерної безпеки для захисту даних

Ефективні заходи захищають конфіденційну інформацію від таких загроз, як крадіжка особистих даних та витoki даних, зокрема тих, що виникають внаслідок підозрілих електронних листів.

У сучасному цифровому середовищі, де величезні обсяги особистої та фінансової інформації поширюються онлайн, наслідки недостатньої безпеки можуть бути руйнівними. Це може призвести не лише до фінансових втрат, але й до значного порушення довіри між користувачами. Ви повинні розуміти ризики, пов'язані із незахищеними системами, оскільки один недогляд може призвести до несанкціонованого доступу до особистих даних. Захистіть свої IT-системи від несанкціонованого доступу, застосовуючи надійні заходи безпеки.

Складний взаємозв'язок між комп'ютерною безпекою та конфіденційністю в Інтернеті стає дедалі важливішим, що підкреслює необхідність надійних захисних заходів.

Надаючи пріоритет безпеці, ви можете краще гарантувати конфіденційність своїх даних, тим самим зберігаючи свою конфіденційність в епоху кіберзагроз. Розгляньте можливість використання VPN для безпечного з'єднання Wi-Fi та уникнення публічних Wi-Fi, щоб покращити свою конфіденційність в Інтернеті.

Види загроз комп'ютерній безпеці та онлайн-загроз

Вам слід знати про різні типи загроз комп'ютерній безпеці, які становлять значні ризики для захисту даних. До них належать:

- кібератаки;
- фішингові атаки;
- шкідливе програмне забезпечення, що походить з підозрілих електронних листів.

Всі вони прагнуть використати вразливості в IT-системах, включаючи вразливості програмного забезпечення та програмне забезпечення сторонніх розробників.

Поширені загрози безпеці даних

Хочете знати, які поширені загрози безпеці даних? Ось огляд для вас: шкідливе програмне забезпечення, фішингові атаки та несанкціонований доступ – це вважаються поширеними загрозами безпеці даних.

Вони можуть призвести до серйозних наслідків, таких як крадіжка особистих даних та витік даних, які впливають як на організації, так і на окремих користувачів. Впровадження заходів безпеки програм та захисту електронної пошти може зменшити ці ризики.

Ці загрози діють за допомогою різних механізмів, спрямованих на вразливості в системах, мережах або поведінці людини. Наприклад, шкідливе програмне забезпечення може проникнути на пристрій користувача через заражені вкладення електронної пошти або завантаження шкідливого програмного забезпечення, зрештою компрометуючи конфіденційну інформацію. Фішингові атаки часто маскуються під законні повідомлення, обманом змушуючи людей розкривати особисті дані або облікові дані для входу. Несанкціонований доступ зазвичай передбачає використання слабких паролів або застарілих заходів безпеки, що дозволяє кіберзлочинцям порушувати бази даних та витягувати конфіденційні дані.

Реальні приклади, такі як витік даних Equifax та злом мережі Sony PlayStation Network, підкреслюють руйнівний вплив цих загроз безпеці – не лише на постраждалі організації, але й на мільйони людей, чиї дані можуть бути використані неналежним чином.

Розуміння кібератак

Кібератаки – це зловмисні спроби порушення безпеки IT-систем та мереж з метою отримання доступу, викрадення або маніпулювання конфіденційними даними. Такі порушення можуть призвести до серйозних наслідків як для окремих осіб, так і для організацій, включаючи проблеми з безпекою обладнання.

Ці загрози можуть виникати з різних мотивів, включаючи фінансову вигоду, політичні цілі або особисту помсту. Кіберзлочинці використовують низку методів, таких як фішингові електронні листи, програми-вимагачі та розподілені атаки типу «відмова в обслуговуванні» (DDoS), для використання вразливостей у системах та IT-обладнанні.

Гучні інциденти, такі як витік даних Equifax у 2017 році та атака програм-вимагача WannaCry, служать яскравим нагадуванням про руйнівний вплив, який ці порушення можуть мати на конфіденційність, фінансову стабільність, цілісність організації та IT-системи.

Щоб зменшити ці ризики, як підприємства, так і приватні особи повинні впроваджувати надійні заходи безпеки. Регулярні оновлення програмного забезпечення, навчання співробітників та передові системи виявлення загроз можуть значно посилити захист від постійно мінливого ландшафту кіберзагроз. Розгляньте можливість звернутися за порадою до споживачів з авторитетних джерел, таких як PCMag, Wired та The Guardian, щоб дізнатися про найновіші методи безпеки.

Найкращі практики для комп'ютерної безпеки

Щоб захистити вашу конфіденційну інформацію та зменшити ризики, пов'язані з кіберзагрозами, впровадження найкращих практик комп'ютерної безпеки може допомогти вашій організації.

Надаючи пріоритет наступним практикам, ви можете покращити загальний рівень безпеки та захистити критично важливі дані від потенційних вразливостей.

1. Впровадження надійних паролів та автентифікації

Номер один: впровадження надійних паролів та багатофакторної автентифікації – це фундаментальний крок у захисті даних, який значно знижує ризик несанкціонованого доступу до конфіденційної інформації та ІТ-систем. Уникайте використання особистої інформації у своїх паролях та будьте обережні з підозрілими електронними листами із запитом на введення облікових даних.

Вживаючи цих заходів безпеки, ви можете створити надійну лінію захисту від кіберзагроз. Надійний пароль повинен складатися з комбінації великих і малих літер, цифр і спеціальних символів, в ідеалі довжина пароля повинна перевищувати 12 символів. Ця складність ускладнює для зловмисників злом паролів методами грубої сили. Не поширюйте свої паролі через незахищені канали, такі як демонстрація екрана або публічні Wi-Fi.

Багатофакторна автентифікація забезпечує додатковий рівень безпеки, вимагаючи від вас підтвердження вашої особи за допомогою другого засобу, такого як код текстового повідомлення або додаток для автентифікації. Такий підхід суттєво мінімізує ймовірність несанкціонованого доступу, навіть якщо паролі скомпрометовані, особливо у віддаленому місці.

Найкращі практики також включають регулярне оновлення паролів та використання менеджера паролів для безпечного зберігання, що ще більше покращує загальну гігієну ваших паролів. Переконайтеся, що ваш менеджер паролів захищений надійними стандартами шифрування.

2. Регулярні оновлення програмного забезпечення та управління патчами

Звичайно, всі ми знаємо, що нам слід регулярно оновлювати наші пристрої, але це особливо важливо для безпеки даних. Регулярні оновлення програмного забезпечення та ефективне управління виправленнями допомагають вашій організації усунути вразливості безпеки, які кіберзлочинці часто використовують для отримання несанкціонованого доступу до ІТ-систем та конфіденційних даних. Це включає забезпечення актуальності програмного забезпечення сторонніх розробників для запобігання зловживанням.

Слідкування за цими оновленнями не лише зміцнює ваш захист від потенційних порушень, але й підвищує загальну продуктивність і надійність системи. В епоху, коли витоки даних стають дедалі поширенішими, важливість управління виправленнями важко переоцінити.

Правильно впроваджені оновлення знижують ризик експлуатації, усуваючи лазівки, якими можуть скористатися кіберзлочинці. Найкращі практики включають встановлення послідовного графіка оновлень, визначення пріоритетів критичних виправлень на основі оцінки ризиків та використання інструментів автоматизації, коли це можливо, для оптимізації процесу. Організації також повинні впроваджувати налаштування конфіденційності для контролю доступу до конфіденційної інформації.

Крім того, організації отримують користь від навчання персоналу важливості обслуговування програмного забезпечення, сприяючи колективному зобов'язанню щодо

захисту конфіденційної інформації. Такі ресурси, як програми навчання з безпеки від Microsoft, можуть бути безцінними в цьому відношенні.

3. Стратегії резервного копіювання даних

Впровадження ефективних стратегій резервного копіювання даних допомагає запобігти втраті даних через кібератак, збої обладнання або випадкове видалення. Це гарантує, що ваша цінна інформація залишатиметься доступною та безпечною протягом усього її життєвого циклу. Розгляньте можливість використання хмарного резервного копіювання та регулярного тестування резервних даних, щоб забезпечити їх цілісність.

Існує кілька методів резервного копіювання, які варто розглянути, зокрема хмарні резервні копії, які забезпечують можливість зберігання даних поза офісом та автоматичну синхронізацію. Крім того, ви можете вибрати знімні варіанти сховища, такі як зовнішні жорсткі диски або USB-флеш-накопичувачі, для локального зберігання даних. Також доцільно регулярно створювати резервні копії даних для захисту від потенційних випадків витоку даних.

Регулярне резервне копіювання не лише захищає вас від непередбачених катастроф, але й відіграє життєво важливу роль у підтримці цілісності даних та забезпеченні їхнього захисту з часом.

Щоб створити надійну стратегію резервного копіювання, важливо встановити графік резервного копіювання, який відповідає частоті оновлення ваших даних, використовувати шифрування для будь-якої конфіденційної інформації та регулярно тестувати процеси відновлення, щоб переконатися, що все працює безперебійно, коли це необхідно. Використовуйте інструменти шифрування для ефективного захисту ваших даних.

Застосовуючи ці методи, ви можете ефективно захистити свої дані від різноманітних загроз та досягти спокою. Розгляньте можливість інтеграції багатофакторної автентифікації для подальшого підвищення безпеки ваших ІТ-систем.

Захист даних у різних середовищах

Мобільні пристрої, віддалені місця та загальнодоступні мережі Wi-Fi – дані потребують захисту в різних середовищах. Тому вам потрібно впровадити індивідуальні заходи безпеки.

Такий підхід є важливим для збереження цілісності та конфіденційності конфіденційної інформації. Переконайтеся, що ІТ-обладнання захищене, а параметри конфіденційності в Інтернеті налаштовані належним чином.

Захист даних на мобільних пристроях

Мобільні пристрої часто стають мішенями для кіберзагроз, включаючи шкідливе програмне забезпечення та несанкціонований доступ, через їхню портативність та зручність підключення. Використання рішень мобільної безпеки може значно підвищити безпеку пристроїв.

Впровадження надійних методів, таких як шифрування, допомагає захистити конфіденційну інформацію, навіть якщо пристрій скомпрометовано. Контроль доступу діє як перша лінія захисту, обмежуючи тих, хто може переглядати дані або взаємодіяти з ними. Використання програм безпеки, які забезпечують виявлення загроз у режимі реального часу, може ще більше посилити цей захисний рівень, а впровадження антивірусного захисту може запобігти кібератакам.

Однак, самих лише технологій недостатньо; підвищення обізнаності користувачів щодо розпізнавання потенційних загроз, таких як фішингові атаки, підозрілі завантаження або підозрілі електронні листи, є надзвичайно важливим. Застосовуючи проактивний підхід та навчаючи користувачів, організації можуть значно посилити свою мобільну безпеку, гарантуючи безпеку даних у швидкозмінному цифровому середовищі.

Захист даних під час віддаленої роботи

Віддалена робота означає доступ до конфіденційної інформації через загальнодоступні мережі Wi-Fi або незахищені мережі, оскільки ці середовища створюють

унікальні проблеми безпеки. Захист даних у такому середовищі має бути головним пріоритетом.

Для ефективного захисту конфіденційних даних важливо використовувати віртуальну приватну мережу (VPN). VPN шифрує ваше інтернет-з'єднання, значно знижуючи ризик перехоплення кіберзлочинцями. Розгляньте можливість використання особистої точки доступу як альтернативи публічному Wi-Fi для безпечнішого з'єднання Wi-Fi.

Крім того, переконайтеся, що ваші з'єднання захищені, використовуючи надійні паролі та двофакторну автентифікацію, коли це можливо. Також важливо оновлювати антивірусне програмне забезпечення та брандмауери, оскільки ці заходи додатково захищають ваші пристрої від потенційних загроз.

Регулярний перегляд та зміна налаштувань безпеки на ваших особистих пристроях допоможе створити безпечніше середовище для віддаленої роботи, захищаючи від несанкціонованого доступу та витоків даних.

Забезпечення безпеки хмарного сховища

Забезпечення безпеки хмарного сховища вимагає впровадження надійних заходів, таких як шифрування та контроль доступу, для захисту конфіденційних даних від несанкціонованого доступу та порушень. Розгляньте можливість використання стандартів шифрування та регулярного оновлення налаштувань конфіденційності для підтримки безпеки даних.

У сучасному цифровому середовищі, де витоки даних стають все більш поширеними, вкрай важливо застосовувати проактивний підхід до захисту хмарного сховища. Організації повинні усвідомлювати, що хоча хмарні рішення пропонують значні переваги, вони також несуть низку потенційних ризиків, включаючи втрату даних та викрадення облікових записів.

Використовуючи найкращі практики, такі як надійні методи шифрування, для захисту даних як під час зберігання, так і під час передачі, компанії можуть значно зменшити ймовірність компрометації своєї інформації. Регулярні аудити безпеки мають вирішальне значення для виявлення вразливостей та забезпечення актуальності протоколів безпеки.

Розуміння цих стратегій може значно покращити загальний рівень безпеки та вселити користувачам впевненість у безпеці їхніх цінних даних.

Технології безпеки даних

Технології безпеки даних допомагають вам у боротьбі з кіберзагрозами, надаючи низку методів захисту конфіденційної інформації та забезпечення цілісності ваших ІТ-систем.

1. Методи шифрування

Методи шифрування пропонують критично важливий рівень безпеки, який захищає цифрову інформацію від несанкціонованого доступу та витоків даних.

Ці методи шифрують конфіденційні дані як під час передачі, так і в стані спокою, гарантуючи, що лише уповноважені особи можуть розшифрувати інформацію та отримати до неї доступ. З огляду на зростаючу залежність від цифрових платформ для особистих та ділових транзакцій, важливість надійних методів шифрування неможливо переоцінити.

Такі інструменти, як AES (Advanced Encryption Standard) та RSA (Rivest-Shamir-Adleman), широко використовуються завдяки своїй ефективності у підтримці цілісності даних.

Застосовуючи передові практики, такі як регулярне оновлення ключів шифрування та впровадження багатфакторної автентифікації, ви можете ще більше покращити свої заходи безпеки. У швидкозмінному цифровому середовищі інформування про нові технології шифрування є критично важливим для будь-якої організації, яка прагне захистити цінні дані від потенційних загроз.

2. Брандмауери та антивірусне програмне забезпечення

Брандмауери та антивірусне програмне забезпечення є критично важливими компонентами захисту даних, що слугують першою лінією захисту від шкідливого

програмного забезпечення та несанкціонованого доступу у ваших ІТ-системах. Впровадження захисту брандмауером може допомогти запобігти несанкціонованому доступу до вашої мережі.

Ці інструменти безпеки працюють шляхом моніторингу та контролю вхідного та вихідного мережевого трафіку, ефективно створюючи бар'єр між вашими довіреними внутрішніми мережами та ненадійними зовнішніми. Брандмауери ретельно перевіряють пакети даних і можуть блокувати потенційні загрози, перш ніж вони досягнуть ваших пристроїв, тоді як антивірусне програмне забезпечення виявляє, поміщає в карантин та видаляє шкідливі програми. Разом вони створюють надійну систему, яка захищає конфіденційну інформацію та забезпечує цілісність системи. Регулярний перегляд та оновлення налаштувань безпеки має вирішальне значення для підтримки ефективної безпеки мережі.

У швидкозмінному кіберсередовищі важливо регулярно оновлювати як брандмауери, так і антивірусні рішення. Таке обслуговування не лише забезпечує їх найновішими визначеннями загроз, але й підвищує їхню здатність боротися з новими вразливостями, що підкреслює важливість проактивних стратегій кіберзахисту.

3. Інструменти запобігання втраті даних

Інструменти запобігання втраті даних (DLP) є важливими для захисту конфіденційної інформації шляхом моніторингу та контролю передачі даних, що ефективно мінімізує ризик несанкціонованого доступу та витоків даних. Використання методів управління даними разом з інструментами DLP може ще більше покращити захист цифрової інформації.

У сучасному цифровому середовищі, де кіберзагрози стають дедалі складнішими та поширенішими, ці інструменти стають ще більш важливими. Рішення DLP працюють, використовуючи комбінацію методів, включаючи перевірку контенту, контекстний аналіз та поведінкову аналітику, для виявлення та захисту конфіденційних даних на різних платформах. Регулярне навчання заходам безпеки та навчання співробітників з безпеки можуть допомогти розпізнати та пом'якшити загрози.

Організації зазвичай впроваджують стратегії, що включають шифрування конфіденційної інформації, забезпечення суворого контролю доступу та навчання співробітників найкращим практикам захисту даних. Вживаючи цих заходів, ви не лише покращуєте загальний рівень безпеки, але й забезпечуєте дотримання правил, зрештою будуючи довіру з клієнтами та зацікавленими сторонами. Регулярні оновлення програмного забезпечення сторонніх розробників можуть допомогти мінімізувати вразливості програмного забезпечення, які можуть бути використані.

Відповідність нормативним вимогам та безпека даних

Дотримання нормативних вимог є вирішальним аспектом безпеки даних для вашої організації. Важливо дотримуватися різних правил захисту даних, таких як GDPR та CCPA, щоб захистити конфіденційну інформацію та зберегти довіру ваших клієнтів. Регулярне оновлення налаштувань конфіденційності даних допоможе забезпечити дотримання вимог.

Огляд правил захисту даних (GDPR, CCPA тощо)

Нормативні акти щодо захисту даних, такі як GDPR та CCPA, забезпечують важливі рамки, яких ви повинні дотримуватися, щоб забезпечити відповідність вашим практикам безпеки даних та захистити особисту інформацію людей.

Ці правила спрямовані на створення балансу між правами осіб контролювати свою особисту інформацію та вашими обов'язками як організації щодо відповідального управління цими даними. Наприклад, GDPR наголошує на суворих вимогах щодо згоди та вимагає розробки чітких протоколів обробки даних, що включає забезпечення прозорості щодо використання даних та забезпечення прав осіб на доступ до своєї особистої інформації або її видалення. Аналогічно, CCPA надає жителям Каліфорнії право знати, які персональні дані збираються та передаються, тим самим розширюючи їхню автономію щодо особистої інформації.

Наслідки цих правил виходять за рамки простого дотримання; недотримання може призвести до значних фінансових штрафів та шкоди репутації. Це підкреслює критичну важливість впровадження надійних стратегій захисту даних у вашій організації.

Організаційні обов'язки щодо безпеки даних

Організації несуть значну відповідальність за безпеку даних, що включає впровадження ефективних стратегій кібербезпеки, забезпечення дотримання нормативних актів та захист конфіденційної інформації. Поради організацій, що надають консультації споживачам, таких як Національний центр кібербезпеки (NCSC), можуть бути безцінними в цьому відношенні.

Щоб ефективно захистити дані, ви повинні застосовувати проактивний підхід, усвідомлюючи, що цифровий ландшафт постійно розвивається та створює нові загрози. Це вимагає регулярної оцінки та оновлення ваших протоколів кібербезпеки для захисту від потенційних порушень та атак шкідливого програмного забезпечення. Дотримання законів про захист даних, таких як GDPR або CCPA, має вирішальне значення для підтримки довіри клієнтів та уникнення значних штрафів.

Також важливо брати участь у програмах навчання та підвищення обізнаності співробітників, оскільки співробітники часто виступають першою лінією захисту від кібератак. Інтегруючи ці заходи, організації можуть створити надійну систему безпеки, яка не лише захищає дані, але й сприяє культурі безпеки та відповідальності.

Реагування на інциденти та відновлення після них

Реагування на інциденти та відновлення є важливими процесами в управлінні порушеннями даних та забезпеченні стійкості організації до кіберзагроз. Ці процеси спрямовані на відновлення нормальної роботи, одночасно захищаючи конфіденційну інформацію.

Дії, які слід вжити після витоку даних

Після витоку даних організаціям вкрай важливо вжити негайних заходів для зменшення збитків, оцінки наслідків та ініціювання процесів відновлення для захисту конфіденційної інформації та відновлення довіри.

Це передбачає швидке стримування порушення для запобігання будь-якому подальшому несанкціонованому доступу, а потім ретельне розслідування для розуміння масштабів порушення та виявлення вразливостей, які були використані. Після завершення розслідування важливо повідомити про інцидент постраждалі сторони, регуляторні органи та зацікавлені сторони, оскільки прозорість має вирішальне значення для підтримки довіри.

Зусилля з відновлення повинні бути зосереджені на відновленні систем та впровадженні заходів для запобігання повторенню. Проведення оцінки після інциденту є життєво важливим для вдосконалення протоколів безпеки, забезпечення того, щоб отриманий досвід спонукав до оновлення існуючих захисних механізмів, та підвищення загальної стійкості організації до майбутніх загроз.

Відновлення даних та систем

Відновлення даних і систем після порушення є критично важливим компонентом процесу реагування на інциденти, що гарантує, що ваша організація може відновити втрачені дані та підтримувати безпеку своєї IT-інфраструктури.

Цей процес не лише спрямований на відновлення скомпрометованої інформації, але й наголошує на впровадженні надійних заходів безпеки для запобігання майбутнім інцидентам. Організації часто покладаються на резервні дані як фундаментальний елемент своєї стратегії відновлення, що дозволяє швидко відновити роботу, мінімізуючи час простою.

Ефективне відновлення вимагає поєднання регулярного резервного копіювання даних, впровадження посиленних протоколів безпеки та постійного навчання персоналу розпізнаванню потенційних загроз. Постійне вдосконалення є важливим; воно спонукає організації вдосконалювати свої системи, оцінювати вразливості та інтегрувати найновіші технологічні оновлення та виправлення.

Застосовуючи проактивний підхід до кібербезпеки, ваша організація може краще захистити критично важливі дані та підвищити загальну стійкість системи.

На рисунку 1 зображена структурна схема роботи системи. Схема розділена на три основних компоненти:

- Flash накопичувач;
- розроблена програма;
- користувач.

Коли користувач вставляє в персональний комп'ютер Flash накопичувач, відбувається розпізнання операційною системою типу пристрою й виводу меню вироблених дій.

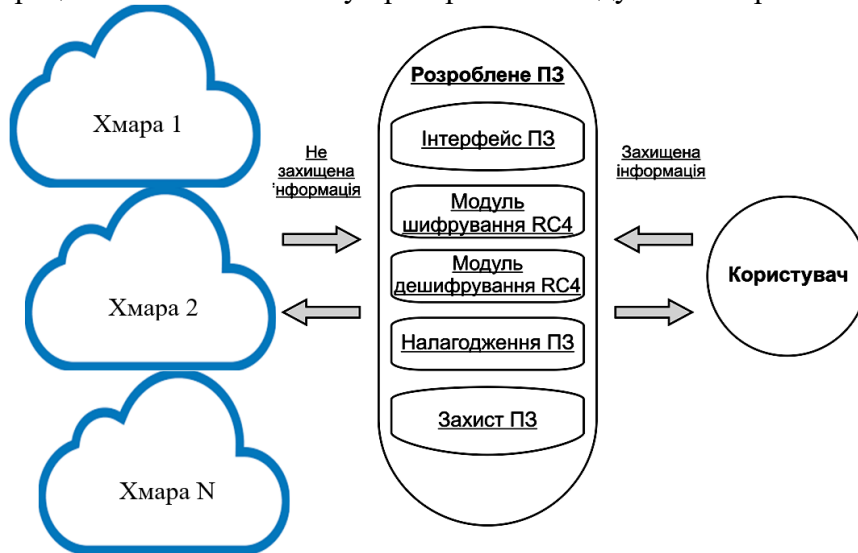


Рисунок 1 – Структурна схема роботи системи

Розроблена програма перехоплює системне повідомлення операційній системі про виклик меню вироблених дій над Flash накопичувачем і активізує власний інтерфейс програми.

Розроблена програма складається з декількох частин:

- інтерфейсу програми;
- модуля потокового шифрування RC4;
- модуля потокового дешифрування RC4;
- налаштування програми й захисту програми.

Розроблена програма управляє процесом обміну інформацією між Flash накопичувачем і персональним комп'ютером, використовуючи потоковий алгоритм шифрування інформації RC4. Завдяки такому підходу, можливо використовувати всі існуючі на даний момент Flash накопичувачі не зупиняючись на окремих реалізаціях з підвищеними вимогами захищеності Flash накопичувача (рисунок 1).

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів захисту персональних даних у мережевих Cloud-системах. Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем захисту персональних даних у мережевих Cloud-системах.

– Досліджена система захисту персональних даних у мережевих Cloud-системах.

– На основі отриманих результатів досліджень створена програмна реалізація системи захисту персональних даних у мережевих Cloud-системах. Розроблені алгоритми дозволяють успішно вирішувати завдання захисту персональних даних у мережевих Cloud-системах. 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., Bebeshko, 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., 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.
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., Prysiazhnyy, 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., Yenchey, 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., Bebeshko, 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.
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 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.
32. 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.

УДК 004

І.Воропай, магістр гр. КІ-24М,*Центральноукраїнський національний технічний університет*

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ВИЯВЛЕННЯ УРАЗЛИВИХ ДОДАТКІВ У МЕРЕЖЕВИХ CLOUD-SERVICES

У статті розроблено програмне забезпечення, яке призначено для системи виявлення уразливих додатків у мережесервісах. Метою розробки є дослідження та принципи побудови системи виявлення уразливих додатків у мережесервісах. Об'єктом дослідження є процес виявлення уразливих додатків у мережесервісах. Предметом дослідження є методи виявлення уразливих додатків у мережесервісах. Методи дослідження базуються на методах захисту інформації у мережі, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи виявлення уразливих додатків у мережесервісах. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

уразливі додатки, Cloud-сервіси

Постановка проблеми. При розміщенні клієнтських додатків у хмарі необхідно передбачити міри захисту на випадок наявності в них уразливостей і інших недекларованих можливостей. Забезпечення безпеки хмарного сервісу – досить складне завдання. Зобов'язання щодо доступності сервісу й захищеності даних у ньому – невід'ємна частина пропозиції й важливий пункт SLA. Провайдери хмарних сервісів не скупляться на реалізацію засобів і мер інформаційної безпеки, оскільки захищеність забезпечує ним вагому конкурентну перевагу. Для цього використовуються антивірусні засоби, міжмережні екрани різних рівнів, системи протидії DDoS і запобігання вторгнень, різноманітні «пісочниці», SOC/SIEM і т.п. У гарному хмарному центрі є цілодобова служба моніторингу й відбиття атак, що складає із кваліфікованих фахівців. Однак забезпечення захисту стає куди більше складним завданням, коли хмарний провайдер надає своїм користувачам можливість розміщати їхні власні сервіси по моделі IaaS і PaaS. Тоді в системі, яка захищається, виникає шар клієнтських додатків, контролювати якість яких провайдер не в змозі. Уразливий додаток може стати проблемою не тільки для тих, хто його написав, але й для інших клієнтів хмарного провайдера. Неодноразово вже виникали ситуації, коли атаці піддавався додаток, розміщений в центрі обробки даних, але під її впливом виявлялися недоступні всі додатки. Крім того, зламавши один додаток, наприклад одержавши до нього привілейований доступ, зловмисник здатний заразити й скомпрометувати інші в цій же хмарі. Як би не були ізольовані ресурси, керування ними (або їхньою частиною) нерідко здійснюється з одного центра.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи виявлення уразливих додатків у мережесервісах.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи виявлення уразливих додатків у мережесервісах.

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

- Огляд існуючих систем виявлення уразливих додатків у мережесервісах.
- Дослідження системи виявлення уразливих додатків у мережесервісах.

– Програмна реалізація системи виявлення уразливих додатків у мережевих Cloud-сервісах.

Об'єктом дослідження є процес виявлення уразливих додатків у мережевих Cloud-сервісах.

Предметом дослідження є методи виявлення уразливих додатків у мережевих Cloud-сервісах.

Методи дослідження базуються на методах захисту інформації у мережі, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Загальнодоступні й приватні хмари піддаються як атакам зловмисників, так і збоєм інфраструктури, наприклад, відключенням живлення. Такі події можуть вплинути на роботу серверів доменних імен, зробити хмара недоступним або прямо порушити функціонування хмари.

Наприклад, атака на Akamai Technologies, проведена 15 червня 2004 р., викликала проблеми з дозволом доменних імен і великий збій, що торкнувся Google Inc., Yahoo! Inc. і багато інших сайтів. У травні 2009 р. Google виявився метою серйозної DoS-атаки (denial-of-service), що вивела з ладу на кілька днів такі сервіси як Google News і Gmail.

Блискавка викликала тривалий простий Amazon.com Inc. 29 і 30 червня 2012. Хмара Amazon Web Services (AWS) у східному регіоні Сполучених Штатів, що складає з десяти центрів даних у чотирьох зонах доступності, спочатку випробовувала проблеми через коливання електроживлення, імовірно, викликаних грозою. 29 червня 2012 гроза на східному узбережжі США вивела з ладу деяку апаратуру Amazon, розташовану у Вірджинії, що порушило роботу компаній, що використовувала системи тільки із цього регіону. Як повідомляють, однієї з жертв цього простою виявився сервіс обміну фотографіями Instagram.

Відновлення після цих подій зажадало багато часу й було пов'язане з рядом проблем. Наприклад, один з десяти центрів не зміг перемкнутися на запасні генератори до того, як сіли джерела безперебійного живлення (UPS). AWS застосувало «площини керування» (control planes), щоб дозволити користувачам перемкнутися на ресурси в інших регіонах, але цей програмний компонент також відмовив.

Процес початкового завантаження виявився недосконалим і збільшив час, необхідне для перезапуску сервісів Elastic Compute Cloud (EC2) і Elastic Block Store (EBS). Ще однією критичною проблемою став «баг» в Elastic Load Balancing (ELB), що служив для маршрутизації трафіку на сервери з доступними ресурсами. Аналогічний «баг» порушив процес відновлення Relational Database Service (RDS). Ця подія виявила «сховані» проблеми, які можуть відбутися тільки при особливих обставинах.

Частини хмари

Провайдер хмарних додатків, провайдер хмарного сховища й провайдер мережі можуть реалізовувати різні політики. Непередбачена взаємодія між балансувальником навантаження й інших реактивних механізмів може привести до втрати динамічної стійкості. Непередбачене сполучення незалежних компонентів, керуючих навантаженням, споживанням енергії й елементами інфраструктури може привести до виникнення небажаного зворотного зв'язка й нестабільності, аналогічно тому, як це може відбутися при маршрутизації, заснованої на політиках, при використанні Internet Border Gateway Protocol (BGP).

Наприклад, балансувальник навантаження провайдеру додатків може взаємодіяти з оптимізатором споживання енергії провайдеру інфраструктури. Деякі з таких сполучень можуть виникати тільки в надзвичайних ситуаціях, і їх буває дуже складно виявити при роботі в нормальних умовах. Це може привести до катастрофічних наслідків, коли система буде намагатися відновитися після серйозного збою, як це й відбулося в 2012 р. з AWS.

Кластеризація ресурсів у центрах даних, розташованих у різних географічних областях, – один із засобів, застосовуваних для зниження ймовірності катастрофічних збоїв. Такий географічний розподіл ресурсів може мати додатковий позитивний побічний ефект. Воно дозволяє скоротити трафік обміну інформацією й витрати на електрику, переводячи

обчислення в ті місця, де електроенергія дешевше. Також це може підвищити продуктивність за рахунок застосування інтелектуальної й ефективної стратегії балансування навантаження.

При організації хмарної інфраструктури ви повинні ретельно збалансувати мети системи, такі як максимальна пропускна здатність, використання ресурсів і фінансові переваги з потребами користувачів, такими як низькі витрати, низький час відгуку й максимальна доступність. За будь-яку оптимізацію системи доводиться платити ростом її складності. Наприклад, затримка при обміні інформацією через глобальну мережу (WAN) істотно більше, ніж у локальній мережі, і вимагає розробки нових алгоритмів глобального прийняття рішень.

Проблеми, що виникають при наданні хмарних послуг

Хмарні обчислення успадковують деякі із проблем від паралельних і розподілених обчислень. Але їм властиві й деякі власні проблеми. Конкретні проблеми відрізняються для трьох моделей надання хмарних послуг, але у всіх випадках вони обумовлені самою природою надання обчислювальних ресурсів як комунальних послуг, заснованого на спільному використанні й віртуалізації ресурсів, і потребуючу модель довіри, відмінну від повсюдно прийнятої моделі, орієнтованої на користувача, що довгий час була стандартом.

Сама значна проблема – безпека. Для майбутнього хмарної послуги надто важливо завоювати довіру великої кількості користувачів. Не можна розраховувати, що загальнодоступна хмара буде прийнятним середовищем для всіх додатків. Додатка підвищеної відповідальності, що управляють критично важливими інфраструктурами, додатка для охорони здоров'я й інші, швидше за все, будуть виконуватися в закритих хмарах.

Багато додатків, що працюють у реальному часі, також, швидше за все, помістяться у закриті хмари. Деяким додаткам найкраще підійде гібридне хмарне середовище. Такі додатки можуть зберігати коштовні дані в закритій хмарі й використовувати загальнодоступну хмару для певних видів обробки.

У моделі Software as a Service (SaaS) виникають ті ж проблеми, що й в інших онлайнових послугах, що вимагає захисту особистої інформації, таких як фінансові або медичні послуги. У цьому випадку користувач взаємодіє із хмарними сервісами через чітко певний інтерфейс. Тому, у принципі, у провайдеру сервісів виникає менше складностей з перекриттям деяких каналів атаки (attack channels).

Проте, такі сервіси уразливі для DoS-атак і зловмисних внутрішніх користувачів. Найбільш уразливі для атак дані в сховище, тому приділите особливу увагу захисту серверів зберігання. Реплікація даних, необхідна, щоб забезпечити безперервність обслуговування при відмові систем зберігання, збільшує уразливість. Шифрування даних може захистити дані при зберіганні, але, в остаточному підсумку, дані прийде розшифрувати для обробки. І тоді вони будуть уразливі для атаки.

Модель Infrastructure as a Service (IaaS), безсумнівно, сама складна з погляду захисту від атак. Справді, користувач IaaS має набагато більше волі, чим у двох інших моделях надання хмарних послуг. Додаткове джерело проблем – те, що чимала кількість хмарних ресурсів можна задіяти для атаки на мережу й інфраструктуру обчислень.

Украй важливою архітектурною особливістю цієї моделі є віртуалізація, але вона робить системи підданими новим видам атак. Довірена обчислювальна база (trusted computing base, TCB) віртуального середовища містить не тільки встаткування й гіпервізор, але й керуючу ОС. Можна зберегти стан всієї віртуальної машини (VM) у файл, щоб її було можна переносити й відновлювати – підтримка цих двох операцій дуже бажана.

Проте, ця можливість ускладнює стратегії по змісту серверів, що належать організації, у необхідному стабільному стані. Справді, заражена VM може бути неактивною під час перевірки систем. Потім вона почне працювати й заразить інші системи. Це – ще один приклад того, як у базових технологіях хмарних обчислень сполучаються корисні й шкідливі ефекти.

Наступна істотна проблема пов'язана з керуванням ресурсами хмари. Кожне стратегія систематичного керування ресурсами (на відміну від керування по ситуації) вимагає

існування керуючих компонентів, призначених для реалізації декількох класів політик: керування доступом, виділення ресурсів, балансування навантаження, оптимізації енергоспоживання й – останнє один по одному, але не по важливості – надання гарантій якості обслуговування (quality of service, QoS).

Щоб реалізувати ці політики, що управляють компоненти повинні мати точну інформацію про глобальний стан системи. Визначення стану складної системи з 106 або більше серверами, розподіленими по великій території, – нездійсненне завдання. Справді, зовнішнє навантаження, а також стан окремих ресурсів, дуже швидко міняються. У результаті керуючі компоненти повинні функціонувати в умовах неповного або приблизного знання про стан системи.

Здається розумним очікувати, що така складна система може функціонувати тільки на основі принципів самоврядування. Але самоврядування й самоорганізація підвищують вимоги до реалізації процедур ведення журналів і аудита, критично важливих для забезпечення безпеки й довіри до провайдеру хмарних обчислень.

При самоврядуванні стає майже неможливим ідентифікувати, з яких причин почате та або інша дія, через якого виник пролом у захисті.

Остання велика проблема, що я торкнуся, пов'язана із сумісністю й стандартизацією. Залежність від постачальника – той факт, що користувач «прив'язаний» до певного постачальника хмарних послуг – серйозна проблема для хмарних користувачів. Стандартизація забезпечує сумісність і, отже, у якомусь ступені, рятує від побоювань, що сервіс, критично важливий для великої організації, буде недоступним протягом тривалого часу.

Уводити стандарти в період, коли технологія ще розвивається, складно, і може виявитися контрпродуктивним, оскільки, можливо, це буде перешкоджати нововведенням. Важливо усвідомлювати складність проблем хмарних обчислень і розбиратися в цілому ряді технічних і соціальних проблем, що виникають при хмарних обчисленнях. Зусилля по переносу ІТ-операцій у загальнодоступні й закриті хмари, виправдаються в довгостроковій перспективі.

АНБ могло використовувати Logjam для атаки на VPN сервери

Безліч хмарних сервісів піддаються недавно знайденої в TLS-протоколі уразливості за назвою Logjam (CVE-2015-4000), повідомляє компанія по інформаційній хмарній безпеці Skyhigh.

Logjam дуже нагадує уразливість FREAK, однак відрізняється тим, що замість ініціювання зміни шифрів RSA на RSA_EXPORT в Logjam виробляється відкат протоколу Діффі-Хеллмана, використовуюваного для одержання ключа для подальшого шифрування, до слабозахищеного рівня DHE_EXPORT. Уразливість може бути проексплуатована для здійснення атаки «людина по-середині», що дозволить одержати доступ до даних, що проходять через TLS-З'єднання.

Logjam вражає всі сервери, які підтримують 512-бітне експортне шифрування, а також всі сучасні браузері. Відповідно до експертів, більше 8% з Топ-мільйона web-сайтів, що використовують HTTPS, і більше 3% ресурсів, відображуваних у браузері як заслуговують довіри, піддані даної уразливості.

У ході атаки з експлуатацією Logjam зловмисники можуть знизити стійкість шифрування в мільйонів HTTPS, SSH і VPN серверів, які підтримують DHE_EXPORT і використовують для генерації ключа прості 512-розрядні групи початкових чисел Діффі-Хеллмана.

На думку фахівців Skyhigh, команда вчених може зламати 768-бітне просте число, а група хакерів, фінансована державою, може замахнутися на 1024-бітне. Злом єдиного, найпоширенішого 1024-бітного простого числа, використовуюваного web-серверами, дозволить прослуховувати підключення до 18% з мільйона найбільш популярних HTTPS-сайтів. Експерти вважають, що АНБ могло використовувати Logjam для атаки на VPN сервери.

Злом хмарних сервісів: Соціальний інжиніринг у дії

Захисне програмне забезпечення сучасних комп'ютерів – антивіруси, файрволи, антишпигуни, антиспамові рішення, системи виявлення вторгнень і т.д. – виконує завдання будь-якої навіть найвищої складності, але всіма цими високотехнологічними рішеннями управляти набагато легше, ніж людьми. Як би складним не було програмне забезпечення, будь-який фахівець із області інформаційної безпеки з легкістю підтвердить, що сама слабка ланка в будь-якій захисній системі – це людський фактор.

В останні роки в багатьох країнах одержав поширення соціальний інжиніринг, тобто метод керування діями людини без використання технічних засобів, заснована на використанні людських слабостей. Пояснення сутності соціального інжинірингу й, зокрема, таких його різновидів, як гіпноз і нейролінгвістичне програмування (НЛП), гідно окремої статті, саме головне, що ключем до розуміння уразливості людського фактора, є взаємодія між свідомістю й підсвідомістю. Люди вірять у те, що приймають рішення усвідомлено, але НЛП і гіпноз уже давно продемонстрували силу підсвідомості, а дослідження останнього років підтвердили, що підсвідоме прийняття рішень випереджає свідоме часом на 10 секунд.

На цьому засновані технології, що дозволяють маніпулювати людьми, щоб змусити їх виконати певні дії й тим самим розкрити конфіденційну інформацію. Розглянемо, як такі методи можуть бути використані для злому хмарних систем.

Приклади несанкціонованого доступу до даних

Дослідницькою групою були внесені зміни в роботу сайту – про це знало керівництво компанії, який належав сайт, але ІТ-фахівці не були попереджені. Для того щоб користувач міг працювати з електронною поштою, на додаток до звичайної вимоги відповістити на секретне запитання система попросила ввести ім'я користувача й пароль. Як результат, протягом години було уведено 25% логінів/паролів. Крім того, пройшло 2 години, перш ніж ІТ-команда зміркувала, що відбувається, і ще 2 години, перш ніж фахівці компанії змогли опублікувати попередження для користувачів. Незважаючи на вжиті заходи, облікових даних користувачів надходили ще кілька годин після того, як було розіслане попередження.

В іншому випадку дослідницька група зареєструвала домен, дуже схожий на домен цільової компанії. Потім всім співробітникам компанії був розісланий лист, що описує нову процедуру введення пароля, у результаті чого співробітники попадали на фальшивий сайт компанії. Адреса підробленого сайту, що містить схожий з реальним домен, відкрито розміщався в листі; дослідники не робили спроб замаскувати URL. Як і передбачалося, більшість співробітників, що одержали лист, слухняно виконали зазначені дії.

Ще одне дослідження показало, що наявність строгих процедур у процесі внесення змін в адміністративний інтерфейс також є уразливим місцем системи безпеки через відсутність гнучкості. Тобто, якщо хакеру вдається реалізувати позаштатну ситуацію, користувач, швидше за все, буде шукати шляхи до її виправлення, і зловмисникові залишиться тільки «підказати» йому відповідь. Таким чином, часто строгі алгоритми роботи системи відкривають особам, які у достатній мірі володіють методами соціального інжинірингу, доступ до конфіденційної інформації компанії.

У цілому експерименти показали, що користувачі не просто не бачать різниці між офіційним і підробленим доменом, проблема набагато глибше. Незважаючи на регулярно проведені в компаніях тренінги й впроваджувані навчальні програми, більшість співробітників воліє знайомитися не з усіма методами виявлення й протидії вторгненням, а лише з тими, які для них важливі, приміром, особливо популярні можливості безпечного онлайн-банкінга й роботи з відомими онлайн-аукціонами. Таким чином, співробітники компаній своїми діями підтвердили, що не очікують фішинг-атак, спрямованих на їхні робітники дані, хоча й знають, що така атака можлива.

Лов на живця

Зрозуміло, розроблювачі програмного забезпечення не можуть повною мірою враховувати людський фактор, але для того, щоб визначити найбільш уразливі місця в системі безпеки окремо взятої компанії, як ні парадоксально, не обійтися знову ж без

допомоги користувачів. Мова йде про імітацію хакерських атак на систему замовника, результати яких дадуть клієнтові механізм для виміру ефективності поточного захисту системи від соціального інжинірингу. Під атакою, таким чином, розуміються різні тестові сценарії, які призначені для оцінки успішності/неуспішності системи.

Певні труднощі представляє розробка подібних атак, оскільки, по-перше, атакувати потрібно не якого-небудь із користувачів, а безпосередньо службу підтримки, змушуючи її надати хакеру права адміністратора, а по-друге, потрібно досить точно й швидко визначити сектор системи для перевірки, щоб не затягувати процес і швидше ліквідувати уразливість.

Злом хмарного сервісу

Здійснювану в дослідницьких цілях атаку можна розділити на кілька фаз. Протягом першої – відбувається збір початкових даних про систему, приміром, про розташовані в інших країнах підрозділах, про територіальне покриття службою підтримки, інформації про клієнтів, а також збір відомостей про топ-менеджерів і директорів компанії.

Друга фаза містить у собі доступ до мереж компанії в нічний час доби, для того щоб оцінити, що відбувається із системою безпеки у відсутності адміністраторів, а також для того, щоб при необхідності змінити IP-адреса. Також у другій фазі відбувається збір даних про недавно зроблені звільнення й скорочення співробітників, а заодно перевіряється, чи внесли адміністратори відповідні зміни в систему. На третьому етапі дослідниками беруться під контроль облікові записи керуючих і технічного директорів цільової компанії. На четвертому здійснюється контакт зі співробітниками, щоб домогтися їхнього особистого розташування.

Результат експериментальної атаки перевершив всі очікування дослідників: вони домоглися бажаного всього за три цілеспрямованих телефонних дзвінків з використанням психологічних методів соціального інжинірингу в підрозділи компанії – у Великобританії, США й у Китаї. Спочатку керуючий директор подзвонив у британський офіс компанії незадовго до закінчення робочого дня, попередив про можливі проблеми й запросив інформацію про доступ до підтримки, але, відпрацьовуючи сценарій зловмисника, не просив відкрити йому доступ у систему. Другий дзвінок надійшов в офіс у США від клієнта керуючого директора, що просив внести зміни в логін і пароль, пояснюючи це тим, що в нього виникли труднощі з доступом у систему. Третій дзвінок надійшов у китайський офіс компанії від технічного директора компанії, що перебуває в надзвичайних обставинах.

Внаслідок атаки дослідникам удалося обійти строгі процедури забезпечення безпеки; співробітники компанії представили дослідникам подробиці облікових записів; трафік удалося перенаправляти на нову адресу, і в цьому був задіяний співробітник компанії; по телефоні був продиктований новий пароль адміністратора. Надзвичайно важливо, що ніхто зі співробітників не спробував установити особистість що дзвонила.

Учасники експерименту, з огляду на характер атаки, відсутність аудита й повідомлень про зміни в системі, прийшли до висновку, що в результаті вторгнення реальних хакерів несанкціонований доступ міг залишатися непоміченим протягом тривалого часу. Таким чином, незважаючи на те, що хмарна система є технічним рішенням, подібні сервіси залежать від людського фактора так само, як більшість систем інформаційної безпеки. Як підтвердив експеримент, соціальний інжиніринг виявився найшвидшим і легенею шляхом до порушення інформаційної безпеки й самим трудновизначним. Методи соціально інжинірингу, на відміну від електронного злому сайтів, майже неможливо каталогізувати, а вплив доводиться оцінювати, покладаючись на показання свідків співробітників, що стали жертвами, причому треба враховувати, що вони можуть псувати реальність, бажаючи врятувати свою репутацію.

У список найпоширеніших застосувань хмарних сервісів входять: зберігання сканів паспорта й інших особистих документів; синхронізація бази паролів, контактів, листів; створення сайтів; зберігання версій вихідних кодів і т.д. Коли хмарний сервіс зберігання даних Dropbox повідомив про закриття уразливості в генераторі посилань, в інтернеті знову заговорили про те, як важливо шифрувати конфіденційні дані, перш ніж викладати їх на

який-небудь ресурс, навіть якщо він приватний. Шифрування файлів (FLE) дійсно дозволить забезпечити захист конфіденційної інформації в хмарі, навіть у випадку виявлення уразливостей контролю доступу до документів користувачів у тім або іншому хмарному сервісі.

Може зложитися враження, що якщо не викладати в хмари секретні дані, або їх шифрувати, то й ризиків ніяких не буде. Чи не так це? Як виявилося, не зовсім.

В інтернеті часто зустрічаються рекомендації з «ефективного використання хмарних файлових сервісів», наприклад – інструкції з вилученого керування комп'ютером, стеженню за комп'ютером під час своєї відсутності, керування torrent-завантаженнями й багато інше. Інакше кажучи, користувачі самі створюють усілякі діри, якими з легкістю скористається й троянець, і хробак, і тим більше хакер, особливо якщо мова йде про цільові атаки.

Ми задалися питанням – наскільки великий ризик зараження корпоративної мережі через хмарний сервіс?

Спочатку, використовуючи фішинг, розроблювач заразив ноутбук співробітника, далі – впровадив шкідливі скрипти в документи, що зберігаються в «хмарній» папці ноутбука. Dropbox автоматично оновив (синхронізував) заражені документи на всіх пристроях, пов'язаних з аккаунтом користувача. Щодо цього Dropbox не унікальний – функція автоматичної синхронізації є у всіх популярних додатках для доступу до хмарних файлових сервісів, у тому числі Onedrive (він же Skydrive), Google Disk, Yandex Disk і т.д.

Коли користувач відкрив заражений документ на робочому комп'ютері, що перебуває в корпоративній мережі, впроваджені в документ скрипти встановили в систему бекдор DropSmack, створений розроблювачем спеціально для цього пен-тесту. Як можна догадатися за назвою, ключова особливість DropSmack – використання хмарного файлового сховища Dropbox як канал для керування бекдором і передачі корпоративних документів назовні крізь корпоративний файрвол.

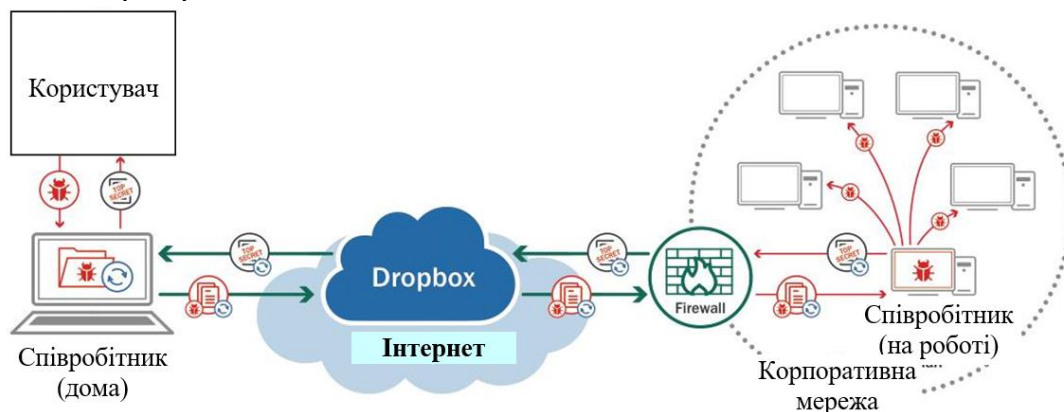


Рисунок 1 – Структурна схема системи

Метод проникнення в корпоративну мережу, використаний розроблювачем у ході пен-тесту, дивує своєю простотою – так, це очевидна діра!

Ми вирішили перевірити, чи використовують справжні зловмисники Dropbox, OneDrive, Yandex Disk і Google Disk для поширення шкідливого ПЗ. Зібравши інформацію з KSN про детектах вірусів, виявлених в «хмарних» папках на комп'ютерах користувачів, ми з'ясували, що такі зараження зафіксовані в дуже невеликого числа користувачів: у травні цього року тільки 8,7 тис. чоловік зштовхнулися із зараженням «хмарної» папки. У користувачів домашніх продуктів ПК на такі шкідливі програми доводиться 0,42% всіх детектів, у користувачів корпоративних продуктів – 0,24%.

Слід зазначити одну немаловажну деталь – якщо вірус потрапив у хмару з одного пристрою, всі підключені до зараженого аккаунту клієнти самі завантажують його на свої пристрої, так ще й по протоколу HTTPS. Навіть якщо на одному із пристроїв антивірус

помітити і видалити заразу прямо в папці синхронізації, хмарний клієнт буде, з обов'язку служби, боротися зі сформованою рассинхронізацією, без кінця завантажуючи вірус із хмари.

За нашим даними, близько 30% шкідливого ПЗ, виявленого в «хмарних» папках на домашніх комп'ютерах, попадає на комп'ютери через механізми синхронізації! У корпоративних користувачів цей показник досягає 50%. Таким чином, механізм, що використовувався демонстраційним вірусом розроблювача, приводить до заражень у реальному житті. На щастя, ми поки не виявили цільових атак з використанням хмарних сервісів зберігання даних.

Серед шкідливого ПЗ, виявленого нами в «хмарних» папках на комп'ютерах користувачів, переважають файли форматів Win32, MSIL, VBS, PHP, JS, Excel, Word, Java. Варто відзначити, що між корпоративним і домашнім користувачами є невелика різниця – у перших частіше зустрічаються заражені файли MS Office, у других у списку є унікальні звірі – шкідливі Android-додатка.

Найчастіше вирусописувачі використовують хмарні сховища не як платформу для поширення, а в якості хостингу для шкідливих програм – у ході дослідження ми не зустріли жодного хробака або бекдора (не вважаючи DropSmack), спеціально націленого на хмарні файлові сховища. Звичайно, самі сервіси намагаються активно боротися зі шкідливими програмами, які займають вільне місце в хмарі. Крім того, хостинг шкідливих програм негативно впливає на репутацію сервісу, хоча формально хмарні сервіси й не несуть відповідальності за те, які файли завантажуються клієнтами в сховище. Очевидно, що регулярне сканування всіх файлів, що втримуються в хмарі, зажадає занадто багато ресурсів, які сервісам вигідніше використовувати для зберігання даних.

Підсумком проведеного дослідження стало розуміння, що ризик зараження корпоративної мережі через хмарне сховище порівняно невеликий – протягом року заразитися ризикує 1 з 1000 корпоративних користувачів, що використовують хмарні сервіси. Однак треба враховувати, що в деяких випадках навіть одиначне зараження комп'ютера в корпоративній мережі може привести до значного збитку.

Можливі міри захисту корпоративної мережі:

- Підсилити захист в Firewall/IDS, заблокувати доступ до серверів відомих сервісів. Більшим мінусом такого підходу є більша ресурсоемність – необхідно уважно стежити, чи не з'явилися нові кандидати в «чорний список».

- Установити багатофункціональний Security Suite, що включає в себе евристичний і поведінковий антивірус, функції обмеження доступу (HIPS), контроль за роботою операційної системи (System Watcher або Hypervisor), захист від експлуатації уразливостей і т.д. При цьому необхідно ретельно все настроїти.

- Тому що навіть самий напередуманий Security Suite може пропустити АРТ, варто звернути увагу на технологію Контроль додатків (у режимі «Заборонено за замовчуванням»). Це, мабуть, один із самих надійних засобів, що дозволяє заблокувати будь-яке невідоме ПЗ (у тому числі розповсюджене в ході цільової атаки). Саме складне завдання, що виникає під час впровадження Контролю додатків, – настроїти відповідні правила, щоб всі дозволені додатки запускалися й оновлювалися без проблем. Для цього виробниками продуктів з функцією Контролю додатків були розроблені спеціальні інструменти – функція відновлення ПЗ через довірені програми відновлення, передвстановлені списки білого ПЗ, що включають всі можливі системні й користувацькі файли, доступ до величезних хмарних сервісів і баз інформації про все різноманіття білого ПЗ.

- В особливих випадках, варто використовувати «Контроль додатків», щоб обмежити використання хмарних клієнтів у корпоративній мережі, тобто дозволити запуск додатків синхронізації «хмарної» папки тільки довіреним співробітникам.

Ну, а для самих-самих закритих систем, таких, які управляють роботою електростанцій, систем водопостачання, зберігають держтайну або дозволяють запускати міжконтинентальні ракети – настійно рекомендуємо повністю відмовити від використання хмарних файлових сховищ.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів виявлення уразливих додатків у мережевих Cloud-сервісах. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем виявлення уразливих додатків у мережевих Cloud-сервісах.
- Досліджена система виявлення уразливих додатків у мережевих Cloud-сервісах.
- На основі отриманих результатів досліджень створена програмна реалізація системи виявлення уразливих додатків у мережевих Cloud-сервісах. Розроблені алгоритми дозволяють успішно вирішувати завдання виявлення уразливих додатків у мережевих Cloud-сервісах. 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., 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., 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, 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 ґешування 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 ґешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Вісник Хмельницького національного університету. Серія: «Технічні науки», № 2 (307). С. 46-52. 2022.
32. 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.

УДК 004

С.Главнов, магістр гр. КІ-24М,

Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ МЕРЕЖЕВОЇ SIEM ДЛЯ АНАЛІЗУ ЗАГРОЗ БЕЗПЕЦІ КОРПОРАТИВНОЇ ІТ-ІНФРАСТРУКТУРИ

У статті розроблено програмне забезпечення, яке призначено для системи мережевої SIEM для аналізу загроз безпеці корпоративної ІТ-інфраструктури. Метою розробки є дослідження та принципи побудови системи мережевої SIEM для аналізу загроз безпеці корпоративної ІТ-інфраструктури. Об'єктом дослідження є процес мережевої SIEM для аналізу загроз безпеці корпоративної ІТ-інфраструктури. Предметом дослідження є методи мережевої SIEM для аналізу загроз безпеці корпоративної ІТ-інфраструктури. Методи дослідження базуються на методах захисту інформації у мережі, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи мережевої SIEM для аналізу загроз безпеці корпоративної ІТ-інфраструктури. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

SIEM, аналіз загроз безпеці, корпоративна ІТ-інфраструктура

Постановка проблеми. Мережі вашої організації є основною інфраструктурою для ваших інформаційно-технологічних (ІТ) систем, операційних технологій (ОТ) та промислових систем управління (ІКС). Тому важливо забезпечити безпеку вашої мережевої інфраструктури, щоб захистити вашу організацію від порушень, вторгнень та інших кіберзагроз. Мережеве ведення журналу та моніторинг подій безпеки допоможуть вам:

- захистити свою мережеву інфраструктуру;
- визначити індикатори компрометації (IoCs);
- своєчасно вживати коригувальних заходів;
- мінімізувати вплив у разі виникнення інциденту безпеки.

Рішення SIEM об'єднує функції моніторингу та ведення журналу. Термін SIEM вперше був введений Gartner у 2005 році для опису комбінації наступних підходів:

- управління інформацією безпеки (SIM), що стосується діяльності, пов'язаної зі збором даних, таких як файли журналів, з кількох джерел у централізоване сховище;
- управління подіями безпеки (SEM), що стосується діяльності, пов'язаної з моніторингом та аналізом конкретних подій безпеки в режимі реального часу, які можуть бути тривожними сигналами.

Традиційно, SIEM-рішення здебільшого пропонували захист для локальних середовищ з обмеженими джерелами даних та можливостями. SIEM-рішення еволюціонували, і SIEM наступного покоління пропонують більше можливостей для боротьби з передовими кіберзагрозами та обробки величезних обсягів даних. Зараз доступно багато хмарних SIEM-рішень, які можуть захищати активи як локально, так і в хмарі.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи мережевої siem для аналізу загроз безпеці корпоративної іт-інфраструктури.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи мережевої SIEM для аналізу загроз безпеці корпоративної ІТ-інфраструктури.

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

- Огляд існуючих систем мережевої SIEM для аналізу загроз безпеці корпоративної IT-інфраструктури.

- Дослідження системи мережевої SIEM для аналізу загроз безпеці корпоративної IT-інфраструктури.

- Програмна реалізація системи мережевої SIEM для аналізу загроз безпеці корпоративної IT-інфраструктури.

Об'єктом дослідження є процес мережевої SIEM для аналізу загроз безпеці корпоративної IT-інфраструктури.

Предметом дослідження є методи мережевої SIEM для аналізу загроз безпеці корпоративної IT-інфраструктури.

Методи дослідження базуються на методах захисту інформації у мережі, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Рішення SIEM наступного покоління включають такі технології для виявлення складних загроз та горизонтального переміщення, а також для автоматизації реагування на інциденти:

Аналіз поведінки користувачів та об'єктів

Аналітика поведінки користувачів та об'єктів (UEBA) використовує алгоритми та машинне навчання для виявлення аномальних моделей поведінки користувачів та пристроїв (наприклад, маршрутизаторів, серверів та кінцевих точок) у мережі. UEBA дозволяє вашій організації виявляти ширший спектр кіберзагроз, таких як атаки методом перебору, розподілені атаки відмови в обслуговуванні (DDoS) та внутрішні загрози.

Оркестрація безпеки та автоматизоване реагування

Оркестрація безпеки та автоматизація реагування (SOAR) допомагають координувати та автоматизувати реагування на виявлені загрози за допомогою автоматизованих сценаріїв або робочих процесів. Вони також використовують штучний інтелект. (Штучний інтелект) вивчає моделі поведінки, щоб передбачати подібні загрози до їх виникнення.

Переваги SIEM-рішень

Рішення SIEM може допомогти керувати ризиками кібербезпеки вашої організації, підтримуючи виявлення загроз, дотримання вимог та управління інцидентами безпеки. Рішення SIEM дозволяють вашій команді безпеки:

- керувати безперервним надходженням даних журналів з багатьох різних джерел:
 - допомагає зменшити вартість окремих інструментів, що використовуються різними групами у вашій організації;
 - централізує дані журналів в одному сховищі;
- співвідносити та аналізувати великі обсяги даних, щоб мати змогу проактивно виявляти потенційні загрози, оскільки вони залишають сліди в різних джерелах журналів;
- автоматизувати завдання безпеки, щоб зменшити навантаження аналітиків безпеки шляхом автоматизації повторюваних завдань;
- отримувати автоматичні сповіщення та відповідні дії за допомогою автоматичного тригера на основі конкретних випадків використання для забезпечення швидкого реагування на інциденти;
- отримуйте дані в режимі реального часу по всій організації, щоб допомогти вашій організації швидко виявляти та усувати сліпі зони вразливостей у вашій мережі;
- пошук історичних даних журналів для різних мережеских вузлів та періодів часу для підтримки аналізу першопричин та виявлення інцидентів після того, як стався витік;
- генерувати звіти для аудиторів, щоб продемонструвати дотримання нормативних вимог та виявляти потенційні порушення на ранній стадії, щоб їх можна було усунути;
- переглядати інформаційні панелі управління, які відображають дані про події в інформаційних діаграмах, щоб побачити закономірності незвичайної діяльності:

○ допомагає вашій організації визначити пріоритети ресурсів для першочергового вирішення найважливіших загроз.

Рішення SIEM дозволяють вашій організації автоматизувати впровадження, оцінку та постійний моніторинг засобів контролю безпеки. Згідно зі спеціальною публікацією (SP) 800-137 Національного інституту технологічних стандартів (NIST), технології SIEM можуть допомогти організаціям автоматизувати багато специфічних засобів контролю безпеки. Ці технічні, операційні та управлінські засоби контролю безпеки описані в документі Кіберцентру «Управління ризиками безпеки IT : підхід життєвого циклу» (ITSG-33).

– Технічні засоби контролю безпеки:

- AC-5 Розподіл обов'язків;
- AU-2 Події, що підлягають аудиту;
- AU-6 Аудиторський огляд, аналіз та звітність;
- Скорочення аудиту AU-7 та створення звітів.

– Контроль операційної безпеки:

- Моніторинг інцидентів IR-5;
- PE-6 Моніторинг фізичного доступу;
- Моніторинг інформаційної системи SI-4.

– Контроль безпеки управління:

- Оцінювання безпеки CA-2;
- Безперервний моніторинг CA-7;
- Оцінка ризиків RA-3;
- Сканування вразливостей RA-5.

Хмарні SIEM-рішення

У сфері кібербезпеки перехід до хмарних SIEM-рішень змінює те, як організації керують своїми даними та взаємодіють з ними. У звіті Gartner за 2023 рік було оцінено, що до кінця року 90% SIEM-рішень пропонуватимуть можливості виключно в хмарі. На відміну від традиційних локальних SIEM-рішень, які вимагають спеціалізованого апаратного та програмного забезпечення у власній інфраструктурі організації, хмарне SIEM-рішення розміщується на серверах, що обслуговуються стороннім постачальником хмарних послуг (CSP).

Хмарні SIEM-рішення дозволяють вашій організації перекласти більшу частину управління інфраструктурою на постачальника послуг зв'язку (CSP) та зосередитися на використанні вашої системи для досягнення ваших цілей безпеки. На практиці це означає, що журнали даних з мережевих пристроїв та систем вашої організації збираються, передаються в хмару та безпечно зберігаються на серверах CSP.

Після цього ваша організація може взаємодіяти з вашими даними через веб-інтерфейсабо інтерфейс прикладного програмування (API), що надається постачальником послуг криптографії (CSP). Цей API зазвичай містить набір інструментів для аналізу даних, візуалізації та звітності. Це дозволяє вашій організації виконувати складну аналітику для виявлення, розслідування та реагування на інциденти безпеки.

Хмарні SIEM-рішення часто оснащені можливостями машинного навчання та штучного інтелекту для кращого виявлення аномалій та потенційних загроз. Це відбувається в режимі реального часу та у великих масштабах, надаючи організаціям потужний, гнучкий та ефективний інструмент для управління своєю кібербезпекою.

Типи хмарних пропозицій

Існує два типи пропозицій для хмарних SIEM-рішень: керовані та некеровані.

Керований

Це ближче до моделі «SIEM як послуга», де постачальник SIEM-рішення відповідає за хмарну інфраструктуру та її обслуговування. Постачальник SIEM-рішення також надає клієнту послуги моніторингу інцидентів у режимі реального часу та виявлення загроз. Клієнт зазвичай має менше контролю над управлінням життєвим циклом SIEM-рішення, оскільки це

є відповідальністю постачальника. Хоча керовані рішення можуть бути дорожчими, вони знімають з клієнта тягар впровадження та обслуговування SIEM-рішення.

Некерований

Клієнт відповідає за створення, підтримку, усунення несправностей та управління життєвим циклом усіх компонентів SIEM-рішення. Третя сторона може надавати додаткову допомогу, але загалом клієнт несе відповідальність за доступність SIEM-рішення та стабільність. Некеровані рішення можуть бути підходящим варіантом для організацій з високочутливими активами, яким потрібен повний контроль над своїм SIEM-рішенням.

Переваги хмарних SIEM-рішень

Хмарні SIEM-рішення можуть забезпечити вашій організації кілька переваг.

Масштабованість та гнучкість

У міру зростання вашої організації або коливань попиту, хмарні рішення можуть адаптуватися до ваших потреб. Така масштабованість також означає, що ви платите лише за те, що використовуєте, що може бути економічно вигідним вибором для багатьох компаній.

Зменшення операційних накладних витрат

Завдяки локальному рішенню SIEM ваша організація відповідає за обслуговування апаратного та програмного забезпечення, що може бути ресурсомістким. Хмарні рішення SIEM перекладають значну частину цієї відповідальності на постачальника послуг зв'язку (CSP). Це дозволяє вашій команді безпеки зосередитися на стратегічних завданнях, а не на обслуговуванні.

Аналітика

Хмарні SIEM-рішення часто включають комерційну готову аналітику (COTS), специфічну для CSP. Ця аналітика розроблена для оптимальної роботи в інфраструктурі постачальника послуг, потенційно пропонуючи покращені можливості виявлення загроз та аналізу даних. Наявність цієї аналітики може покращити можливості вашої організації щодо кіберзахисту, використовуючи спеціалізовані знання та ресурси постачальника.

Недоліки хмарних SIEM-рішень

Хоча хмарні SIEM-рішення можуть запропонувати багато переваг вашій організації, вам слід знати про потенційні недоліки.

Проблеми конфіденційності даних

Коли ви використовуєте хмарне SIEM-рішення, ваші дані зберігаються на серверах постачальника послуг зв'язку (CSP). Перш ніж переходити на хмарне рішення, переконайтеся, що ви повністю розумієте та знайомі з методами обробки та зберігання даних вашого постачальника.

Зафіксованість постачальника

Перехід на хмарне SIEM-рішення може призвести до прив'язки до постачальника, тобто до ситуації, коли важко або дорого перейти до іншого постачальника або повернутися до локального рішення. Багато хмарних сервісів є власністю CSP, що може ускладнити перенесення даних. Перш ніж вибрати хмарне SIEM-рішення, переконайтеся, що ви розумієте умови надання послуг, зокрема, що передбачає зміна постачальників.

Вартість

Хмарні SIEM-рішення можуть забезпечити економію коштів, особливо з точки зору обслуговування та інфраструктури, але вони також можуть збільшити витрати. Це особливо актуально, якщо ваша організація використовує багато даних, оскільки багато CSP стягують плату залежно від обсягу оброблених даних.

Безпечне розгортання та експлуатація SIEM-рішень є життєво важливими. SIEM-рішення слід розглядати як систему вищої цінності, таку як адміністративний контроль або контроль доступу системи. Через свою роль у моніторингу та виявленні інцидентів безпеки, слід приділяти особливу увагу забезпеченню безпеки як продукту, так і постачальника. У разі виникнення вразливості нульового дня, а також через чутливість даних та рівень доступу до рішення SIEM, Кіберцентр вважає за потрібне розробляти архітектуру SIEM на основі рішень кількох постачальників, а не бути прив'язаним до одного. Такий підхід покращує

загальний рівень безпеки, зменшуючи ризики, пов'язані з вразливостями, характерними для певних постачальників.

Неправильно впроваджене SIEM-рішення може призвести до більшої кількості хибнопозитивних результатів, виявлення більшої кількості «аномальних» подій та генерування додаткових, некорисних сповіщень. Це може створювати навантаження на ресурси вашої команди кібербезпеки. Впроваджуючи наведені нижче найкращі практики, ваша організація може отримати максимальну користь від вашого SIEM-рішення.

Загальні рекомендації

- Визначення варіантів використання для моніторингу, оповіщення та аудиту:
 - З цих випадків використання визначте джерела журналів, які потрібно отримати та проаналізувати.
 - Розгляньте можливість проведення перевірки концепції (POC), щоб оцінити, чи підходить SIEM-рішення для вашого середовища:
 - Налаштуйте POC у тестовому середовищі, яке базується на чітко визначених сценаріях користувачів і є репрезентативною підмножиною вашої інфраструктури та даних.
 - Визначте свої найважливіші ресурси, такі як дані та пристрої, і налаштуйте SIEM-рішення для їх моніторингу.
 - Налаштуйте відповідний моніторинг джерел журналів та сповіщення, щоб отримувати сповіщення про проблеми зі збиранням журналів.
 - Оцініть, скільки даних ви хочете зібрати, щоб отримати повне уявлення про вашу мережу.
 - Як мінімум, вам слід збирати дані журналу про:
 - транзакції авторизації (успішні та невдалі спроби);
 - зміни привілеїв користувачів, включаючи зміни облікових записів користувачів (зокрема створення та видалення), зміни членства в групах та механізмів автентифікації (паролі та багатофакторна конфігурація), а також додавання або видалення привілейованого доступу;
 - помилки програми;
 - процеси згоди, такі як умови та положення;
 - дії, що виконуються всіма користувачами з правами адміністратора;
 - реєстрація нових пристроїв в інфраструктурі, включаючи будь-які мобільні телефони та персональні пристрої, що дозволяють використовувати власні пристрої.
 - Запобігайте збору конфіденційних даних вашим SIEM-рішенням, таких як:
 - фінансова інформація (наприклад, банківські записи або дані кредитної картки);
 - персональну інформацію (наприклад, ідентифікаційний номер, виданий урядом);
 - паролі та ключі шифрування;
 - Зрозумійте вимоги до дотримання вимог вашого бізнесу та налаштуйте SIEM-рішення відповідно до них.
 - Регулярно перевіряйте та тестуйте своє SIEM-рішення, щоб переконатися, що воно правильно налаштоване на основі впроваджених заходів безпеки та політик.
 - Розробіть план реагування на інциденти, щоб ваша організація була готова належним чином впоратися з подією, коли трапляється інцидент безпеки:
 - Для отримання додаткової інформації зверніться до нашої публікації «Розробка плану реагування на інциденти» (ITSAP.40.003).
 - Синхронізуйте всі мережеві пристрої з центральним сервером часу, щоб гарантувати, що записані журнали аудиту використовують одне й те саме джерело часу;
 - Налаштуйте щонайменше 3 сервери часу для полегшення обслуговування та усунення несправностей.
 - Підпишіться на зовнішні канали загроз і створюйте сповіщення на основі даних, що надсилаються, регулярно оновлюйте логіку виявлення для виявлення нових загроз:

○ Кіберцентр надає ІоС організаціям, включаючи партнерів у канадській критичній інфраструктурі, через автоматизовану систему під назвою AVENTAIL, яку можна інтегрувати безпосередньо у вашу SIEM.

Дані журналу якості

Щоб ваша організація отримувала найкориснішу інформацію про діяльність у вашій мережі, переконайтеся, що високоякісні дані журналів надходять до вашого інструменту SIEM.

Виберіть відповідні методи збору журналів

Рішення SIEM можуть збирати та зберігати журнали безпеки з різних джерел. Визначте, який метод збору журналів підходить для потреб вашої організації.

– Потік журналів: Пристрої генерують журнали та надсилають їх безперервним потоком до колектора журналів рішення SIEM. Це забезпечує рішення SIEM інформацією в режимі реального часу.

– Надсилання журналів: Пристрій автоматично збирає журнали та надсилає (завантажує) їх безперервно або через регулярні проміжки часу до колектора журналів рішення SIEM. Колектор журналів налаштовано на прийом журналів у певному форматі та за певним протоколом (syslog, FTP тощо).

– Збір журналів: Як і при надсиланні журналів, цей метод використовує збирач журналів рішення SIEM для ініціювання підключення та запиту журналів. Цей метод часто використовується для збору журналів на рівні операційної системи за допомогою програмного агента.

Перегляд та оновлення аналізаторів журналів

Різні системи генерують журнали в різних форматах. Деякі формати журналів мають чітко визначену структуру та їх легко використовувати в SIEM-рішеннях, тоді як інші формати журналів менш узгоджені та складніші для аналізу та обробки в SIEM-рішеннях. Переконайтеся, що вибране вами SIEM-рішення може зрозуміти отримані журнали.

Формати журналів також можуть змінюватися з часом (наприклад, після оновлень програмного забезпечення), що може призвести до того, що SIEM не зможе аналізувати та індексувати журнали з певного джерела. Регулярно переглядайте аналізатори журналів та оновлюйте їх за потреби.

Правильне керування сховищем журналів

Дані журналів, отримані рішенням SIEM, зберігаються відповідно до налаштованих політик зберігання. Журнали можна надсилати до сховища для архівування або до механізму кореляції рішення SIEM, де вони будуть проаналізовані та зіставлені з іншими журналами. Така кореляція може надати важливу інформацію вашій IT-команді.

Залежно від обраного вами рішення SIEM, журнали можуть зберігатися або в отриманому вигляді, або у стиснутому форматі. Оскільки пошук стиснутих журналів займає більше часу, деякі рішення SIEM зберігають останні журнали в нестиснутому форматі. Після певного часу журнали стискаються, щоб зменшити використання пам'яті.

SIEM-рішення можуть отримувати тисячі журналів щосекунди, тому зберігання нестиснених журналів протягом тривалого періоду може призвести до високих витрат на зберігання. Якщо SIEM-рішення зберігає журнали в хмарі, витрати на зберігання також можуть значно зрости.

Видалення журналів після того, як вони більше не мають цінності, допоможе зменшити витрати на зберігання та продуктивність. Журнали, обсяг яких перевищує політику зберігання, можна відкинути або зберігати в дешевших рішеннях.

Зберігання даних журналу

Політики зберігання журналів можуть допомогти контролювати потреби в сховищі. Розробляючи політику зберігання журналів вашої організації, ретельно обміркуйте, як довго слід зберігати журнали безпеки. Як загальне правило, ми рекомендуємо зберігати важливі журнали вашої організації щонайменше 6 місяців. Для більш критичних журналів розгляньте період зберігання 13 місяців.

Термін зберігання залежатиме від вашого:

- галузеві стандарти організації;
- нормативні акти та закони;
- конкретні проблеми кібербезпеки, унікальні для вашого бізнес-середовища;
- витрати на зберігання та доступність;

Багато компрометацій виявляються через довгий час після того, як стався витік. Згідно з публікацією IBM «Вартість звіту про витік даних за 2023 рік», середній час виявлення витоку становив 204 дні. Якщо у вашій організації стався витік, ваші журнали є важливим доказом, який допоможе вам виявити та розслідувати інцидент. Ретельно розробляйте політику зберігання журналів та періодично переглядайте її, щоб перевірити, чи потрібні коригування та чи зберігаються ваші журнали протягом належного часу.

Активация індексації найчастіше шуканих полів

Журнали з різних типів джерел містять різну інформацію та використовують різні формати. Рішення SIEM використовують аналізатори журналів для розуміння форматів журналів та інформації, яку вони містять. Це може включати сам журнал, інформацію про дату та час, а також розташування імені користувача або імені машини в потоці журналів. Ці поля можна індексувати, що призведе до швидшого пошуку.

Індексування журналів пришвидшує пошук, але вимагає додаткових ресурсів сховища та центрального процесора (CPU), що може вплинути на продуктивність рішення SIEM. Ми рекомендуємо індексувати лише ті поля, які часто шукаються.

Рішення SIEM повинно надавати інформацію про пошукові запити, зокрема, які поля шукаються та чи індексуються ці поля. Використовуючи цю інформацію, адміністратор SIEM може активувати або деактивувати індексацію залежно від того, як часто виконується пошук у полях.

Нормалізувати дані журналу

Нормалізація журналів важлива для кореляції подій та розслідування інцидентів. Рішення SIEM може отримувати журнали в різних форматах. Наприклад, ваша мережа може мати пристрої в різних часових поясах, деякі журнали можуть використовувати 12-годинний формат, а інші – 24-годинний, або журнали Active Directory (AD) можуть містити імена користувачів, тоді як хмарні журнали відображають адресу електронної пошти користувача як його ім'я користувача.

Рішення SIEM повинно мати можливість нормалізувати якомога більше полів, щоб обмежити кількість рядків пошуку, що вказують на одного й того ж користувача або ресурс. Під час розслідування інцидентів пошук подій, що відбулися протягом певного періоду, повинен повертати журнали з усіх пристроїв, незалежно від часового поясу, на який налаштовано рішення SIEM.

Налаштування правил кореляції та порогових значень

Кореляція подій стосується аналізу подій у бізнес-контекстах та встановлення зв'язків між ними на основі набору попередньо визначених правил. Ці правила дозволяють вашому SIEM-рішенню визначати, які підозрілі дії слід розглядати як потенційні загрози безпеці. Для точного виявлення інцидентів механізм кореляції SIEM-рішення має бути налаштований належним чином. Налаштуйте правила кореляції та встановіть порогові значення на основі конкретних випадків використання або бізнес-потреб вашої організації. Ви можете почати зі стандартних правил конфігурації SIEM-рішення та деактивувати й активувати параметри відповідно до того, що ви хочете корелювати.

Архітектура нульової довіри

Термін «нульова довіра» (ZT) являє собою систему безпеки для захисту інфраструктури та даних. Центральний принцип ZT полягає в тому, що жоден суб'єкт (додаток, користувач чи пристрій) в інформаційній системі не є довіреним за замовчуванням. Довіра має оцінюватися та перевірятися щоразу, коли суб'єкт запитує доступ до нового ресурсу. Ступінь наданого доступу динамічно коригується залежно від рівня довіри, встановленого з суб'єктом. ZT передбачає прийняття нового підходу до безпеки, завжди

припускаючи порушення та зосереджуючись на захисті ресурсів (наприклад, послуг та даних). Архітектура нульової довіри (ZTA) – це корпоративний підхід до проектування систем, у яких безпека базується на принципах ZT. У стандарті NIST SP 1800-35B «Впровадження архітектури нульової довіри» описано приклади рішень для впровадження ZTA. Ці рішення припускають, що технологія SIEM є однією з базових функцій кібербезпеки організації, можливості якої поступово додаються в міру розвитку ZTA. Рішення SIEM підтримують впровадження ZTA, оскільки зібрані ними дані можуть бути використані в механізмі політик ZTA для прийняття рішень щодо динамічного доступу.

Великі організації та підприємства стикаються з постійно мінливим ландшафтом кіберзагроз. Щоб пом'якшити атаки з боку передових зловмисників, ваша організація повинна інвестувати в інструменти безпеки, які надають аналітику активності у вашій мережі в режимі реального часу. Інструменти кібербезпеки, такі як рішення SIEM, можуть забезпечити вам єдиний інтерфейс для отримання цієї аналітики. Рішення SIEM може допомогти вашій організації виявляти, аналізувати та реагувати на кіберзагрози, перш ніж вони порушать вашу бізнес-операцію. Як і у випадку з будь-яким важливим IT- рішенням, вам слід зважити всю інформацію, представлену в цій публікації, з урахуванням конкретних потреб та обставин вашої організації, щоб визначити, чи є рішення SIEM найкращим для вас.

Інтеграція сканера уразливостей з SIEM дозволяє сполучити кілька методів виявлення погроз і значно підвищити ймовірність своєчасного виявлення. Приміром, SIEM може виявити аномалію через baseline, але без інформації про те, що на активі є уразливість, SIEM не зможе сказати, із чим саме ця аномалія зв'язана. При наявності відомостей від сканера уразливості, SIEM зможе зробити вивід про те, що виробляється експлуатація уразливості. Маючи інформацію про уразливість, а також про критичність активів від сканера уразливостей, система SIEM здатна пріоритизувати інциденти по їхній критичності. Це дозволить у першу чергу реагувати на значимі інциденти, важливі для бізнесу

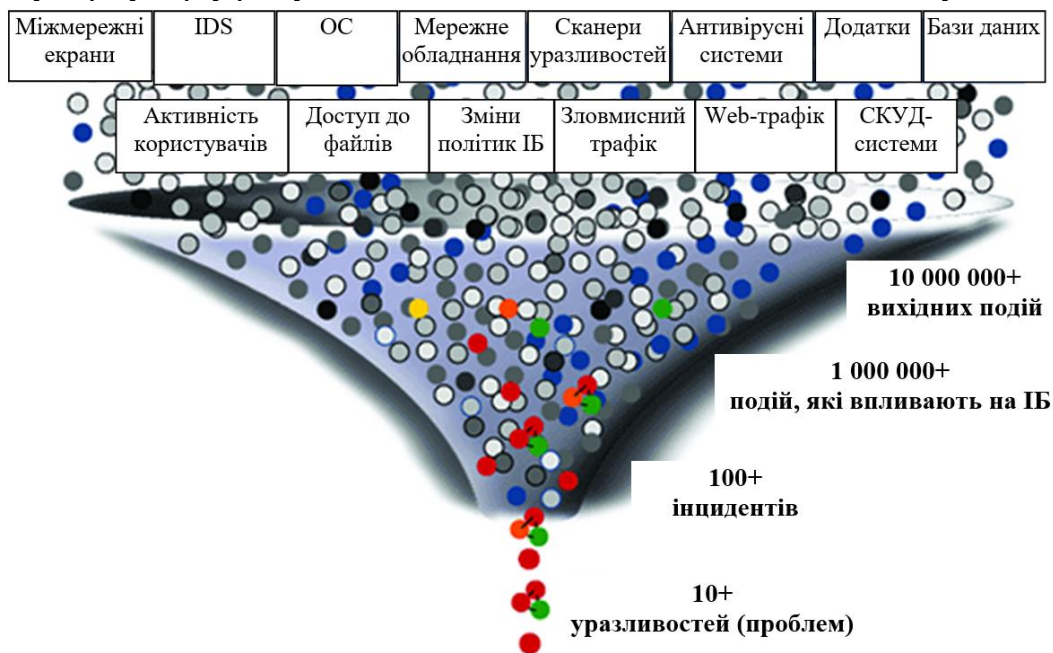


Рисунок 1 – Структурна схема системи

Сканер уразливостей є відмінним постачальником інвентаризаційної інформації для SIEM, наприклад, про версії програмного забезпечення і його конфігурацій. Ця інформація може використовуватися при виявленні інциденту, при з'ясуванні причин його виникнення. Використання убудованого в SIEM механізму перевірки відповідності внутрішнім політикам і високорівневим стандартам без інтеграції зі сканером уразливостей не дає повноцінної картини, тому що використовується дуже мала частка технічних вимог.

Жоден джерело не надасть більше детальної й повної інформації про наявність уразливості й про можливість її експлуатації (з урахуванням топологічної структури мережі й конфігурацій) краще, ніж сканер уразливостей. Уразливість може бути присутнім, але бути при цьому неексплуатований (закритий мережний порт, зупинена служба, на активному мережному встаткуванні організована VLAN або правилами міжмережного екрана заблокований трафік на даний порт). Інформація про це може істотно знизити залишкові ризики, допоможе витратити кошти на дійсно необхідні засоби захисту, а також виключити помилкові інциденти.

Процес керування конфігураціями, що так складно реалізувати, стає простим при використанні зв'язування SIEM і сканера уразливостей. Ви можете аналізувати, що змінилося, ким і коли були зроблені зміни, а також можете автоматично оцінити, на що вони вплинули. Для цього необхідно лише скласти найпростіші правила кореляції в SIEM і налаштувати параметри переданої інформації від сканера; всю іншу логіку здійснить сама система SIEM. Природно, що чим більше ефективних джерел інформації в SIEM, тим більше ймовірність виявлення погрози на ранній стадії її виникнення. Ви можете використовувати SIEM або сканер уразливостей окремо. Але описане зв'язування значно мінімізує ризики.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів мережевої SIEM для аналізу загроз безпеці корпоративної IT-інфраструктури. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем мережевої SIEM для аналізу загроз безпеці корпоративної IT-інфраструктури.
- Досліджена система мережевої SIEM для аналізу загроз безпеці корпоративної IT-інфраструктури.
- На основі отриманих результатів досліджень створена програмна реалізація системи мережевої SIEM для аналізу загроз безпеці корпоративної IT-інфраструктури. Розроблені алгоритми дозволяють успішно вирішувати завдання мережевої SIEM для аналізу загроз безпеці корпоративної IT-інфраструктури. 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., 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.
2. 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.
3. 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.
4. 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.
5. Smirnov, O., Neskoriy, T., Fedorov, E., Rudakov, K., Neskoriy, A. «Method Detection Audit Data Anomalies on Basis Restricted Cauchy Machine» CEUR Workshop Proceedings, Volume 3187, 2022,
6. 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.
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 гешування 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 гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 1(67). С. 84-89.
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., 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.
14. 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.
15. 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.
16. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
17. 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.
18. 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.
19. 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.
20. 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.
21. 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.
22. 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.
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., 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.
26. 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.
27. 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.
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

М.Грищенко, магістр гр. КІ-24М,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ МЕРЕЖЕВОГО АНТИВІРУСНОГО КОМПЛЕКСУ ДАТА-ЦЕНТРУ

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

мережа, антивірус, дата-центр

Постановка проблеми. Масове використання комп'ютерів, а також швидкий розвиток комп'ютерних мереж (зокрема мережі Інтернет) сприяли появі й поширенню шкідливих програм – комп'ютерних вірусів. Віруси часом роблять роботу на комп'ютері неможливою. Вони, залежно від ситуації, можуть завдати значної шкоди як інформації, так і самому комп'ютеру.

Незважаючи на поширену думку, центри обробки даних не є «куленепробивними» від хакерських атак. Ви можете бути в більшій небезпеці, якщо володієте сервером, оскільки кіберзлочинці нападуть на вас з усією силою. На ринку є чимало антивірусних продуктів, але не всі вони підходять для центру обробки даних. Гарна новина полягає в тому, що з найкращим антивірусом ви можете перестати турбуватися про будь-які зовнішні загрози.

Іншими словами, центр обробки даних – це обладнання, яке зберігає інформацію (для бізнесу, урядів тощо). Крім того, той факт, що до цих даних можна отримати доступ з будь-якого куточка світу, перетворює центри обробки даних на корисний інструмент. Усі уповноважені сторони можуть отримати ту саму інформацію, фактично не відвідуючи місцезнаходження центру обробки даних. Однак, оскільки інформація вільно передається між різними комп'ютерами, це полегшує злочинцям її отримання.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи мережевого антивірусного комплексу дата-центру.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи мережевого антивірусного комплексу дата-центру.

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

- Огляд існуючих систем мережевого антивірусного комплексу дата-центру.
- Дослідження системи мережевого антивірусного комплексу дата-центру.
- Програмна реалізація системи мережевого антивірусного комплексу дата-центру.

Об'єктом дослідження є процес мережевого антивірусного комплексу дата-центру.

Предметом дослідження є методи мережевого антивірусного комплексу дата-центру.

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

Виклад основного матеріалу. Класифікація комп'ютерних вірусів

Вся наявна розмаїтість комп'ютерних вірусів можна класифікувати по різних ознаках, – наприклад по середовищу перебування, по руйнівних можливостях, по особливостях побудови й т.д.

За способом зараження:

– резидентні – віруси, що залишають в оперативній пам'яті свою резидентну (постійну) частину, що потім перехоплює звертання до програм, що заражаються, і впроваджується в них;

– нерезидентні – віруси, які не заражають оперативну пам'ять і проявляються лише при запуску інфікованої програми.

По цілісності:

– монолітні – віруси, програми яких являють собою єдиний блок;

– розподілені – віруси, програми яких розділені на частини, що містять інструкцію з відтворення вірусу (наприклад, одна якась частина заражає комп'ютер, а потім завантажує з Інтернету інші частини, що виконують шкідливу дію).

Інші шкідливі програми

Крім розглянутих вище комп'ютерних вірусів, існують і інші види шкідливих програм. Серед них, наприклад, можна назвати:

– мережні хробаки – шкідливі програми, які поширюються по комп'ютерних мережах, обчислюючи адреси мережних комп'ютерів і розсилаючи по цих адресах свої копії;

– троянські програми («троянські коні», квазивіруси) – шкідливі програми, які не здатні до самопоширення, а маскуються під якусь корисну або цікаву програму, руйнують завантажувальний сектор і файлову систему або збирають і пересилають своєму творцеві інформацію, що не підлягає розголошенню (наприклад, ваші особисті паролі);

Антивірусні програми

Антивірусні програми призначені для захисту комп'ютерів від більшості вірусів, хробаків і «троянських коней», які можуть видаляти файли, одержувати доступ до особистих даних або використовувати заражену систему як засіб атаки на інші комп'ютери.

Антивірусні програми звичайно використовують два різних методи для виконання своїх завдань:

1) сканування (перегляд) файлів для пошуку вже відомих вірусів, для яких у вірусній базі (щовходить у комплект антивірусної програми спеціальної БД) є інформація про характерні фрагменти вірусного програмного коду (сигнатурах вірусів);

2) виявлення підозрілого поведіння будь-якої програми, що схоже на поведінку зараженої програми («евристичне сканування»).

Антивірусне програмне забезпечення складається з пакета програм, які виявляють, запобігають розмноженню й видаляють комп'ютерні віруси й інші шкідливі програми.

При виборі антивірусної програми необхідно враховувати наступні параметри, яким антивірус повинен відповідати:

1. Сталість і надійність роботи. Цей параметр є визначальним. При стабільній роботі антивірусної програми немає відчуття, що якісь заражені файли залишилися непоміченими.

2. Великий обсяг і постійне відновлення вірусної бази. Сюди ж ставиться вміння програми швидко пізнавати види вірусів працювати з файлами різних типів (архівними, документами), і здійснювати автоматичну перевірку всіх нових файлів у міру їхнього копіювання.

3. Швидкість роботи антивірусу й додаткові функції. До додаткових функцій можна віднести наявність евристичного сканування й можливість лікування заражених файлів (коли віруси з них віддаляються, а файли приводяться у вихідний стан, що був до їхнього зараження).

4. Підтримка різних програмою багатьох операційних систем – багатоплатформеність. При роботі в мережному варіанті немаловажним є також наявність в антивірусної програми серверних модулів, призначених для адміністрування, і наявність можливості роботи на різних серверах.

Захист робочого столу

У минулому захист робочих столів був єдиною «сферою», де використовувалися антивіруси. Сьогодні він все ще має вирішальне значення для захисту центрів обробки даних, але має великий недолік. Річ у тім, що для його роботи кожен кінцевий користувач повинен регулярно оновлювати своє програмне забезпечення. Крім того, важко відстежувати їх усі, що наражає центр на небезпеку.

Сучасні антивіруси для комп'ютерів мають численні автоматичні сповіщення. Люди часто забувають про них, відкладають їх або ігнорують, що, знову ж таки, робить всю систему вразливою. Ось як працює захист комп'ютера: антивірус сканує диски та оперативну пам'ять (RAM), шукаючи шкідливий код у базі даних.

Також, щойно система виявляє потенційно небезпечний файл/програму, користувач отримує сповіщення. Далі користувач може вибрати одну з наступних дій: видалення вірусу, спроба очищення файлів/програм або поміщення їх у карантин. Це все, що вам потрібно знати про антивірусний захист робочого столу. Він не ідеальний, але й донині центри обробки даних включають його як надійний рівень захисту.

Захист сервера

У цьому випадку антивірусне рішення працює на рівні поштового сервера. Це означає, що більшість шкідливих кодів будуть знищені ще до того, як вони потраплять на комп'ютери користувачів. На жаль, навіть за наявності антивіруса, що захищає сервери, вірусам все ж вдається потрапити в мережу. Захист сервера так само важливий, як і захист робочого столу, але в більшості випадків він є «бонусом», і саме тому міжнародні компанії його використовують.

Якщо ви покладаєтеся лише на антивірус сервера, а шкідливе програмне забезпечення потрапляє на робочі столи, ніщо не завадить йому пошкодити/знищити конфіденційні бізнес-дані. Тому вам потрібно використовувати все це разом, включаючи наступний (і останній) захист – на рівні «шлюзу». Він працює подібно до захисту сервера, але має дещо інший підхід.

Захист шлюзу

Ідея полягає в тому, щоб зупинити шкідливе програмне забезпечення в найвіддаленішій точці, задовго до того, як воно отримає шанс досягти мережі. Поки віруси/пошкоджені повідомлення тримаються на відстані, вони не зможуть завдати жодної шкоди центру обробки даних. Шлюзи існують не так давно, але вони вже довели свою ефективність як захист на рівні серверів і робочих столів.

Інтеграція антивірусного програмного забезпечення в мережеве обладнання є серцем і душею підходу шлюзу. На рівні шлюзу антивірус сканує всі вхідні повідомлення, шукаючи будь-які потенційні загрози. Крім того, коли він виявляє заражені повідомлення, він або зупиняє їх, поміщає в карантин, або видаляє їх. На думку експертів, це прогресивне рішення є дуже перспективним і, найімовірніше, стане новою нормою в найближчі роки.

Завдяки інтегрованим продуктам, вбудованим безпосередньо в мережі, захист центрів обробки даних від зовнішніх загроз стане набагато комфортнішим. Вам слід знати, що уряди різних країн також використовують підхід «центр обробки даних/сервер», і це одна з причин, чому безпека кінцевих точок стає важливою частиною світу, в якому ми зараз живемо.

Антивірусний комплекс дата-центру – це не тільки антивірус і антишпиун. Він визначає й нейтралізує різні види небажаного ПЗ.

Основні переваги:

- Невимогливість до ресурсів – відмінно працює на настільних ПК, ідеальний для роботи на ноутбуках.
- Можливість установки на заражену машину й лікування ураженої системи.

- Коректна перевірка «на лету» вхідної й вихідної пошти по протоколах SMTP, POP3, IMAP, NNTP.
- Захист від шпигунських, рекламних програм, хакерських утиліт і програм-дозвонників.
- Висока частота відновлень вірусних баз – до декількох разів у годину! Відновлення виробляється з локальних серверів мережі.

Масове поширення комп'ютерних вірусів, а також активне обговорення в пресі планів інформаційної війни із залученням хакерів для придушення ворожих систем керування й передачі даних привели до того, що питання про створення засобів протидії й захисти здобуває нову якість. На думку ряду закордонних експертів, держава, що програла в інформаційній війні, буде відкинута у своєму розвитку на багато десятиліть.

Сьогодні вже ясно, що традиційні методи побудови систем захисту інформації не принесуть бажаного результату. Треба шукати принципово нові підходи до рішення цієї проблеми. Справжня стаття покликана дати «інформацію до міркування» для розроблювачів антивірусних систем, щоб вони змогли глянути на свою предметну область із іншої сторони, а саме – з боку Природи, що створила, напевно, саму зроблену систему захисту – імунну систему організму.

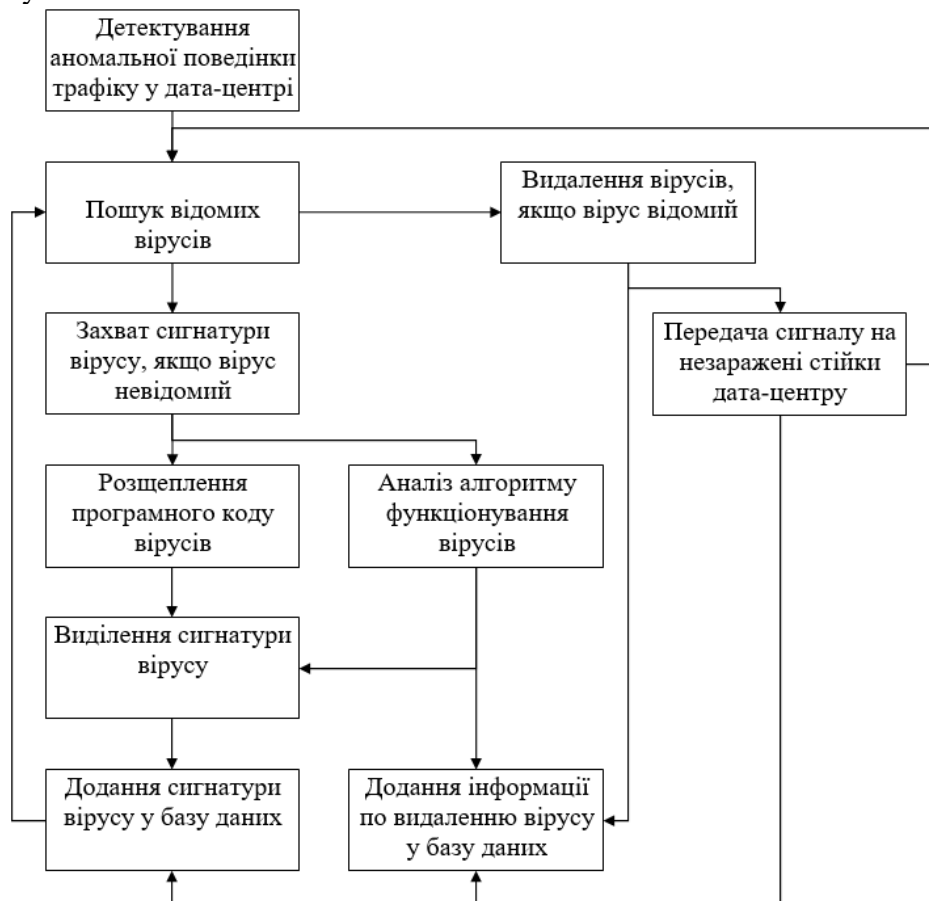


Рисунок 1 – Структурна схема системи

Уже розроблений ряд алгоритмів, що дозволяють писати віруси, які принципово не можна виявити жодним з існуючих способів. Багато хто відзначають, що самоідентифікуємий довільним образом код одержати просто неможливо. У кожному разі, є тверді рамки, які дозволяють ту саму операцію реалізувати обмеженим числом способів. Способи ці відомі заздалегідь, що, у принципі, дозволяє перелічити всі ключові фрагменти вірусів, а значить – безпомилково їх розпізнати.

Однак якщо припустити, що архітектура процесора може бути довільною, або навіть динамічно синтезованою в процесі виконання, то досить написати емулятор відповідного

процесора – деяку віртуальну машину, що буде виконувати код вірусу, побудований на певних принципах.

Вірус, написаний на віртуальній машині, вимагає дуже багато часу для аналізу традиційними методами. Виходить, потрібні засоби автоматичної боротьби з такого роду деструктивними програмами. Питання лише в тім, на яких принципах повинна базуватися така антивірусна система? Відповідь виявляється дивно простою: на принципах імунної системи людини. Дійсно, у нашій організмі функціонує чудова система, здатна боротися з мільярдами хвороботворних антигенів.

Антивірусна технологія антивірусного комплексу дата-центру побудована на основі моделі імунної системи людини.

Очевидно, що створити систему захисту інформації комп'ютерної мережі по прямій подібі імунної системи людини практично неможливо, так у цьому й немає необхідності. Однак той факт, що імунна система досягла досконалості в боротьбі із хвороботворними й чужорідними антигенами, говорить про те, що багато принципів, що сформували імунну систему, досить ефективні й можуть бути використані з тим допущенням, що працювати вони будуть не з біохімічними антигенами, а з антигенами програмними, тобто інформаційними.

Поряд із цим останні досягнення в області створення багатоагентних інтелектуальних систем дозволяють сподіватися, що найближчим часом штучна імунна система буде створена і її ефективність не опуститься нижче ефективності її природного прототипу.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів мережевого антивірусного комплексу дата-центру. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем мережевого антивірусного комплексу дата-центру.
- Досліджена система мережевого антивірусного комплексу дата-центру.
- На основі отриманих результатів досліджень створена програмна реалізація системи мережевого антивірусного комплексу дата-центру. Розроблені алгоритми дозволяють успішно вирішувати завдання мережевого антивірусного комплексу дата-центру. 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., 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.
2. 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.
3. Smirnov, O., Kuznetsov, A., Kiian, A., Kuznetsova, K., Ivko, T., Prokopovych-Tkachenko, D., «Soft Decoding Based on Ordered Subsets of Verification Equations of Turbo-Productive Codes», CEUR Workshop Proceedings Volume 2353, CEUR Workshop Proceedings 2019, Pages 873-884.
4. 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.
5. 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.
6. 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.
7. 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.
8. 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.

9. 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.
10. 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.
11. 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.
12. Smirnov, O., Kuznetsov, A., Shekhanin, K., Chepurko, I. Detecting Hidden Information in FAT. 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. 412-429. – ISBN: 978-0-9989826-8-7 (Hardback), ISBN: 978-0-9989826-9-4 (Ebook)
13. 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).
14. Смірнов О.А., Гнатюк С.О., Кавун С.В., Терейковський І.А., Жмурко Т.О., Смірнов С.А., Коваленко А.С. Основи безпеки в комп'ютерних мережах. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2018. – 177 с.
15. Смірнов О.А., Стасєв Ю.В., Бараннік В.В. Коваленко О.В., Доренський О.П., Дреєв О.М., Вялкова В.І. Інформаційна безпека держави. Підручник – Кіровоград: РВЛ КНТУ, 2016. – 263 с
16. Смірнов О.А., Кавун С.В., Коваленко О.В., Дреєв О.М. Мережні інформаційні технології. Навчальний посібник – Кіровоград: РВЛ КНТУ, 2016. – 159 с.
17. Смірнов О.А., Кавун С.В., Коваленко О.В., Доренський О.П., Дреєв О.М., Вялкова В.І. Комп'ютерні мережі. Навчальний посібник – Кіровоград: РВЛ КНТУ, 2016. – 233 с.
18. Смірнов О.А., Стасєв Ю.В. Бараннік В.В. Захист інформації в автоматизованих системах управління. Навчальний посібник – Харків: ХУПС, 2015. – 264 с.
19. 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
20. 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.
21. 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.
22. 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.
23. 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.
24. 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.
25. 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.
26. 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.
27. 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.
28. 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.
29. 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.
30. 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.
31. 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.

УДК 004

А.Дабич, магістр гр. КІ-24М,

Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ АУДИТУ БЕЗПЕКИ МЕРЕЖЕВИХ ICS/SCADA

У статті розроблено програмне забезпечення, яке призначено для системи аудиту безпеки мережесистем ICS/SCADA. Метою розробки є дослідження та принципи побудови системи аудиту безпеки мережесистем ICS/SCADA. Об'єктом дослідження є процес аудиту безпеки мережесистем ICS/SCADA. Предметом дослідження є методи аудиту безпеки мережесистем ICS/SCADA. Методи дослідження базуються на методах захисту інформації у мережі, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи аудиту безпеки мережесистем ICS/SCADA. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

аудит безпеки, мережа, ICS/SCADA

Постановка проблеми. Починаючи з кінця 60-х років минулого століття, промислові системи керування (Industrial Control System; ICS) з'явилися практично у всіх сферах, що мають відношення до сучасного життя: енергетика, промисловість, комунальні системи й інші області.

З моменту винаходу блокового цифрового контролера в 1968 році й до середини 90-х промислові системи керування були практично ізольовані й могли працювати з дуже обмеженим набором вхідних і вихідних даних із зовнішніх джерел.

Однак з появою дешевого устаткування, операційної системи Microsoft Windows, Active Directory і загальної стандартизації, сучасні корпоративні мережі стали одержувати й обробляти дані (а також виконувати інші безліч інших операцій) з мереж за межами традиційних ICS-мереж.

Незважаючи на те, що на даний момент уживає безліч зусиль по сегментації мереж пов'язаних з інформаційними й промисловими технологіями, границі дотепер залишаються розмитими, що доставляє багато головного болю фахівцям з безпеки, що працює в багатьох індустріях.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи аудиту безпеки мережесистем ICS/SCADA.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи аудиту безпеки мережесистем ICS/SCADA.

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

- Огляд існуючих систем аудиту безпеки мережесистем ICS/SCADA.
- Дослідження системи аудиту безпеки мережесистем ICS/SCADA.
- Програмна реалізація системи аудиту безпеки мережесистем ICS/SCADA.

Об'єктом дослідження є процес аудиту безпеки мережесистем ICS/SCADA.

Предметом дослідження є методи аудиту безпеки мережесистем ICS/SCADA.

Методи дослідження базуються на методах захисту інформації у мережі, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Системи безпеки ICS/SCADA захищають промислові системи керування та мережі диспетчерського керування й збору даних, які керують 90% критичної інфраструктури в усьому світі, запобігаючи кібератак, які завдають середньої шкоди в розмірі 5,9 мільйона доларів на інцидент. Системи промислового керування керують електромережами, що обслуговують 7,8 мільярда людей, водоочисними спорудами, що переробляють 147 мільярдів галонів щодня, та виробничими підприємствами, що виробляють товарів на суму 14,2 трильйона доларів щорічно. Ці системи щодня стикаються з 2400 кібератак, причому успішні порушення призводять до збоїв у роботі, які тривають в середньому 23 дні, та загрожують безпеці людей у 47% інцидентів, що потребують комплексного захисту.

Ключові висновки:

- Системи ICS/SCADA контролюють 90% глобальної критичної інфраструктури, і на ці мережі щодня направляється 2400 кібератак.
- Порушення безпеки коштують організаціям в середньому 5,9 мільйона доларів США з 23-денними перебоями в роботі
- 73% систем ICS/SCADA мають невивправлені вразливості через вимоги цілодобової роботи
- Сегментація мережі зменшує успішність атак на 84% за умови правильного впровадження розділення IT/OT
- Відповідність таким стандартам, як NIST SP 800-82 та IEC 62443, запобігає 67% поширених векторів атак.

Безпека ICS/SCADA – це захисні заходи, технології та практики, що захищають промислові системи управління, мережі диспетчерського контролю та збору даних від кіберзагроз, фізичних атак та операційних збоїв. Безпека ICS/SCADA охоплює комплексний захист операційних технологій, що контролюють промислові процеси у виробничому, енергетичному, водному та транспортному секторах. ICS представляє ширшу категорію операційних технологій, що контролюють промислові процеси, тоді як SCADA спеціально контролює та контролює розподілені активи в різних географічних регіонах.

ІКС включає програмовані логічні контролери (ПЛК), розподілені системи керування (РСК) та людино-машинні інтерфейси (ХМІ), що керують 4,7 мільйонами промислових об'єктів по всьому світу. Системи SCADA збирають дані в режимі реального часу з 23 мільйонів віддалених терміналів (RTU) по всьому світу, що дозволяє операторам контролювати та керувати інфраструктурою, що охоплює тисячі миль. Зв'язок між ІКС та SCADA передбачає функціонування СКАДА як рівня нагляду над компонентами ІКС, що забезпечує централізовану видимість та контроль критично важливих операцій.

Як працює безпека ICS/SCADA?

Безпека ICS/SCADA працює за допомогою багаторівневих захисних механізмів, включаючи сегментацію мережі, спеціалізовані протоколи, системи виявлення вторгнень та контроль доступу, що захищають промислові мережі від кіберзагроз. Мережева архітектура реалізує рівні моделі Purdue, що відокремлюють корпоративні IT від операційних технологій за допомогою демілітаризованих зон та брандмауерів. Промислові протоколи, такі як Modbus, DNP3 та OPC, вимагають протокольних залежних засобів контролю безпеки, що виявляють шкідливі команди та спроби несанкціонованого доступу.

Механізми безпеки включають односпрямовані шлюзи, що запобігають досягненню 99,9% мережових атак критично важливих систем керування. Сегментація мережі створює ізольовані зони, зменшуючи поверхню атаки на 73% та обмежуючи порушення в певних областях. Системи виявлення вторгнень щодня відстежують 8,4 мільярда пакетів промислової мережі, виявляючи аномальну поведінку, що вказує на кібератаки або несправності системи.

Чому безпека ICS/SCADA є критично важливою для бізнес-операцій?

Безпека ICS/SCADA має вирішальне значення для бізнес-операцій, оскільки потенційні наслідки включають виробничі втрати в розмірі 1,4 мільйона доларів США

щогодини, інциденти безпеки, що щорічно впливають на 10 000 працівників, та збої в інфраструктурі, що порушують роботу мільйонів громадян. Кібератаки на промислові системи зросли на 140% між 2020 і 2024 роками, причому програми-вимагачі були спрямовані на 56% виробничих потужностей і спричиняли середній час простою 21 день. Передові постійні загрози з боку 37 угруповань національних держав активно націлені на критичну інфраструктуру з метою шпигунства та потенційних можливостей порушення роботи.

У 2010 році Stuxnet продемонстрував вразливість ICS, знищивши 1000 іранських центрифуг за допомогою складних маніпуляцій з ПЛК, одночасно відображаючи операторам нормальну роботу. У 2015 році шкідливе програмне забезпечення BlackEnergy порушило роботу українських енергомереж, залишивши 230 000 жителів без електроенергії протягом 6 годин у зимових умовах. У 2017 році шкідливе програмне забезпечення Triton/Trisis було спрямоване на системи безпеки, намагаючись відключити можливості аварійного вимкнення на нафтохімічних об'єктах, що потенційно могло спричинити вибухи.

Поширені вразливості присутні у 73% систем ICS/SCADA, включаючи застарілі технології, яким в середньому 19 років, і які не мають вбудованих функцій безпеки. Плоска мережева архітектура у 61% об'єктів дозволяє зловмисникам рухатися в горизонтальному напрямку після того, як зловмисники порушують захист периметра. Відсутність моніторингу в режимі реального часу у 43% промислових мереж дозволяє зловмисникам діяти непоміченими в середньому протягом 246 днів.

Як організації можуть подолати проблеми безпеки ICS/SCADA?

Організації можуть подолати проблеми безпеки ICS/SCADA, впроваджуючи спеціалізовані стратегії, що враховують унікальні операційні обмеження, включаючи вимоги до цілодобової доступності, 20-річний життєвий цикл обладнання та критично важливі для безпеки операції, які не терплять перебоїв. Обмеження щодо виправлень впливають на 82% середовищ ICS, де системи не можна вивести з режиму автономного режиму для оновлень, що вимагає компенсуючих елементів керування, таких як віртуальне виправлення та мережева ізоляція. Застарілі системи, несумісні із сучасними інструментами безпеки, вимагають використання технологій-обгорт, що забезпечують захист без модифікації оригінального обладнання.

Спеціалізовані інструменти безпеки для ОТ, розроблені для промислових протоколів та вимог реального часу, захищають системи, не впливаючи на роботу. Рішення для пасивного моніторингу аналізують мережевий трафік без надсилання пакетів, запобігаючи випадковим збоям у роботі системи, які впливають на 11% активних сканерів. Інструменти інвентаризації активів виявляють 100% підключених пристроїв, включаючи 31%, які зазвичай невідомі операторам, завдяки комплексним процесам виявлення.

Програми навчання персоналу навчають 2,3 мільйона промислових операторів у всьому світі ризикам кібербезпеки та процедурам реагування. Інженерні команди проходять навчання з безпеки операційних систем, що охоплює безпечне програмування для ПЛК, посилення мережевої архітектури та реагування на інциденти. Перехресне навчання між командами IT та операційних систем усуває прогалини в знаннях, і 89% успішних програм потребують управління культурними змінами.

Поширені загрози для ICS/SCADA

Поширеними загрозами для ICS/SCADA є цільове шкідливе програмне забезпечення, дії інсайдерів, компрометація ланцюгів поставок, мережеві атаки та зловживання фізичним доступом, що завдає середньої шкоди в розмірі 5,9 мільйона доларів США за інцидент. Ці загрози використовують вразливості операційних технологій за допомогою складних методів атак, розроблених спеціально для промислового середовища.

Шкідливе програмне забезпечення та програми-вимагачі, спрямовані на SCADA

Шкідливе програмне забезпечення та програми-вимагачі атакують системи SCADA через спеціалізовані варіанти, розроблені для промислових процесів, причому кількість атак зросла на 2000% з 2010 року. Атаки програм-вимагачів на промислові об'єкти вимагають

середніх платежів у розмірі 2,3 мільйона доларів США, шифруючи НМІ та бази даних історії, критично важливі для операцій. Програма-вимагач EKANS спеціально націлена на промислові системи управління, перевіряючи та завершуючи 64 процеси, специфічні для ICS, до початку шифрування. Методи збереження шкідливого програмного забезпечення використовують інженерні робочі станції, причому 43% атак відбуваються із заражених ноутбуків постачальників під час технічного обслуговування.

Внутрішні загрози та людські помилки

Внутрішні загрози та ризики людських помилок становлять 34% інцидентів безпеки ICS, причому зловмисники завдають збитків у середньому на суму 4,7 мільйона доларів США через саботаж або крадіжку даних. Внутрішні загрози включають співробітників, підрядників та постачальників з доступом до систем, що становить 67% ризиків безпеки, часто без навчання з питань безпеки. Людська помилка спричиняє 52% інцидентів безпеки ICS, включаючи неправильну конфігурацію, переходи за фішинговими посиланнями та випадкове відключення засобів контролю безпеки. Моніторинг привілейованих користувачів виявляє 89% внутрішніх загроз, зменшуючи вплив інцидентів на 71% завдяки ранньому виявленню та реагуванню.

Компроміси в ланцюжку поставок

Компрометації ланцюгів поставок впливають на ICS/SCADA через атаки, спрямовані на постачальників та інтеграторів, які зросли на 430% між 2020 і 2024 роками, торкнувшись тисяч клієнтів нижчої ланки. Атаки на ланцюги поставок, такі як SolarWinds, вплинули на 18 000 організацій, включаючи операторів критичної інфраструктури, які керують системами живлення та водопостачання. Апаратні імплантати, виявлені у 0,3% поставок промислового обладнання, забезпечують постійний бекдор-доступ, що витримує оновлення прошивки та скидання системи. Вразливості сторонніх компонентів впливають на 73% пристроїв ICS через спільні бібліотеки та вбудовані системи, що вимагають комплексної безпеки ланцюга поставок.

Мережева атака

Методи мережевих атак включають атаки типу «людина посередині», які перехоплюють та змінюють 31% незашифрованого зв'язку ICS, маніпулюючи показаннями датчиків та командами керування. Атаки типу «відмова в обслуговуванні», спрямовані на промислові мережі, спричиняють середній час простою 14 годин, що коштує 940 000 доларів США за інцидент через втрати виробництва. Експлуатація протоколів використовує незахищені за своєю природою промислові протоколи, 67% з яких не мають можливостей автентифікації або шифрування. Мережева розвідка виявляє вразливі системи у 94% промислових мереж протягом 72 годин після першого доступу.

Експлуатація фізичного доступу

Фізичний доступ дозволяє здійснювати експлуатацію шляхом обходу засобів контролю безпеки мережі, причому 23% об'єктів мають недостатній фізичний захист критично важливих систем керування. Атаки на основі USB через знімні носії залишаються ефективними у 61% систем з обмеженим доступом, поширюючи шкідливе програмне забезпечення по ізольованих мережах. Введення несанкціонованих пристроїв, включаючи точки бездротового доступу, щорічно ставить під загрозу 17% захищених об'єктів, створюючи несанкціоновані мережеві мости. Фізичне втручання в датчики та виконавчі механізми призводить до збоїв у процесах, які не виявляються системами кібермоніторингу, зосередженими на мережевому трафіку.

Що таке стратегії та найкращі практики кібербезпеки ICS/SCADA?

Стратегії кібербезпеки ICS/SCADA – це підходи до глибокого захисту, що поєднують сегментацію мережі, принципи нульової довіри, безпечний віддалений доступ, безперервний моніторинг та планування реагування на інциденти, що зменшує успішність атак на 84%. Ці стратегії враховують унікальні вимоги до операційних технологій, зберігаючи при цьому доступність та безпеку системи.

Як сегментація мережі захищає ICS/SCADA?

Сегментація мережі захищає ICS/SCADA, розділяючи IT- та OT-середовища за допомогою брандмауерів, зменшуючи успішність горизонтального переміщення на 91% під час порушень. Сегментація мережі реалізує модель Пердью, створюючи ієрархічні зони з контрольованим зв'язком між рівнями, що містять 87% атак у початкових зонах компрометації. Мікросегментація в OT-мережах ізолює критичні системи, обмежуючи радіус вибуху під час виникнення інцидентів. Розгортання DMZ між IT- та OT-мережами фільтрує 4,7 мільярда спроб підключення щодня, блокуючи 99,3% несанкціонованого трафіку.

Як принципи нульової довіри застосовуються до ICS/SCADA?

Принципи нульової довіри застосовуються до ICS/SCADA шляхом перевірки кожного з'єднання незалежно від джерела, що зменшує несанкціонований доступ на 94% завдяки постійній перевірці. Архітектура нульової довіри для ICS/SCADA перевіряє всіх користувачів, пристрої та програми, запобігаючи 78% атак на основі облікових даних. Доступ з мінімальними привілеями обмежує користувачів мінімально необхідними дозволами, що містить пошкодження від скомпрометованих облікових записів. Безперервна перевірка відстежує моделі поведінки, виявляючи аномалії у 97% сценаріїв внутрішніх загроз.

Що таке протоколи безпечного віддаленого доступу?

Безпечні протоколи віддаленого доступу замінюють 73% вразливих VPN-з'єднань на зашифровані сервери переходів та рішення для керування привілейованим доступом. Багатофакторна автентифікація запобігає 99,9% автоматизованих атак на портали віддаленого доступу, що використовуються постачальниками та підрядниками. Запис та моніторинг сеансів відстежують усі віддалені дії, надаючи судово-медичні докази для 100% віддалених сеансів. Контроль доступу на основі часу обмежує вікна з'єднань, зменшуючи вразливість на 67% порівняно з методами постійного доступу.

Як працюють безперервний моніторинг та виявлення аномалій?

Безперервний моніторинг та виявлення аномалій працюють шляхом аналізу 12 мільярдів подій мережі ICS щодня, виявляючи загрози протягом 4 хвилин після початкової активності. Безперервний моніторинг використовує алгоритми машинного навчання для базової оцінки нормальної роботи, а потім виявляє відхилення з точністю 94% та рівнем хибних спрацьовувань 0,3%. Моніторинг активів відстежує зміни конфігурації, виявляючи несанкціоновані модифікації, щомісяця впливають на 31% пристроїв ICS. Моніторинг змінних процесу виявляє маніпулювання показаннями датчиків та командами керування, що вказують на кіберфізичні атаки.

Чому важливі планування реагування на інциденти та проведення навчальних заходів?

Планування реагування на інциденти та практичні навчання є важливими, оскільки плани, специфічні для ICS/SCADA, скорочують час відновлення на 73% порівняно із загальними процедурами реагування на IT. Плани реагування на інциденти враховують унікальні операційні вимоги, надаючи пріоритет критично важливим для безпеки системам та підтримуючи роботу під час інцидентів. Практичні навчання, що проводяться щоквартально, покращують координацію команди, виявляючи прогалини в процесах у 89% симуляцій. Посібники з поширених сценаріїв, включаючи атаки програм-вимагачів та системи безпеки, допомагають у прийнятті рішень, що запобігають паніці.

Що таке стандарти безпеки ICS/SCADA та рамки відповідності?

Стандарти безпеки та структури відповідності ICS/SCADA є базовими вимогами та найкращими практиками для організацій, які дотримуються структур, що зменшує кількість інцидентів безпеки на 67% порівняно з об'єктами, що не відповідають вимогам. Ці стандарти враховують унікальні вимоги до операційних технологій, включаючи продуктивність у режимі реального часу, доступність та безпеку.

Стандарт NIST SP 800-82 надає комплексні рекомендації щодо безпеки ICS, яких прийняли 43% операторів критичної інфраструктури США, враховуючи унікальні вимоги до

240 засобів контролю безпеки. Впровадження зменшує вразливості на 71% завдяки систематичному управлінню ризиками та вибору засобів контролю безпеки. Серія ISA/IEC 62443 представляє міжнародні консенсусні стандарти безпеки промислової автоматизації, що впроваджені в 67 країнах.

Стандарти NERC CIP вимагають від 3000 північноамериканських операторів оптових електричних систем дотримання 45 вимог за 11 стандартами. Порушення призводять до щоденних штрафів у розмірі 1 мільйона доларів, тоді як впровадження запобігає 73% поширених векторів атак за допомогою необхідних заходів контролю. Керівні принципи CISA містять галузеві рекомендації щодо безпеки ICS для 16 секторів критичної інфраструктури, що дозволяє 4700 організаціям отримувати інформацію про загрози.

Специфічні для GCC правила стосуються регіональних вимог безпеки ICS/SCADA, а структура NESAS OAE передбачає 33 елементи керування для операторів критичної інфраструктури. Стандарти NCSA Катару вимагають оцінки безпеки ICS для національної інфраструктури, що виявляє вразливості у 94% оцінених систем. Регіональне співробітництво через GCC-CERT обмінюється інформацією про загрози між державами-членами, запобігаючи транскордонним кіберінцидентам.

Незважаючи на важливість правильної ізоляції й інтерес до теми, пов'язаної з експертизою мереж, в інтернеті мало інформації стосовно цього питання. У цьому розділі будуть освітлені найпоширеніші проблеми, пов'язані з ізоляцією мереж, з якими ми зіштовхувалися під час попередніх експертиз. Сподіваємося, що ця інформація допоможе пентестерам глибше поринути в цю тему, а співробітникам, відповідальним за безпеку, відкриє завісу методів, якими користуються зловмисники для одержання доступу до нижніх шарів мережі керування виробничими процесами з боку корпоративної мережі.

Тестування сегрегації мережі звичайно складається з декількох кроків:

- Збір інформації.
- Ідентифікація місця проникнення.
- Доступ до сегрегованої мережі.

Збір інформації

Збір інформації в основному спрямований на ідентифікацію будь-яких незахищених даних, зв'язаних мережею керування виробничими процесами. Ця інформація може розкрити деталі про мережу керування, які допоможуть зловмисникові одержати доступ. Звичайно тут мається на увазі наступне:

– Інформація про персонал, що має відношення до керування процесами -технологи, оператори, IT-персонал і інші ключові люди звичайно володіють конфіденційною інформацією про мережу керування виробничими процесами. Пошук в Active Directory по співробітниках, які виконують вищезгадані ролі, може допомогти в ідентифікації імен робочих станцій і спільно використовуваних мережних ресурсах (кулях), до яких є доступ. Уже цей крок значно скорочує обсяг аналізованих даних і загальна кількість зусиль, необхідних для одержання доступу до мережі керування, оскільки в цьому випадку увага буде зосереджено тільки на певних хостах і кулях.

– Мережні діаграми й проектна документація – ця інформація може допомогти зловмисникові зрозуміти механізми роботи мережі керування процесами на фундаментальному рівні, а також виявити імена хостів і IP-адреси як відправні крапки для наступного збору відомостей. Більше того, в ідеальній ситуації мережна документація може дати повну картину керування, що відбувається в мережі, виробничими процесами й допомогти виявити хости, які потрібно атакувати в першу чергу. Після ідентифікації файлових серверів у корпоративній мережі й інформаційних репозитаріїв (наприклад, SharePoint) мережна документація звичайно шукається у файлах VSD, PDF і DOC / DOCX, що перебувають у директоріях або кулях, що мають відношення до відповідних процесів.

– Документація на мережу керування процесами -ця інформація може містити деталі офіційних процедур, пов'язаних з вилученням доступом, інструкції про авторизацію на хости, що мають відношення до виробничих процесів, і дані про технології (використовуваних і

невикористовуваних). У багатьох випадках, у подібній документації втримується надзвичайно важлива й конфіденційна інформація (наприклад, логіни й паролі), що є безцінною під час експертизи сегрегації мережі. Ця документація може перебувати усередині ІТ-куля й директорій або іноді в папках і кулях, що мають відношення безпосередньо до виробничих процесів.

– Мережні пристрої й бекапи систем – конфігураційні файли файервола, роутера й світча, які перебувають усередині резервної копії в корпоративній мережі, часто допомагають побудувати оптимальну схему проникнення в мережу керування. При вивченні конфігурації мережних пристроїв можна виявити хости в корпоративній мережі, до яких дозволений вилучений доступ через протоколи RDP, VNC і SSH. Якщо в корпоративній мережі перебувають бекапи систем, пов'язаних з керуванням процесами, то із цих даних можна легко витягти хеші й інші конфіденційні відомості. Ця інформація часто може бути отримана через додатки для ІТ-керування або мережного резервного копіювання, а також у корпоративні або мережних ІТ-кулях.

Ідентифікація місця проникнення

Один із ключових моментів на етапі збору інформації – ідентифікація існуючих місць проникнення в мережу керування виробничими процесами з корпоративної мережі. У більшості ситуацій можна знайти наступні типи місць проникнення:

– Jump-сервер (jumpbox) / Термінальний сервер- Доступ до мережі керування процесами з корпоративної мережі часто дозволений через хост, що функціонує як jump-сервер (або jump box). Звичайно вилучений доступ здійснюється через протоколи RDP, VNC і SSH. Хоча іноді використовуються додатки для віртуалізації робітників столів на зразок Citrix. Організації, що приділяють мірам безпеки особлива увага, часто використовують рішення, що підтримують багатофакторну автентифікацію під час вилученого доступу.

У документації часто описуються офіційні процедури для вилученого доступу до мережі керування виробничими процесами. Jump-сервера або термінальних служб також можуть бути ідентифіковані за допомогою аналізу мережних діаграм або конфігураційних файлів файервола для хостів, яким дозволені з'єднання з корпоративної мережі через стандартні порти вилученого доступу. Дослідження робочих станцій персоналу в корпоративній мережі, що має відношення до керування процесами, часто є ефективним способом ідентифікації jump-серверів і протоколу, використовуваного для вилученого доступу:

– VPN-доступ – Обраним користувачам, що звичайно мають відношення до керування процесами, може бути дозволений прямий VPN-доступ з метою вилученого керування мережею. Так само як і у випадку з jump-серверами тут може використовуватися багатофакторна автентифікація.

Іноді для цих користувачів може бути створена окрема група. Вивчення імен і опису груп, у які входять ключові співробітники, що мають відношення до виробничих процесів, звичайно дозволяє виявити групу користувачів, у яких є VPN-доступ. Далі починається дослідження робочих станцій цих користувачів на предмет присутності VPN-інтерфейсів або додатків, а також активних з'єднань до мережі керування виробничими процесами. Ці робочі станції можуть використовуватися як міст до мережі керування.

– Дводомні хости – У типовій мережі, пов'язаній з керуванням виробничими процесами, трохи хостів можуть бути зконфігуровані як дводомні або за допомогою додаткових правил файервола, які дозволяють доступ до мережі керування. Звичайно в цю категорію попадають сервера, що зберігають архівні дані, використовувані з метою аналізу й поліпшення продуктивності виробничих процесів. Одержання доступу до цих хостів часто дає прямий доступ до мережі керування виробничими процесами без необхідності використання офіційних процедур вилученого доступу. Навіть якщо архівні сервера не дають розширеного доступу до мережі керування, дослідження активних з'єднань допомагає виявити діапазони цільових IP-адрес.

Найбільш надійний спосіб пошуку хостів з архівними даними – аналіз мережної документації й діаграм. Крім того, незайвим буде звернути увагу на імена хостів (архівні хости часто мають імена “HI”, “HIS”, “HIST” або щось у такому дусі). Можна спробувати посканувати порти, однак це завдання ускладнюється тим, що не існує єдиного стандарту портів, використовуваних виробниками. Хоча багато організацій використовують архівні сервера на базі системи OSISoft PI, які можна виявити за допомогою сканування найпоширеніших портів, пов'язаних із цим програмним забезпеченням (<https://techsupport.osisoft.com/troubleshooting/kb/2820osi8>). У цілому, якщо виробник системи керування відомий або виявлений у процесі аналізу, то далі вивчається загальнодоступна документація на предмет використання розповсюджених портів для наступного сканування в корпоративній мережі.

Ще один ефективний метод виявлення дводомних хостів – обстеження корпоративної мережі за допомогою виконання вилучених команд певним чином (наприклад, WMI або PSEXEC) і добування активних з'єднань, мережних інтерфейсів і таблиць маршрутизації. Ці дані потім використовуються для пошуку хостів, що мають доступ до мережі керування виробничими процесами. Хоча цей метод створює багато шуму, забирає багато часу й може видавати величезні обсяги інформації для парсингу, особливо в більших мережах. З іншого боку, фільтрація по отриманим раніше діапазонах IP-адрес, які використовуються мережею керування, значно спрощує завдання.

Доступ до сегрегованої мережі

Після одержання потенційних місць проникнення в мережу керування виробничими процесами наступний крок – дослідження кожного місця на предмет присутності розповсюджених уразливостей з метою одержання доступу до мережі керування. Нижче перераховані найпоширеніші проблеми, які були виявлені під час експертизи різних мереж.

– Небезпечні паролі – Паролі є серйозною проблемою для співробітників, відповідальних за безпеку мережі керування виробничими процесами, з кількох причин. Основна проблема полягає в складності мотивації інженерів і інших користувачів, у яких є доступ до мережі керування, до використання стійких паролів. Найчастіше використовуються ті самі паролі й у корпоративній мережі й у мережі керування, оскільки користувачі не бажають управляти набором паролів і вважають, що ризик злому мережі ніщо малий. Після компрометування корпоративної мережі й злому / одержання паролів ключових співробітників, ті ж самі паролі можуть використовуватися для доступу до мережі керування виробничими процесами через раніше отримані місця проникнення.

Дуже часто використовуються стандартні або слабкі паролі, які встановлені виробником за замовчуванням. Ці паролі ніколи не міняються, щоб уникнути проблем, пов'язаних з відхиленням від стандартної конфігурації. Часто імена користувачів і паролів збігаються (наприклад, operator: operator, manager: manager, supervisor: supervisor) або використовуються варіації ім'я виробника (наприклад, Administrator: siemens).

Ситуація погіршується ще тим, що політики блокування паролів, використовуваних у виробничих процесах, звичайно не визначені через запобігання випадкових блокувань, які можуть привести до проблем або зупинки всього процесу. Хоча ця ідея й має право на життя, але з іншої сторони зловмисникові відкриваються можливості для прямого підбора облікових записів. Ця проблема в комбінації з попередніми (слабкі й повторно використовувані паролі) робить атаку по переборі надзвичайно ефективною при спробі одержання доступу до мережі керування виробничими процесами.

– Зберігання паролів у відкритому виді – Облікові записи, використовувані при керуванні технологічними процесами, часто втримуються в документації. Будь-які репозиторії, де зберігається документація мережі керування виробничими процесами, повинні бути досліджені на етапі збору інформації при експертизі сегрегації мережі. Будь-яка знайдена документація повинна бути проаналізована на предмет паролів, використовуваних у місцях проникнення.

– Домен корпоративної мережі підключений до мережі керування – У випадку присутності в корпоративній мережі дводомних хостів або робітників станцій з VPN-доступом ці хости звичайно приєднані до домену в Active Directory. Відповідно, стає можливим одержання доступу до цих хостам прямо за допомогою високопривілейованих облікових записів, використовуваних в Active Directory з боку корпоративної мережі (наприклад, за допомогою облікового запису адміністратора домену). В організаціях, де безпеки приділяється особлива увага, уживають додаткові кроки по обмеженню доступу до цим хостам тільки для певних користувачів або груп. Хоча якщо корпоративна мережа скомпрометована, те досить просто знайти потрібних користувачів і витягти паролі з пам'яті.

– Відкриті уразливі служби – У місцях проникнення можуть використовуватися додаткові служби (наприклад, бази даних або веб-застосунка), уразливі до найпоширеніших атак. Кожний хост, у якого є доступ до мережі керування виробничими процесами, повинен бути просканий на предмет присутності неврахованих служб. У випадку знаходження подібних служб потрібно провести аналіз на предмет наявності уразливостей або розповсюджених помилок у конфігурації, які можуть стати причиною компрометування всього хоста.

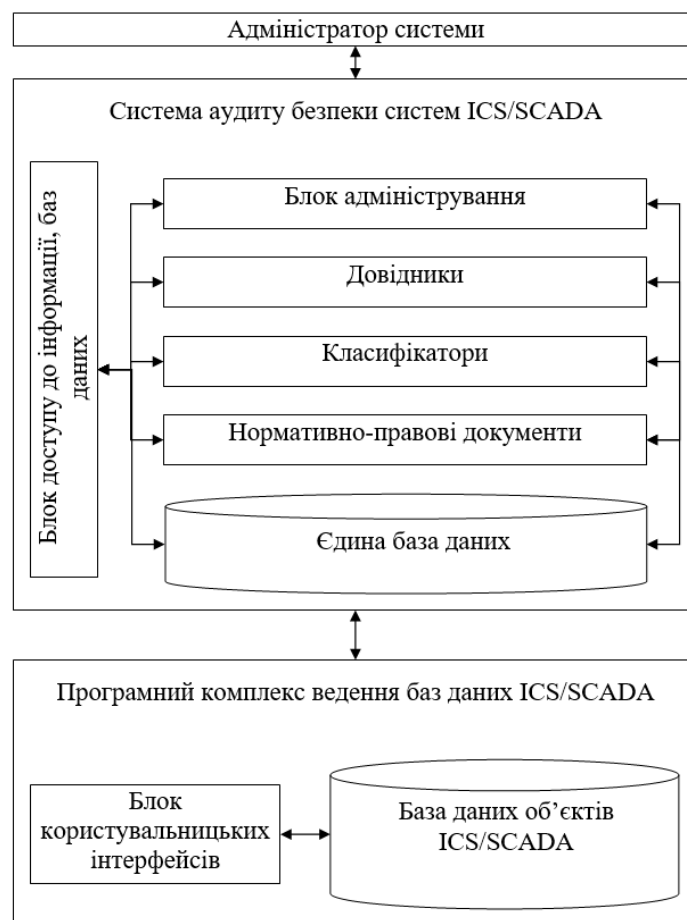


Рисунок 1 – Структурна схема системи

Якщо ви коли-або, виконуючи пентести ICS-інфраструктури, зіткнулися з однією з наступних ситуацій, негайно рапортуйте про критичну проблему:

- У корпоративній мережі виявлений трафік Modbus/DNP3.
- З корпоративної мережі є доступ до людино-машинного інтерфейсу (HMI) із правами не тільки на читання.
- Пінгування ядерного реактора за допомогою NMAP приводить до необоротних наслідків.

Сподіваємося, що остання ситуація з вами ніколи не трапиться. У противному випадку, бажаємо вам залишитися цілим і непошкодженим.

Незважаючи на те, що навколо нас багато чого залежить від ICS-технологій, існує явний недолік інформації щодо безпеки подібних систем.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів аудиту безпеки мережевих ICS/SCADA. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем аудиту безпеки мережевих ICS/SCADA.
- Досліджена система аудиту безпеки мережевих ICS/SCADA.
- На основі отриманих результатів досліджень створена програмна реалізація системи аудиту безпеки мережевих ICS/SCADA.

Розроблені алгоритми дозволяють успішно вирішувати завдання аудиту безпеки мережевих ICS/SCADA. 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. Вінтенко Б.Ю., Миронець І.В., Смірнов О.А. «Модель комп'ютерно-орієнтованої процедури системи підтримки оперативного персоналу АЕС». IV Міжнародна науково-практична Інтернет-конференція «Інновації та перспективні шляхи розвитку інформаційних технологій (ІППІТ-2025)» м.Черкаси 25 листопада 2025 року – Черкаси: ЧДТУ.– 2025. – С.101-103.
2. 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.
3. 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.
4. 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.
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. 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.
9. 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.
10. 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». Центральноукраїнський науковий вісник. Технічні науки. 2025. Вип. 11(42), ч. II. С.52-62.
11. 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.
12. 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.
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. 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. 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.
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. 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.
19. 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.
20. 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.
21. 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.
22. 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.
23. 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.
24. 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.
25. 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.
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., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». *CEUR Workshop Proceedings. Volume 2740*, 2020, Pages 102-114.
28. 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.
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., 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.
31. 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

Н.Дворцов, магістр гр. КН-24М,*Центральноукраїнський національний технічний університет*

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ІНТЕЛЕКТУАЛЬНОГО РОЗПІЗНАВАННЯ З ВИКОРИСТАННЯМ ОСОБЛИВИХ ТОЧОК

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

інтелектуальне розпізнавання образів, використання особливих точок

Постановка проблеми. Для людей розпізнавання образів – це когнітивний процес у мозку. Ми можемо без зусиль зіставити інформацію, яку бачимо, з даними, що зберігаються в нашій пам'яті. Ми можемо миттєво розрізнити зображення квітки та тварини або впізнати знайоме обличчя, гортаючи Instagram.

Розпізнавання образів відбувається в нашому мозку, коли ми зіставляємо інформацію, з якою ми стикаємося, з даними, що зберігаються в нашій пам'яті. Рецептори розпізнавання образів (PRR) у нашому організмі мають специфічну місію з виявлення та боротьби з патогенними та пов'язаними з пошкодженнями молекулярними патернами. Але це біологія, а не технології.

У машинному навчанні розпізнавання образів – це технологія, яка зіставляє інформацію, що зберігається в базі даних, з вхідними даними шляхом визначення спільних характеристик.

Іноді люди плутають машинне навчання та розпізнавання образів. Щоб спростити це, скажімо, що розпізнавання образів – це один із видів машинного навчання.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи інтелектуального розпізнавання з використанням особливих точок.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи інтелектуального розпізнавання з використанням особливих точок.

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

- Огляд існуючих систем інтелектуального розпізнавання з використанням особливих точок.
- Дослідження системи інтелектуального розпізнавання з використанням особливих точок.
- Програмна реалізація системи інтелектуального розпізнавання з використанням особливих точок.

Об'єктом дослідження є процес інтелектуального розпізнавання з використанням особливих точок.

Предметом дослідження є методи інтелектуального розпізнавання з використанням особливих точок.

Методи дослідження базуються на методах теорії розпізнавання образів, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Розпізнавання образів даних

Розпізнавання образів – це похідна від машинного навчання, яка використовує аналіз даних для розпізнавання вхідних шаблонів та закономірностей. Ці дані можуть бути будь-чим: від тексту та зображень до звуків чи інших визначених якостей.

Ця техніка дозволяє швидко та точно розпізнавати частково приховані візерунки навіть у незнайомих об'єктах. Розпізнавання візерунків передбачає класифікацію та кластеризацію точок даних на основі знань, отриманих статистично з минулих представлень.

Що таке шаблони з точки зору даних?

Розпізнавання образів включає обробку необроблених даних у кластеризовані образи або ознаки.

Шаблони – це характеристики даних, які можуть бути безперервними, як-от спектральні особливості мовлення, або дискретними/двійковими, як у випадку тексту чи зображень. Шаблон зазвичай має векторне представлення.

Закономірності, математично вивчені моделями машинного навчання (за допомогою методів статистичного розпізнавання образів), призначаються цільовому класу на основі абстракції, згенерованої за допомогою знань предметної області та ознак, витягнутих з вхідних даних.

Як працює розпізнавання образів?

Тепер перейдемо до обговорення складових частин методу розпізнавання образів

Пошук закономірностей у даних:

– Збір та попередня обробка даних. Система розпізнавання образів може працювати з будь-яким типом даних, таким як текст, відео, аудіо тощо, та попередньо обробляти ці вхідні дані. Цей етап є важливим, оскільки він зосереджений на доповненні даних та фільтрації шуму в системі.

– Представлення даних. Потім нейронна мережа аналізує відфільтровані дані, щоб отримати та виявити значущу інформацію. Витягнуті ознаки сегментуються на те, що становить шаблони.

– Прийняття рішень. Виявлені притаманні закономірності та висновки вводяться в режим 1 для прогнозування класів (позначений набір даних), прогнозування кластерів (непозначений набір даних) або прогнозування значення (де в гру вступає регресія) на основі бізнес-випадку використання.

Етапи розпізнавання образів

Розпізнавання образів – це розділ машинного навчання, який зосереджується на розпізнаванні шаблонів даних. Він складається з двох основних частин:

1. Дослідницьке розпізнавання образів – спрямоване на виявлення шаблонів даних загалом. Алгоритми зосереджені на пошуку прихованих шаблонів або кластерів ознак у даних. Вони в основному покладаються на ненавчальну класифікацію, яка призначає вхідний шаблон як невизначений клас.

2. Описове розпізнавання образів – спрямоване на категоризацію виявлених образів та ідентифікацію їх як частини заздалегідь визначеного класу. В основному використовується контрольована класифікація.

Розпізнавання образів часто є завданням класифікації або категоризації. Класи або визначаються системою (у випадку контрольованої класифікації), або вивчаються на основі подібності між образами (як у випадку неконтрольованої класифікації).

Типи моделей розпізнавання образів

Статистичне розпізнавання образів

Як випливає з назви, ця модель спирається на історичні дані та статистичні методи для вивчення особливостей і закономірностей з даних. Це включає збір спостережень, їх вивчення та аналіз для виведення загальних правил або концепцій, які можна застосувати до нових, невидимих спостережень.

Візерунок групується на основі його ознак, а кількість ознак визначає, як візерунок розглядається як точка в d -вимірному просторі. Для розпізнавання візерунків використовується цей простий метод:

1. Представлення. Визначення способу зв'язку об'єктів, можливо, за допомогою n -вимірного векторного простору.
2. Узагальнення. Правила та концепції, які можна вивести з заданого представлення набору прикладів і, отже, застосувати до невидимих точок даних.
3. Оцінювання. Оцінки точності та достовірності моделі для оцінки продуктивності системи.

Наприклад, ця модель зручна під час розробки штучного інтелекту для фінансового сектору, щоб прогнозувати ціни на акції на основі минулих ринкових тенденцій та екстраполювати ринкові умови з минулих даних.

Розпізнавання синтаксичних образів

Шаблони, що містять структурну або реляційну інформацію, важко кількісно визначити як вектори ознак через їхню складність. У таких випадках статистичного розпізнавання шаблонів може виявитися недостатнім.

Однак, ви можете класифікувати дані на основі структурної схожості у шаблонах даних. Саме тому методи розпізнавання синтаксичних шаблонів працюють для розпізнавання зображень та аналізу сцен, де шаблони складні, а кількість ознак велика.

Розбиття складних шаблонів на простіші ієрархічні підшаблони зручно для розпізнавання доріг, річок чи людей на зображеннях, або синтаксису та граматики в тексті.

Розпізнавання нейронних образів

Безумовно, це найпопулярніший метод виявлення закономірностей завдяки ступеню складності, з якою він може впоратися.

Штучна нейронна мережа – це обчислювальна система, змодельована за архітектурою нейронної мережі, подібно до того, як людський мозок обробляє складні сигнали.

Він може навчитися розпізнавати закономірності в різних типах даних (наприклад, текстових, візуальних чи аудіо) та ефективно працювати з невідомими даними.

Зіставлення шаблонів

Цей метод зіставляє характеристики об'єкта з попередньо визначеним шаблоном та ідентифікує об'єкт за посередництвом.

Його зазвичай використовують у комп'ютерному зорі для виявлення об'єктів у таких галузях, як робототехніка, відстеження транспортних засобів та інших, щоб знаходити невеликі ділянки зображення, що відповідають шаблону.

Наприклад, у медичній візуалізації вузлики виявляються за допомогою методів зіставлення шаблонів.

Порада професіонала: ознайомтеся з нашим списком інноваційних застосувань штучного інтелекту в охороні здоров'я.

Переваги та проблеми розпізнавання образів

Тепер давайте коротко розглянемо переваги та недоліки методу розпізнавання образів.

Розпізнавання образів – переваги:

– Розпізнавання образів допомагає вирішувати сценарії класифікації, такі як проблеми біометричного виявлення та класифікація вузликів на пухлинні/непухлинні клітини в медичній візуалізації.

– Розпізнавання образів корисне для виявлення об'єктів, особливо для ідентифікації віддалених та прихованих об'єктів або тих, що видно під іншими кутами, ніж у вхідних даних. Моделі штучного інтелекту можуть робити нюансовані спостереження та

співвідносити численні образи на величезних обсягах даних, що є одним із найцінніших застосувань розпізнавання образів.

– Розпізнавання образів вміє підсумовувати всі вектори ознак та шаблони даних, що дозволяє йому прогнозувати ціни на акції та робити точні екстрапольовані прогнози загалом.

Розпізнавання образів – труднощі:

– Розпізнавання образів, як правило, вимагає багато даних. Іншими словами, для навчання нейронних мереж аналізу образів потрібно багато навчальних даних. Зберігання таких величезних обсягів даних може ще більше обмежити застосування розпізнавання образів.

– Проблеми з якістю даних. Дані для навчання алгоритмів машинного навчання повинні надходити з надійних джерел. Вони повинні бути вільними від упередженості та шуму, які перешкоджають ідентифікації шаблонів та можливостям нейронної мережі приймати рішення.

– Тривалий час навчання. Виявлені закономірності не тільки важко аналізувати, але й потребують багато часу для збору даних, їх попередньої обробки та навчання моделі.

Застосування розпізнавання образів

Розпізнавання образів має низку більш і менш відомих застосувань у різних галузях промисловості.

Прогноз фондового ринку

Прогнозування майбутньої вартості акцій є одним із найскладніших завдань. Спочатку використовувалися лінійні моделі машинного навчання та навчання рішень, але тепер також використовуються моделі глибокого навчання. Багато трейдерів використовують графічні патерни в поєднанні з іншими алгоритмами розпізнавання образів, що включають глибоке навчання та LSTM, для прийняття торгових рішень та прогнозування фондового ринку.

Дослідження аудиторії

Розпізнавання образів служить способом опису даних шляхом виділення їх відмінних рис, які самі по собі є закономірностями. Воно використовується для аналізу доступних даних користувачів та їх сегментації за вибраними ознаками.

Google Analytics є одним із відомих джерел таких функцій. Дані, зібрані Google Analytics, можуть бути пов'язані з тим, що клієнт має намір купити, коли відвідує певний веб-сайт, кількістю людей, які переглянули публікацію, та чи взаємодіяли вони з контентом, наприклад, з кліками. Перегляд даних про транзакції може допомогти у визначенні моделей поведінкової сегментації під час відвідування веб-сайтів та транзакцій електронної комерції.

Багато OTT-платформ та компаній електронної комерції покладаються на складні механізми штучного інтелекту, які аналізують моделі поведінки користувачів, щоб персоналізувати свої пропозиції. Прикладами цього є рубрики «Вам також може сподобатися» від Netflix та «Люди також купують» від Amazon.

Розпізнавання текстових шаблонів

Розпізнавання образів – це спосіб ідентифікації складових частин тексту, таких як слова, граматики та шаблон, якому він дотримується. Це використовується в засобах перевірки граматики, машинному перекладі, категоризації контенту тощо.

Відгуки клієнтів

У світі бізнесу обробка тексту широко використовується для покращення обслуговування клієнтів. Системи розпізнавання образів шукають корисну інформацію у відгуках клієнтів та оглядах продуктів. Це включає такі речі, як використані ключові слова, почуття клієнта та його бажання. Це важливо для таких речей, як аналіз конкурентів та ринку. Ми можемо дізнатися, що люди думають про компанію, де вона знаходиться тощо.

Оптичне розпізнавання символів (OCR)

Оптичне розпізнавання символів, або OCR, – це технологія, яка дозволяє перетворювати відскановані документи, знімки екрана та інші цифрові зображення на електронні файли, які можна редагувати та шукати. OCR економить час і підвищує

ефективність, усуваючи необхідність ручного введення даних. Для виконання OCR цифрові зображення спочатку сегментуються та обробляються для виявлення оптичних шаблонів. Потім ці шаблони класифікуються як літери, цифри, символи тощо. У банківському секторі OCR також використовується для перевірки підписів.

Чат-бот

Кожен чат-бот працює за допомогою алгоритму машинного навчання для класифікації тексту на основі властивого йому шаблону речення та генерації відповідної відповіді. Куратор системи відповідає за зіставлення всіх можливих шаблонів з набором можливих відповідей. Цей метод перебору, що використовує обробку природної мови як основу, є ще одним чудовим прикладом застосування розпізнавання образів.

Розпізнавання зображень

На зображеннях розпізнавання образів можна використовувати для пошуку країв, ліній та форм. Це використовується в обробці зображень, комп'ютерному зорі тощо.

Розпізнавання медичних зображень

Одна з найпоширеніших проблем у медичній візуалізації стосується низької якості, що ускладнює інтерпретацію зображень рентгенологами.

Щоб подолати це, у біомедичній візуалізації використовуються методи комп'ютерного зору для виявлення наявності пухлин або ідентифікації початку захворювань. Ця комп'ютерна діагностика проводиться шляхом спостереження за значущими особливостями та аномаліями у закономірностях, які можуть бути приховані від людей.

Ці методи розпізнавання образів у поєднанні з обробкою зображень також використовуються в розробці ліків. Наприклад, секвенування ДНК відіграло важливу роль у розробці вакцини проти Covid.

Візуальний пошук зображень

Обробка зображень та комп'ютерний зір, що використовуються пошуковими системами та майданчиками електронної комерції, покладаються на методи розпізнавання образів для підтримки пошуку зображень.

Це працює так само, як і буквено-цифровий пошуковий запит, але з використанням зображень. Метадані зображень та додаткові текстові підказки підвищують ефективність результатів і допомагають краще фільтрувати варіанти на основі контексту.

Наприклад, такі технології широко застосовуються Google та Amazon.

Розпізнавання голосу

Розпізнавання образів використовується в пристроях з голосовою активацією для визначення шаблонів мовлення. Це дозволяє таким пристроям, як автомобільні навігаційні системи, Alexa та голосові пошукові системи, розуміти команди та реагувати на них.

Методи розпізнавання мовлення також використовуються в програмах для перетворення тексту в голос та голосу в текст, таких як Google Assistant. Це дозволяє людям з вадами зору чути та надсилати текст у відповідь.

Голосові помічники для бізнесу (наприклад, електронної комерції) також використовують ці методи, щоб забезпечити цілодобову підтримку мільйонам користувачів веб-сайтів і мобільних додатків.

Автоматичне розпізнавання мовлення – це технологія, яка може прослуховувати команди та реагувати на них, позбавляючи людей необхідності вводити довгі команди. Автоматичне субтитрування – це ще одна технологія, яка перетворює мовлення на текст, а потім відображає його на екрані. Це можна побачити на YouTube або Facebook, де субтитри генеруються автоматично для відео.

Робота голосових помічників

Крім того, розпізнавання образів допомагає ідентифікувати музику, скопійовану в іншого виконавця. Розглядаючи форми хвиль та амплітуди звуку, експерти можуть визначити, чи схожий один музичний твір на інший. Це може допомогти вирішити проблеми з авторським правом для музикантів.

Розвідка виявлення вторгнень

Розпізнавання образів можна використовувати для вирішення проблем безпеки, наприклад, шляхом виявлення громадянських заворушень через соціальні мережі.

Щохвилини в соціальних мережах генерується багато даних, і штучний інтелект може допомогти перетворити ці дані на корисну інформацію, виявляючи закономірності. Наприклад, Facebook використовує розпізнавання образів для виявлення фальшивих профілів, створених за допомогою фотографій профілів інших людей.

Комп'ютерні мережі мають системи виявлення вторгнень, які аналізують структуру даних та вхідного трафіку. Залежно від структури даних, вони можуть оцінювати будь-які аномалії або вторгнення в систему та допомагати запобігати атакам на захищені мережі.

Ключові висновки

Технологія розпізнавання образів використовується в аналізі великих даних для пошуку комбінацій властивих їм закономірностей, які часто або рідко зустрічаються разом. Ця інформація формує набір ознак для даних і допомагає в прогнозуванні невидимих даних.

Існує безкінечна кількість можливостей, оскільки розпізнавання образів стає все більш футуристичним та інтелектуальним, що має великий вплив на життя людини.

Майбутнє застосувань розпізнавання образів лежить у сфері обробки зображень, таких як медична діагностика, виявлення об'єктів, комп'ютерний зір, обробка природної мови, розпізнавання рукописного тексту та багато іншого.



Рисунок 1 – Структурна схема системи

Наскільки добре спрацьовують пристрої ідентифікації за особою?

Комп'ютери здатні робити усе більше різноч. речі, але, проте, вони не є чарівним засобом. Якщо самі люди часто не можуть довідатися суб'єкта, зображеного на фотографії, то якої надійності можна чекати від комп'ютера? Людський мозок найвищою мірою пристосований до розпізнавання осіб, приміром, маленькі діти запам'ятовують обличчя набагато краще, ніж будь-які інші форми. Крім усього іншого, людський мозок володіє набагато більшою, ніж комп'ютери, здатністю компенсації змін освітленості й кута зору. Справа в тому, що особи мають надзвичайно складний рисунок і часто відрізняються друг від друга тільки невлотимими деталями, тому нерідко як людині, так і комп'ютеру буває неможливо зіставляти зображення при наявності різниці у висвітленні, кута огляду камери, не говорячи вже зміни зовнішнього вигляду самої особи.

Тому не дивно, що проведені урядом США дослідження програмних засобів розпізнавання за особою встановили високий відсоток помилкового розпізнавання безневинних людей і ідентифікації їх з фотографіями інших осіб, що перебувають у базі даних, а також нездатність цих засобів розпізнати справжніх злочинців, навіть якщо їхній фото є в наявності в базі даних.

Приміром, дослідження, проведене Національним інститутом стандартів і технологій (NIST), установило, що рівень помилкової ідентифікації або нерозпізнавання суб'єктів, чий фотографії були зроблені всього 18 місяців назад, дорівнює 43%. При цьому фотографії, використані в дослідженні, були зняті в ідеальних умовах, що досить важливо, тому що

програми розпізнавання за особою дуже погано справляються з оцінкою зміни освітленості або кута нахилу камери. "Важкі" для них і фотографії із жвавим тлом. Дослідження NIST також дійшло висновку, що зміна кута нахилу камери на 45 градусів робить такі програми практично марними. Щонайкраще технологія розпізнавання особи спрацьовує в строго контрольованих умовах, коли суб'єкт дивиться прямо в камеру при яскравій освітленості. Правда, інше дослідження, проведене Міністерством оборони США, виявило високий рівень помилкової ідентифікації навіть при таких ідеальних умовах. Таким чином, від знімків із зернистим зображенням або старими фотографіями, типу тих, які зберігаються в особистих справах, буде дуже мало користі.

Крім цього, піднімалися питання про те, наскільки добре спрацьовують програми відносно темношкірих людей, риси особи яких можуть не розрізнятися об'єктивними, оптимізованими для зйомки людей зі світлою шкірою.

У розпорядженні уряду перебуває величезна, готова до використання база даних зображень осіб громадян – це фотографії водійських посвідчень. За законом, уряд не може продати ці фотографії приватним компаніям, однак не передбачено ніяких обмежень для використання цих знімків самим урядом для цілей відеоспостереження й ідентифікації. Федеральний уряд США приступилося до фінансування експериментальних проєктів по використанню фотографій з водійських посвідчень у базах даних систем біометричної ідентифікації.

Недоторканність приватного життя

Одна з потенційних погроз полягає в тому факті, що розпізнавання по рисунку особи в сполученні з усе більше широким застосуванням відеоспостереження згодом буде проникати в усі нові й нові області. Після установки подібного роду систем спостереження їхнє застосування рідко обмежується цілями, для яких вони були призначені споконвічно. Виникають всі нові способи їхнього використання, а організації й оператори таких систем часто не можуть устояти від спокуси розширити з їхньою допомогою свою владу й вплив, наносячи тим самим ще один удар по правах громадян. В остаточному підсумку, погроза полягає в тому, що широко застосовуване відеоспостереження змінить характер, сприйняття і якість повсякденного життя громадян.

Іншою погрозою є можливість зловживання. Застосування ідентифікації за особою в місцях суспільного користування, таких як аеропорти, залежить від широкого впровадження відеомоніторингу – проникаючої форми спостереження, за допомогою якої особистий і приватний характер поведінки може реєструватися графічними засобами. Досвід показує, що відеоспостереженням будуть зловживати. Системи відеокамер управляються звичайними людьми, які привносять на місце своєї роботи всі свої наявні упередження й упередженість. Наприклад, у Великобританії, де дуже широко використовуються камери відеоспостереження в публічних місцях, було виявлено, що оператори невинувато зосереджують увагу на темношкірих, оператори-чоловіки часто схильні "підглядати" за жінками.

Хоча поліцейське відеоспостереження не так широко поширене в США, розслідування, проведене газетою Detroit Free Press показало, які види зловживань можуть мати місце. Перевіряючи, як використовувалася база даних, доступна правоохоронним органам Мічигану, журналісти газети виявили, що поліцейські застосовували її для того, щоб допомогти своїм друзям або навіть колегам по роботі стежити за жінками, загрожувати водіям, відслідковувати подружжя, що живуть окремо, і навіть залякувати політичних опонентів. Неминуча істина полягає в тому, що чим більше людей мають доступ до бази даних, тим більше ймовірність, що цією базою даних будуть зловживати.

Розпізнавання за особою особливо піддано зловживанням, тому що дана технологія може використовуватися пасивним образом, тобто для її застосування не потрібне згода або участь суб'єкта, за яким ведеться спостереження. Камеру можливо встановити в будь-якому місці й "натренувати" її на людей. Сучасні телекамери легко забезпечують перегляд осіб з

відстані більше 90 м. Люди поведуться по-іншому, якщо знають, що за ними спостерігають, і мають право знати про те, що їхні рухи і їхнє поведіння відслідковуються.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів інтелектуального розпізнавання з використанням особливих точок. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем інтелектуального розпізнавання з використанням особливих точок.
- Досліджена система інтелектуального розпізнавання з використанням особливих точок.
- На основі отриманих результатів досліджень створена програмна реалізація системи інтелектуального розпізнавання з використанням особливих точок.

Розроблені алгоритми дозволяють успішно вирішувати завдання інтелектуального розпізнавання з використанням особливих точок. 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., Dorenskiy, 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., Мацуї 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., 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.
13. 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.
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., 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.
 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 користувацького 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., 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.
 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, 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.
 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., Neskoriadiya T., Fedorov E., Rymar P. «Neural Network Modeling Method of Transformations Data of Audit Production with Returnable Wastes». 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., 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., 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.
 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

О.Драганець, магістр гр. КІ-24Мз,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ГІПЕРКОНВЕРГЕНТНОЇ ІНФРАСТРУКТУРНОЇ ПЛАТФОРМИ

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

гіперконвергентна інфраструктурна платформа

Постановка проблеми. Не таємниця, що для кращого використання ресурсів, у будь-яких системах, інформаційні не виключення, ресурси варто збирати в загальні пули, для того, щоб їх можна було доцільно перерозподіляти. У комп'ютерингу оптимізація в частині використання ресурсів почалася давно, ще із систем розподілу часу. Потім прийшла черга віртуалізації. У другому десятилітті ХХІ століття фокус уваги природно змістився на гіперконвергенцію й дезагрегацію, тому що на даному рівні розвитку технологій створювати ресурсні пули можна цими двома альтернативними способами. Розходження між ними полягають у відношенні до віртуалізації. Якщо залишатися на фізичному рівні, то варто діяти засобами дезагрегації. Якщо ж фізичні ресурси можна перетворити у віртуальні, то тоді переважніше засобу гіперконвергенції. Гіперконвергенція дозволяє створювати програмно-центричні інфраструктури, у яких тісно інтегровані різноманітні «апаратні ресурси» (commodity hardware), але на ринок такі інфраструктури виводяться під брендом одного вендору.

Префікс «гіпер» припускає існування й просто конвергентних систем. Спільно два типи систем утворюють підхід, що споконвічно називали інтегрованим стеком (integrated stack). Загальним для обох є те, що в масштабований стек збираються три основні компоненти – мережі, сервери й системи зберігання інформації (СЗД), і вони поєднуються засобами віртуалізації й керування.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи гіперконвергентної інфраструктурної платформи.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи гіперконвергентної інфраструктурної платформи.

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

- Огляд існуючих систем гіперконвергентної інфраструктурної платформи.
 - Дослідження системи гіперконвергентної інфраструктурної платформи.
 - Програмна реалізація системи гіперконвергентної інфраструктурної платформи.
- Об'єктом дослідження є процес гіперконвергентної інфраструктурної платформи.

Предметом дослідження є методи гіперконвергентної інфраструктурної платформи.

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

Виклад основного матеріалу. Конвергентна й гіперконвергентна інфраструктури спрощують підтримку інфраструктури віртуальних робочих столів і віртуалізації настільних систем, оскільки вони розроблені з орієнтацією на просту установку й виконання складних завдань.

Конвергентна інфраструктура поєднує в одному корпусі чотири основних компоненти ЦОД: обчислювальні пристрої, пристрої зберігання, мережні пристрої й засоби віртуалізації серверів. Гіперконвергентна інфраструктура дозволяє домогтися більше щільної інтеграції більшого числа компонентів із застосуванням програмних засобів.

І в конвергентній, і в гіперконвергентній інфраструктурі всі елементи сумісні в роботі один з одним. Завдяки цьому ви зможете для своєї компанії одноразово закуповувати необхідні пристрої зберігання й мережні пристрої, а вони, як відомо, мають величезне значення в інфраструктурі віртуальних робочих столів. Це дозволяє спростити процес розгортання такої інфраструктури – те, чого так довго чекали й чому зрадіють багато компаній, яким необхідно здійснити віртуалізацію настільних систем.

Незважаючи на свою цінність і інноваційність, до даних технологій є кілька питань щодо цільового призначення й відмінностей. Спробуємо розібратися з тим, які функціональні можливості пропонують конвергентні й гіперконвергентні інфраструктури й чим вони відрізняються.

Що таке конвергентна інфраструктура?

Конвергентна інфраструктура поєднує в одному шасі обчислювальні пристрої, сховища, мережні пристрої й засоби віртуалізації серверів, завдяки чому ними можна управляти з одного місця. До можливостей керування може відноситися й керування інфраструктурою віртуальних робочих столів, залежно від обраної конфігурації й виробника.

Апаратні засоби, що йдуть у комплекті конвергентної інфраструктури, попередньо налаштовані на підтримку будь-яких цільових завдань: інфраструктури віртуальних робочих столів, бази даних, спеціальні додатки й так далі. Але фактично у вас немає достатньої волі для зміни обраної конфігурації.

Незалежно від обраного способу розширення середовища інфраструктури віртуальних робочих столів, ви повинні розуміти, що наступне вертикальне масштабування буде витратним і зажадає багато часу. Додавання окремих компонентів перетворюється стає складним і позбавляє вас багатьох переваг конвергентної інфраструктури. Додавання робочих машин і розширення ємності зберігання в корпоративній інфраструктурі може бути таким же дорогим, що говорить про необхідність правильного планування будь-якого розгортання інфраструктури віртуальних робочих столів.

З іншого боку, усе компоненти конвергентної інфраструктури можуть працювати протягом тривалого часу. Приміром, комплектний сервер такої інфраструктури працює добре навіть без інших компонентів інфраструктури.

Розвиток IT-Технологій не стоїть на місці, у світло виходять нові більше ефективні рішення, і одним з таких нововведень є конвергентні інфраструктури.

Converged Infrastructure (CI), або конвергентні інфраструктури, – це відроджені мейнфрейми, технологія CI насамперед дозволяє зібрати разом обчислювальні потужності роз'єднаних серверів, технології зберігання даних, що дозволяє забезпечувати більше ефективну динамічність систем. Поряд з розвитком цих технологій з'явилася й нечисленна категорія інших машин – analytic appliance, які дозволяють обробляти більші масиви даних буквально в режимі реального часу.

Що ж таке CI – конвергентна інфраструктура?

– CI – насамперед – це сукупність взаємодоповнюючих компонентів – модулів зберігання даних, серверів, програмного забезпечення, мережного встаткування, керування, а так само засобів автоматизації.

– CI – це продукт еволюції корпоративних ЦОД, у загальному виді, Converged Infrastructure – це мейнфрейми, що володіють більше оптимальною архітектурною гнучкістю.

Фахівці затверджують, що існує три основних причини придбання конвергентної інфраструктури:

- досить великий вік технологій віртуалізації;
- неминуче старіння нинішньої інфраструктури;
- визнана ефективність приватних хмар.

Розвиток конвергентних інфраструктур ні в кого не залишає сумніви, багато Хто IT-компанії вже спеціалізуються на розробці CI. Усім відомі VMware, Dell-EMC, Intel і Cisco запропонували ринку конвергентних інфраструктур Vblock, а NetApp, VMware і Cisco змогли запропонувати інфраструктуру FlexPod, корпорація Oracle є розроблювачем Private Cloud Architecture, а Dell має у своєму анамнезі Virtual Integrated System, а IBM представляє PureSystems.

Конвергентні інфраструктури умовно підрозділяються на три групи:

- Reference Architecture – референсна архітектура.
- Single Stack Infrastructure – інфраструктура єдиного стека.
- True Converged Infrastructure – істинно конвергентна архітектура.

Референсна архітектура

Референсна архітектура – це сукупність шаблонів рішень для CI. Сюди можна віднести VSPEX від EMC, а так само FlexPod від NetApp.

Основа FlexPod – це продукти NetApp, такі як, накопичувачі FAS6200, програмна ж частина – це операційна система Data ONTAP. Фактично, FlexPod – це не закінчене рішення, а до певної міри рекомендація зі створення архітектури.

Поки відомо кілька конфігурацій FlexPod, найпоширеніша з яких – це FlexPod для VMware, що збирається на базі vCenter Standard, Cisco Unified Computing System, комутаторів Nexus, а так само керуючого ПЗ.

VSPEX – у принципі, та ж сама референсна архітектура, але яка надає більшу волю вибору, але, загалом кажучи, він не поставляється окремо у вигляді самостійного продукту. Існує 14 конфігурацій, що підтримують хмарні додатки, у кожній з яких відбувається різне сполучення компонентів – керуючого ПЗ, гіпервізори, стійкові сервери, комутатори й системи зберігання.

Стекові інфраструктури

До таких інфраструктур можна віднести Dell Active System (раніше називалися vStart) і IBM PureSystems.

Dell Active System

Існує чотири версії Dell Active System, у кожній з яких зібрані в одну стійку системи зберігання, сервери, що управляє ПЗ. Кожна версія має індекс, що вказує число віртуальних машин – Active System 50, Active System 200, Active System 800 і Active System 1000. Установка цих систем досить проста, за словами розроблювачів, такі системи можуть являти собою подоба корпоративного iPod, у якому є тільки саме необхідне, тому що система призначена для простих користувачів, які не повинні зазнавати труднощів про відновленні ПЗ або моніторингу пристроїв. Саме рішення виконується в заводських умовах, користувач лише підключає його до мереж – електричної й інформаційної. Dell Active System складається із серверів PowerEdge, систем керування Dell Management, комутуючих пристроїв PowerConnect і пристроїв зберігання EqualLogic.

Всі системи оснащені передвстановленим гіпервізором, причому, якщо назва кінчається на m, те, виходить, система оснащена Microsoft Hyper-V, а v – VMware ESXi. Рішення vStart комплектуються Windows Server 2008 R2 Datacenter Edition, що надає більші можливості віртуалізації й використання Dell OpenManage, для якого необхідна наявність

спеціального процесора, що відслідковує системи зберігання й сервери. Моделі Dell Active System комплектуються двомісячною ліцензією ESXi, а так само консоллю vCenter Server.

Половина стійки займається версією Active System 50, де розташовані сервера PowerEdge R630 у кількості двох штук і пам'яттю до 64Гб у кожному, а так само комутатором на 24 порту, що підключається до мережі зберігання, і, крім того, дисковим масивом EqualLogic PS6100X обсягом 28,8 Тб.

Версія Active System 100 оснащена одним сервером PowerEdge R630, трьома Dell R730 і сховищем PS6000XV, а версія ctive System 200 уже має шість серверів R730 і два накопичувачі, крім того, обидві ці версії оснащені накопичувачем типу PowerConnect 6248.

IBM PureSystems

Розробка цієї системи велася ще з 2008 року, однак, про вихід продукту заявили лише у квітні 2012. Поки ще не можна повністю оцінити готове рішення, компанія IBM представляє лише перші наробітки в цій сфері. Фахівці затверджують, що поява PureSystems порівнянна з появою в 1964 році мейнфрейма System/360. Поряд із цим, IBM знову здобуває статус розроблювача закінчених рішень. Багато хто затверджує, що з появою PureSystems неминуче відбудеться поступовий відхід блейд-серверів.

Рішення PureSystems – це прорив, у ньому все ново – починаючи від самого виконання й закінчуючи системою керування. Загалом кажучи, PureSystems – це сімейство, що поки що містить у собі два члени – PureFlex System, а, крім того, PureApplication System. Перше рішення має три версії.

IBM PureSystems – прогрес даного рішення в наявності, навіть у конструктивних особливостях. Розроблювачі відмовилися від стандартного 1U форм-фактора, розробивши нове поняття «шасі», що може бути заповнено будь-яким устаткуванням, створеним у нових універсальних форм-факторах. Подібне рішення – це можливість для інтеграції в одну інфраструктуру всіляких систем – мережних і обчислювальних ресурсів, пристроїв зберігання й т.д. конструктивно система виконана у вигляді шасі 10U, причому, одна стійка може вмістити в себе 4 таких шасі. Подібна конструктивна реалізація доводить, що IBM зволіла піти від серверів-лез.

PureFlex System створена як інфраструктурна основа приватних хмар, складається із двох основних компонентів – це обчислювальні вузли, сконструйовані на основі процесорів Intel і IBM Power, а так само системи керування IBM Flex System Manager. СЗД у цьому випадку служать Storwize V7000. ОС для даного рішення – це Windows, SUSE Linux Enterprise Server і т.д, а гіпервізори – Microsoft Hyper V і VMware ESX.

Шасі Flex System Enterprise Chassis сконструйовано так, що має 14 або 7 місць, у яких розміщуються обчислювальні вузли. Усе шасі мають автономне живлення, потужні системи охолодження, керування й вводу-виводу. Два модулі Chassis Management Modules здійснюють керування, які працюють разом з модулем Integrated Management Module. У свою чергу система IBM Flex System Manager служить для віртуалізації, керування системою зберігання й мережами, а введення-вивід здійснюється за допомогою адаптерів, які дозволяють робити обмін даних по мережі Fibre Channel, FCo, Ethernet, і InfiniBand.

А от системи інтелекту PureFlex представлені в традиційні й зовсім нових формах. До традиційних рішень можна віднести системи підвищення надійності, зручності сервісу й готовності, крім того, систему виявлення причин виникаючих проблем, а так само зв'язок із сервісом IBM, одержання й зберігання даних про порушення системи. Крім того, система може протистояти мережним атакам і спробам злому.

Немаловажне значення має й технологія Expert Integrated System, що накопичує різний досвід роботи PureFlex, поки що вона не автоматизує використання системи, однак, помітно полегшує роботу оперативного персоналу, а, крім того, пред'являє занижені кваліфікаційні вимоги до операторів.

Загалом кажучи, існуюча база даних, що є сховищем шаблонів експертизи, що містять відомості, наприклад, про те, як правильно збалансувати навантаження, як розподіляти ресурси системи. Сама бібліотека створюється виробником системи, однак, доступ до неї

відкритий і для інших виробників ПЗ, вони так само можуть поповнювати її шаблонами, що рекомендують тієї або іншої дії.

Lenovo IBM Flex System здатна містити 4 різних обчислювальні моделі. Приміром, система Flex System x240, а так само IBM Flex p24L містить два сокета, призначених для ядер Intel Xeon, система IBM Flex p460 оснащена чотирма сокетом для процесорних рішень IBM Power7, а Flex System p260 – два сокет для того ж Power7, однак, всі моделі можуть мати до десяти різновидів, які розрізняються кількостями ядер, параметрами адаптерів і т.д.

За гнучкість введення-виводу відповідають до дев'яти контролерів, але в системі PureFlex відсутні убудовані системи зберігання інформації, за неї відповідають накопичувачі Storwize V7000.

Мабуть, навіть важко представити, які гігантські можливості надає подібний універсальний конструктор, тому для полегшення вибору компанія IBM виділяє три основних комплектації. Таким чином, для малого або середнього бізнесу призначаються System Express, System Standard – це підтримка стандартних корпоративних пропозицій, а System Enterprise – система, призначена для СУБД із більшим обсягом інформації й з підвищеною вимогою надійності.

PureApplication System

PureApplication System не сильно відрізняється від вищезгаданої системи PureFlex, однак, вона характерна не занадто розвитий мережною підсистемою, але більшою кількістю процесорів, крім того, рішення має убудовану систему зберігання. Рішення PureApplication дозволяє встановлювати від 96 до 608 ядер, оперативна ж пам'ять варіюється від 1,5 Тб до 9,7 Тб, сховище даних має обсяг 6,4 Тб на твердотільних дисках і 48 Тб звичайних жорстких дисків.

Існують так само платформи, призначені для певних класів застосунків. В 2008 році у світло вийшла платформа Exadata – Oracle Database Machine, що була створена разом з HP. Однак, уже через два роки була розроблена машина сполучні ПЗ – Exalogic Elastic Cloud. Обое рішення призначені для створення хмарних сервісів, характерні горизонтальною масштабованістю, а так само забезпеченням швидкої підтримки і розгортання застосунків.

Exalogic, в основному, призначена для взаємодії з Oracle Fusion Middleware, Oracle Fusion Applications, а так само Enterprise Java, однак, поряд із цим дозволяє використовувати й додатка, адаптовані до Weblogic. Дане рішення являє собою повністю зконфігуровану закінчену систему, що містить у собі сервери, модулі зберігання інформації, комутаційні компоненти. Існує три базові конфігурації – Full Rack, Half Rack і Quarter Rack, у кожній з яких є в наявності засоби резервування, необхідні мережні елементи, а так само кластеризована система даних. Конфігурація стійки дозволяє мати від 8 до 30 модулів обчислення як x86, так і x64. Цікаво, що обчислювальні модулі автономні й мають власне окреме живлення, а так само по двох накопичувача SSD, на яких утримуються діагностична інформація, а так само образ операційної системи. Система Exalogic заснована на мережі InfiniBand Fabric, що може зв'язувати компоненти, одержуючи, у підсумку, єдиний мейнфрейм. Подібне середовище розроблене для корпоративних Java-застосунків, крім того, існує друга версія цієї системи, у якій замість SSD твердотільних накопичувачів присутні звичайні магнітні жорсткі диски, що відповідають вимогам СУБД.

HPE CloudSystem Matrix

А от рішення HP CloudSystem Matrix засноване на архітектурі BladeSystem. Модель складається із сукупності мережних і обчислювальних елементів, модулів зберігання інформації, елементів живлення й системи охолодження. На даний момент відомі дві моделі – це BladeSystem Matrix, зібраний на RISC-процесорах, або на архітектурі x86. Базовий комплект цього рішення являє собою набір двох модулів комутування Virtual Connect Flex-10, сервер управління HP ProLiant DL360, а так само ПЗ Matrix Operating Environment, а рішення з ОС HP-UX характерно наявністю ліцензії HP-UX 11i v3 VSE-OE Integrity. Щоб забезпечити постійну доступність, а так само відновлення у випадку яких-небудь збоїв на платформу Integrity додається компонент HP Serviceguard.

Інфраструктура розроблена таким чином, що дозволяє планувати навантаження й виділення ресурсів системи, а так само вносити які-небудь необхідні зміни. У системі відбувається регулярне фіксування таких показників, як потужність, завантаження мережних ресурсів і процесорів. Великий спектр рішень HP BladeSystem Matrix, убудованих у систему може захистити й автоматично відновити робочий стан компонентів, а так само ліквідувати наслідку збоїв. За допомогою цієї системи віртуальні й фізичні сервера вертаються в робочий стан за секунди, а система Virtual Connect дозволяє швидко створювати локальні мережі, призначені для зберігання інформації всієї інфраструктури. подібна технологія дозволяє значно спростити зв'язність сервера й збільшити пропускну здатність мережі.

Технологія Matrix Orchestration Environment дозволяє значно спростити процес створення інфраструктури для конкретного додатка, а так само подальша його підтримка. У ході планування Matrix Orchestration Environment розробляє шаблон, у якому втримується опис серверів, а так само їхніх з'єднань між собою, після чого шаблон уже використовується для розробки конкретної конфігурації при створенні певної інфраструктури в Matrix.

Існує так само досить численна категорія інфраструктур, поява якої було обумовлено наявністю проблем великого обсягу даних. Подібні системи досить різноманітні, однак, їх поєднує повсюдне використання архітектур на основі масового паралелізму.

Подібні системи розробляються з 1984 року, уперше цією проблемою всерйоз зацікавилася фірма Teradata, її сьогодинішній продукт – це Active Enterprise Data Warehouse, що характерно наявністю власного зв'язку за назвою Bynet. Крім того, у цей час компанія Netezza пропонує власне рішення за назвою Performance Server, де відбувається сполучення стандартних лез зі спеціальними Snippet Processing Unit.

А от деякі компанії можуть запропонувати винятково програмні рішення даної системи, засновані на MPP-конфігураціях, як апаратна частина які використовую стандартні сервери. Універсальні такі системи тим, що не мають особливої прив'язки до тої або іншої апаратної конфігурації, у їхній основі лежить технологія MapReduce. Як приклад, може виступати рішення Vertica Analytics Platform, однак, система не виявляє особливих вимог до апаратної частини, єдине побажання розроблювачів – це двоядерні процесори – одне ядро призначене для ОС, а друге – для роботи з даними. Все інше, що необхідно для створення самої СУБД, уже закладено в системі.

Oracle Exalytics характерна наявністю 1 Терабайт оперативної пам'яті, а, крім того, 40 процесорів, а так само системою TimesTen In-Memory Database, що використовує алгоритм збереження даних, використовуваних найчастіше.

Конкурентами Exalogic поки що є IBM Smart Analytics Systems, а так само EMC Greenplum, однак, на відміну від цих систем, Exalytics здатний взаємодіяти тільки з Exadata, що служить джерелом даних Adaptive In-Memory Cache.

І останнє рішення в сфері конвергентних інфраструктур – це щира конвергентна інфраструктура, подібне рішення вийшло в результаті спільної роботи трьох корпорацій – Cisco, Dell EMC, VMware, а так що само примкнули Intel. У результаті їхньої діяльності світло побачила спільна організація за назвою Virtual Computing Environment. Дана фірма пропонує набір продуктів Vblock, характерних наявністю наступних компонентів – системи віртуалізації, такі як VMware vCenter Server, VMware vSphere, комутаторів Nexus і Cisco, системи обчислення – Cisco Unified Computing System, а так само технологій зберігання інформації EMC Symmetrix VMAX, систем безпеки RSA enVision, а так само апаратних елементів – кабелів, стійок, ІБЖ і т.д.

Подібне рішення досить непросте, тому його остаточне складання має деякі складності. У зв'язку із цим три корпорації об'єднали виробництво й поставку готових рішень. Така єдність значно спрощує процес створення й розгортання інфраструктур, тому що кожна модель перевірена й оптимізована для більше ефективного використання наявних ресурсів. Існує кілька версій Vblock – 0, 1, Series 300 і 700, які відрізняються розміру й технологіями зберігання даних. Початкове рішення – це версія Vblock 0, що сконструйована на накопичувачі Celerra, а саме потужне рішення – це версія Vblock 700 на системі

зберігання Symmetrix. Крім того, рішення середнього рівня, такі як Vblock 300, створені на основі накопичувача VNX. EMC Atmos – це система об'єктного зберігання, призначена для хмарних обчислень, що підтримує обсяги даних до петабайта.

Загалом, розвиток конвергентних інфраструктур – це прорив у сфері IT-Технологій, що приведе до відсутності необхідності безлічі фахівців, що працюють у сфері певних технологій. Крім того, безліч підприємств зможе підібрати необхідні для себе рішення, налаштовані для рішення тих або інших виробничих завдань.

Що таке гіперконвергентна інфраструктура?

Гіперконвергентна інфраструктура була побудована на базі конвергентної інфраструктури й поданні про програмно-визначаємий ЦОД. Вона поєднує все компоненти звичного нам ЦОД в одній системі. Всі чотири ключових компоненти конвергентної інфраструктури на місці, але іноді в неї також входять додаткові компоненти, такі як ПЗ для резервного копіювання, можливості миттєвих знімків, функціонал дедуплікації даних, проміжне стиск, оптимізація роботи глобальної обчислювальної мережі (ГОМ) і багато чого іншого. Конвергентна інфраструктура в першу чергу опирається на апаратні засоби, а програмно-визначаємий ЦОД найчастіше адаптується під будь-яке апаратне забезпечення. У гіперконвергентній інфраструктурі ці дві можливості об'єднані.

Підтримка гіперконвергентної інфраструктури здійснюється одним постачальником. Нею можна управляти, як однією системою за допомогою єдиного набору інструментів. Для розширення інфраструктури просто потрібно встановити блоки необхідних пристроїв і ресурсів (наприклад, сховище) в основний системний блок. І робиться це буквально на лету.

Тому що гіперконвергентна інфраструктура є програмно-визначаємий (тобто, робота інфраструктури логічно відділена від фізичного встаткування), взаємна інтеграція компонентів більше щільна, чим у звичайній конвергентній інфраструктурі, а самі компоненти повинні перебувати поруч, щоб працювати коректно. Це дозволяє використовувати гіперконвергентну інфраструктуру для підтримки ще більшої кількості робочих навантажень, чим у випадку зі звичайною конвергентною інфраструктурою. Це пояснюється тим, що в ній є можливість зміни принципу визначення й налаштування на програмному рівні. Крім того, ви зможете зробити так, щоб вона працювала зі спеціалізованими додатками й робочими навантаженнями, чого попередньо налаштовані конвергентні інфраструктури робити не дозволяють.

Гіперконвергентна інфраструктура особливо коштовна для роботи з інфраструктурою віртуальних робочих столів, оскільки дозволяє виконувати швидке масштабування без додаткових витрат. Найчастіше у випадку із класичною інфраструктурою віртуальних робочих столів всі зовсім по-іншому – компаніям перед масштабуванням необхідно купувати більше ресурсів або чекати, поки віртуальні робочі столи використовують виділений простір і мережні ресурси, а потім по факті додавати нову інфраструктуру.

Обидва сценарії вимагають серйозних грошових і тимчасових витрат. Але, у випадку з гіперконвергентною інфраструктурою, при необхідності розширення сховища ви можете просто встановити необхідні пристрої в існуючих стек. Масштабування можна виконувати швидко – протягом часу, необхідного для поставки встаткування. При цьому вам не прийде проходити повну процедуру повторної оцінки й перенастроювання корпоративної інфраструктури.

Крім того, при переході з фізичних ПК на віртуальні робочі системи вам будуть потрібні пристрої для виконання всіх обчислювальних операцій, які звичайно виконують ноутбуки й ПК. Гіперконвергентна інфраструктура із цим дуже допоможе, оскільки найчастіше йде в комплекті з більшим обсягом флеш-пам'яті, що позитивно позначається на продуктивності роботи віртуальних робочих столів. Це підвищує швидкість операцій введення/виводу, згладжує роботу при високих навантаженнях, і дозволяє вам виконувати сканування на віруси й інші види моніторингу у фоновому режимі (не відволікаючи користувачів).

Гнучкість гіперконвергентної інфраструктури робить її більше масштабованою й рентабельною, у порівнянні з конвергентною, оскільки в ній є присутнім можливість додавання обчислювальних пристроїв і пристроїв зберігання в міру необхідності. Вартість початкових капіталовкладень для обох інфраструктур висока, але в довгостроковій перспективі вартість вкладених коштів повинна окупитися.

На сьогоднішній день багато замовників у сфері середнього й великого бізнесу переходять до використання гіперконвергентних систем при розгортанні корпоративної ІТ-інфраструктури, і це обумовлено безумовними плюсами даних систем: легкістю масштабування і єдиним програмним інтерфейсом керування.

Гіперконвергентні системи поєднують у собі сервери, системи зберігання даних, мережний функціонал і програмне забезпечення. Такий підхід дозволяє знизити тимчасові й бюджетні витрати при створенні інфраструктури, а також спрощує експлуатацію системи.

По даним Gartner ринок гіперконвергентних платформ (HCI – Hyper-Converged Infrastructure) стрімко росте й досягне до 2026 року 5 мільярдів доларів. на даний момент HCI найбільш застосовні в сфері корпоративних ЦОД з кількох причин:

- Вирішують завдання масштабування ІТ-інфраструктури.
- Знижують витрати на розширення ІТ-інфраструктури.
- Зменшують кількість керованих систем.
- Збільшують швидкодію за рахунок використання SSD-Накопичувачів.
- Оптимізують програмну й апаратну платформи для спільної роботи.

Крім цього HCI дозволяють розгорнути програмно-конфігуруємі ЦОДи (SDDC)

Архітектура й рішення різних виробників

HCI, як правило, складаються з декількох модулів, що становлять горизонтально-масштабований кластер, що містить звичайно від 4 до 64 вузлів. Кожний з вузлів містить у собі обчислювальне ядро, систему зберігання, мережні ресурси й гіпервізор.

Крім цього, HCI поставляються програмним забезпеченням для розподілу ресурсів системи й керування масштабуванням. ПЗ може бути встановлене заздалегідь або поставлятися окремо – більша частина HCI-рішень поставляється із передінстальованими програмними компонентами.

Крім традиційних HCI існують і рішення з референсною архітектурою, що дозволяє компонувати HCI під конкретне завдання. Такі системи пропонують розроблювачі платформи EVO:RAIL. Система Glob від компанії Green IT може використовувати зовнішню СЗД, різні процесори, включаючи бюджетні варіанти Intel Xeon. Рішення Huawei FusionCube дозволяє вибирати блейд-вузли половинної або повної довжини з різними типами накопичувачів. Крім цього, деякі системи, наприклад, NetApp FlexPod використовують замість традиційних СЗД системи SDS.

Завдання й сценарії роботи

Більшість із існуючих HCI здатні вирішувати широке коло завдань:

- Підтримка застосунків аналітики й систем OLTP.
- Підтримка критично важливих застосунків.
- Створення ресурсного пула на основі серверів і модернізація інфраструктури ЦОДа.

- Розгортання VDI і часток хмарних систем.

HCI можна застосовувати для віртуалізованих застосунків, при цьому для різних віртуальних середовищ використовуються спеціальні конфігурації. Наприклад, для середовищ VMware оптимізовані системи VxRail, що використовують програмне забезпечення VMware vSphere і VMware VSAN. Цільовими завданнями цієї платформи є: аналітика «великих даних», Microsoft Exchange, САПР, наукові розробки, середовища вилучених філій і офісів, а також навантаження з підвищеними вимогами до графічних ресурсів.

Крім цього, виробники пропонують референсні системи для більше вузького класу навантажень, таких як додатка ERP і CRM.

Завдяки гнучкості рішень, великій кількості виробників і широкому вибору продуктів системи HCI закономірно займають свою нішу в сфері великого бізнесу при розгортанні масштабних ЦОД. Разом з тим, з'являються нові системи, які можуть бути актуальні для замовників у сфері середнього бізнесу, що робить ринок HCI-рішень одним з тих, що найбільш розвиваються в IT-індустрії на сучасний момент.

Недовга історія гіперконвергенції, що почалася із середини нульових років XXI століття, цікава своєю еволюцією. Початок був покладений утворенням альянсів декількома компаніями, що досить нетипово для ринку. Спільно вони запропонували так звані інтегровані стеки. Раніше інших – група VCE (VMware, Cisco й EMC) зі своїм Vblocks, потім група в складі VMware, Cisco і NetApp з мережею зберігання Fco і стеком FlexPod. Слідом був секстет у складі Dell, Fujitsu, HP, Microsoft, IBM і NEC з рішенням навколо гіпервізора Microsoft Hyper-V, а також дві самостійні компанії – Oracle з рішенням Exalogic і HP з Matrix.

Консолідовано виниклий рух в одному напрямку найбільших виробників змусило задуматися про фундаментальність передбачуваного зрушення.

І насправді, поява інтегрованих стеков змінило правила гри.[1] Раніше підприємству не залишалося нічого іншого, як збирати системи власними силами або прибігати до послуг компаній-інтеграторів, а інтегрований стек можна було купити готовим, майже як домашній кінотеатр. Зрозуміло, тонкі цінителі й критики, яких у комп'ютерингу не мало, завжди знайдуть у будь-якому інтегрованому рішенні масу недоліків. Так було, наприклад, з інтегрованими пакетами ПЗ для ПК. Об'єднання редакторів, СУБД і електронних таблиць в одному продукті приймалося ними в багнети доти, поки не з'явився один загальний Microsoft Office, на цьому всі дискусії закінчилися.

Суперечки ні, за окремими показниками готовий комплекс може уступати спеціалізованим рішенням, але в нього є головне достоїнство – можливість зсуву витрат з експлуатаційних (OpEx) у бік інвестиції в нові рішення (CapEx), тобто на підтримку виконання нового функціонала. Продовживши паралель із аудіо, можна сказати, що готові інтегровані стеки дозволяють витрачати більше грошей на музику, а не на техніку для її відтворення.

Потім виникло нове узагальнене поняття «конвергентні інфраструктури» (Converged Infrastructure, CI).[2] Звичайно під CI розуміють цілісне закінчене рішення, зібране із взаємодоповнюючих готових компонентів: серверів, систем зберігання, комунікаційного встаткування й ПЗ для керування інфраструктурою, що включає засобу для автоматизації й оркестровки. У деяких випадках до складу CI можуть входити ще й спеціалізовані апаратні модулі керування. Керуюче ПЗ й спеціалізовані модулі забезпечують централізоване керування звичайно віртуалізованими й об'єднаними в загальні пули ресурсами, що розподіляються між різними додатками. Це підвищує економічну ефективність і знижує вартість експлуатації. Поява CI стало закономірним результатом еволюції корпоративних ЦОД у напрямку до приватних хмар.

За ступенем консолідованості CI можна розділити на три групи:

- шаблон, або референсна архітектура (Reference Architecture, RA);
- інфраструктура єдиного стека (Single Stack Infrastructure, SSI);
- істинно конвергентна інфраструктура (True Converged Infrastructure, TCI).

У першому випадку консолідація зводиться до окремих конфігурацій, які рекомендувалися, що складається з компонентів від різних виробників. У другому – весь стек устаткування виробляється й збирається в єдине ціле, а в третьому – у єдине ціле збираються компоненти від різних виробників, тобто в TCI об'єднані переваги RA і SSI.[3]

І, нарешті, ще один логічний крок. Його зробила компанія-стартап Nutanix, запропонувавши Complete Cluster – масштабовану інфраструктуру, що поєднує в собі складові частини корпоративної системи: комп'ютерні ресурси й ресурси систем зберігання у

формі однакових базових модулів. Надалі саме такі інфраструктури стали називати гіперконвергентними (Hyperconverged Infrastructure, HCI).[4]

Відмінна риса Complete Cluster і всіх його послідовників складається в можливості збирати з модулів приватна корпоративна хмара без додаткових вкладень у мережні СЗД SAN або NAS. Ідея Complete Cluster, здавалося б, лежала на поверхні. Відомо, що успіх таких гігантів, як Google, Yahoo, Amazon і Facebook, значною мірою базується на власних блокових пропріетарних технологіях, використовуваних для створення ЦОД. Чому б не застосувати аналогічні підходи до істотно меншим корпоративних ЦОД із класичними серверами й системами зберігання, адаптованими до традиційних навантажень? Такого роду запозичення досвіду має сенс, оскільки в сучасних корпоративних ЦОД, незалежно від їхнього масштабу, домінують близькі віртуалізовані навантаження.

Засновники Nutanix раніше інших звернули увагу на дві проблеми класичних ЦОДів, що складаються із серверів, SAN і NAS. Перша пов'язана зі спадщиною старих традицій – ЦОД створювалися розраховуючи на статичне навантаження, а нове подання про динамічне навантаження виникло у зв'язку з віртуалізацією серверів і переходом до хмар. Динаміка полягає в необхідності на лету створювати віртуальні машини, переміщати їх між серверами, однак у цих умовах керування існуючими мережними системами зберігання стає складн і незручним і відмахнутися від цієї проблеми вже не можна.

Росте кількість віртуальних машин, обсяг даних, якими вони оперують, збільшується, причому в чималому ступені кількісним змінам сприяють нові технології віртуалізації, зокрема, віртуалізація настільних систем.

Ще одна проблема сучасних ЦОДов виникає через те, що вони проектувалися з урахуванням невідповідності між усе більше зростаючою продуктивністю процесорів і повільністю, у силу їхньої механічної природи, жорстких дисків. Цей розрив приймався як даність, і його доводилося компенсувати за допомогою тих або інших методів розподілу даних по дисках. Однак з'явилися твердотільні накопичувачі (SSD) зі швидкістю обміну на два-три порядки вище, ніж у традиційних жорстких дисків (HDD), що могло б нівелювати розрив, але інфраструктура виявилася не підготовлена до них, і проста заміна HDD на SSD створює нову проблему – існуючі мережі не в змозі впоратися зі зростаючою потребою у швидкості передачі даних, що утрудняє використання переваг SSD.

В Nutanix відверто визнавали, що вони запозичили підхід до горизонтального масштабування, а їхній власний внесок складається в поширенні методики Google на корпоративні системи й пропозиції створення «готових до вживання» блоків для будівництва корпоративних систем. Для того щоб застосувати Complete Cluster до умов окремо взятого підприємства, загальну ідею довелося серйозно переробити. Якщо Google File System являє собою власне замовлене рішення, адаптоване для специфічних внутрішніх застосунків (пошук і електронна пошта), то Nutanix пропонує більше загальне рішення, адаптоване до умов корпоративної віртуалізованого середовища з упором на її особливі вимоги: ефективне керування даними, високу готовність, резервування, відновлення після збоїв.

Архітектура Nutanix Complete Cluster являла собою кластер з горизонтальним масштабуванням, зібраний з високопродуктивних вузлів. Окремий вузол має у своєму составі процесори, пам'ять і локальну систему зберігання, що складає з дисків HDD і SSD. На кожному вузлі працює власний екземпляр гіпервізора. Вузол служить хостом для працюючих на ньому віртуальних машин. Для об'єднання ресурсів окремих систем зберігання в єдиний віртуалізований пул служить SOCS (Scale-out Converged Storage) – аналог Google File System. Віртуальні машини за допомогою SOCS оперують даними точно так само, як якби вони працювали з SAN, інакше кажучи, SOCS служить у якості гіпервізора систем зберігання, переміщаючи дані якнайближче до тої віртуальної машини, на якій вони використовуються, що підвищує продуктивність і знижує вартість. Крім того, Complete Cluster служить інструментом для горизонтального масштабування аж до декількох сотень вузлів.

Порівнюючи CI і HCI, можна використовувати будівельну аналогію. У першому випадку конструкцію збирають із визначеного набору великих блоків від зв'язаних між собою виробників, а в другому використовують підходящі з наявних на ринку цегл. Звичайно в створенні CI провідна роль належить тому зі членів альянсу, хто поставляє керування, але про інших, хто поставляє сервери, СЗД, мережі й віртуалізацію, теж не забувають. А системи класу HCI поставляються одним вендором, він збирає все необхідне в корпус (box) такими необхідними речами як засобу для резервного копіювання, створення снеп-шотів, дедуплікації, компресії в режимі in-lint і т.буд. Конкретний состав набору в різних виробників може варіюватися, деякі, наприклад, SimpliVity, для прискорення використовують власні спеціалізовані інтегральні мікросхеми ASIC.

Ким би не була зроблена HCI, створюється віртуалізована інфраструктура, точніше кажучи, інфраструктура, віртуалізована по визначенню. Вона має наступні достоїнства:

- Гнучкість – реалізуються можливі типи масштабування.
- Економічна ефективність – знижуються як CAPEX, так і OPEX.
- Висока готовність – природне резервування блоків і швидка реконфігурація.
- Захищеність даних – дані не прив'язані до єдиного з погляду уразливості місцю.
- Ефективність роботи з даними – скорочуються витрати на СЗД і мережі.

В HCI реалізуються три типи масштабування: добре відоме по кластерах горизонтальне (scale out), по мейнфреймам і Unix-серверах вертикальне (scale up) і нове scale through.

Якщо порівнювати два підходи – гіпервіртуалізацію з дезагрегацією, то можна виразити обережне припущення про те, що в цих двох підходів можуть бути різні споживачі. У програм-гіпервізорів і в технології віртуалізації в цілому є межі, тому HCI, швидше за все, не вийде за межі приватних хмар. У дезагрегації меж немає, тому її сфера застосування – ЦОДи компаній-гіперскейлерів, постачальників послуг глобальних хмар.

Програмні й мережні рішення для гіперконвергентних інфраструктур

Гіперконвергентні інфраструктури (HCI) стають однією з найбільш перспективних технологій для створення приватних і гібридних хмар. Ідею HCI запропонували стартапи, які раніше інших осознали можливість радикальних змін і що встигли зайняти лідируючі позиції в цьому сегменті ринку. Однак останнім часом і галузеві великовагові поїзди, що як звичайно затрималися на старті, але які володіють достатнім науковим і технічним потенціалом, роблять все можливе, щоб зайняти належне їм положення.



Рисунок 1 – Структурна схема системи

Загальна ситуація така: незалежно від того, під яким брендом виробляється та або інша конкурентна НСІ, вона складається із чотирьох взаємозалежних компонентів – сервери, СЗД, мережа й віртуалізація СЗД із метою створення загальних пулів (Storage Pool). Щодо цього, мабуть, єдине виключення являє собою зовсім що недавно з'явився трикомпонентний підхід до утворення НСІ на базі Intel Xeon Scalable із чип-сетом Intel C620 і СЗД Optane SSD.

Як постачальник НСІ, за рідкісним винятком, виступають компанії, що забезпечують функціонала, а саме два перших з перерахованих вище чотирьох компонентів. Вони можуть самі робити сервери й/або СЗД, або ж можуть здобувати їх, практично не маючи власного виробництва, тобто бути, як зараз говорять, фаблес.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів гіперконвергентної інфраструктурної платформи. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем гіперконвергентної інфраструктурної платформи.
- Досліджена система гіперконвергентної інфраструктурної платформи.
- На основі отриманих результатів досліджень створена програмна реалізація системи гіперконвергентної інфраструктурної платформи.

Розроблені алгоритми дозволяють успішно вирішувати завдання гіперконвергентної інфраструктурної платформи. 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. 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.
2. 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.
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. 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.
6. 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.
7. 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.
8. 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.
9. 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.
10. 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.
11. 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.
12. 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.
13. 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.
 14. 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.
 15. 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.
 16. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
 17. 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.
 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., 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.
 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., 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.
 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., 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.
 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., 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.
 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.

УДК 004

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

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ЗАХИСТУ КОРПОРАТИВНИХ ДОДАТКІВ, ЯКІ РОЗРОБЛЯЮТЬСЯ ЗА ДОПОМОГОЮ МЕТОДОЛОГІЇ AGILE

У статті розроблено програмне забезпечення, яке призначено для системи захисту корпоративних додатків, які розробляються за допомогою методології Agile. Метою розробки є дослідження та принципи побудови системи захисту корпоративних додатків, які розробляються за допомогою методології Agile. Об'єктом дослідження є процес захисту корпоративних додатків, які розробляються за допомогою методології Agile. Предметом дослідження є методи захисту корпоративних додатків, які розробляються за допомогою методології Agile. Методи дослідження базуються на методах захисту інформації у комп'ютерних мережах, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи захисту корпоративних додатків, які розробляються за допомогою методології Agile. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

система захисту, корпоративні додатки, Agile

Постановка проблеми. Гнучка розробка програмного забезпечення (Agile) – це тип методології, який зосереджений на основному принципі гнучкості. Методи гнучкої розробки визнають, що для отримання найкращих кінцевих продуктів у найкоротші терміни може знадобитися зміна культури або мислення поряд з іншими змінами в процесі. Незважаючи на широке впровадження з моменту першого впровадження на початку 2000-х років з Agile-маніфест, за останні п'ять років DevOps став стандартною методологією, яка використовується для створення чудових програмних продуктів. Однак сьогодні, DevSecOps – це золотий стандарт розробки безпечних додатків.

Створення гнучкого середовища розробки пропонує кілька ключових переваг. Сучасний бізнес працює швидше, ніж будь-коли раніше, тому команди розробників повинні мати можливість своєчасно реагувати на ринкові сили, водночас надаючи пріоритет ефективній доставці програми. Agile надає платформу, яка дозволяє командам швидко рухатися та створювати високоякісні продукти завдяки таким методам, як постійне тестування протягом усього процесу розробки. Пошук більш гнучких методів розробки дозволяє забезпечити безпечніший життєвий цикл розробки програм від коду до хмари. Успішне впровадження практик безпеки разом зі гнучкою розробкою програмного забезпечення дозволяє швидко розробляти безпечний код, або DevSecOps.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи захисту корпоративних додатків, які розробляються за допомогою методології agile.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи захисту корпоративних додатків, які розробляються за допомогою методології Agile.

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

- Огляд існуючих систем захисту корпоративних додатків, які розробляються за допомогою методології Agile.

– Дослідження системи захисту корпоративних додатків, які розробляються за допомогою методології Agile.

– Програмна реалізація системи захисту корпоративних додатків, які розробляються за допомогою методології Agile.

Об'єктом дослідження є процес захисту корпоративних додатків, які розробляються за допомогою методології Agile.

Предметом дослідження є методи захисту корпоративних додатків, які розробляються за допомогою методології Agile.

Методи дослідження базуються на методах захисту інформації у комп'ютерних мережах, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Навіть якщо ви бездоганно дотримувалися всіх найкращих практик гнучкої розробки, у гнучкій розробці програмного забезпечення все одно існують ризики. Гнучка розробка програмного забезпечення довела, що вона пропонує більше переваг, ніж недоліків, тому важливо розуміти потенційні ризики безпеки щоб ви могли пом'якшити їх завчасно.

Відсутність документації процесу

Agile надає пріоритет робочим продуктам над документацією. Деякі Agile-команди доводять це до крайності та прагнуть до нульової документації, але більшість типових, добре функціонуючих Agile-команд зосереджуються на мінімізації документації та забезпеченні того, щоб документування додавало цінності.

Однак така практика створює певні ризики в розробці програмного забезпечення. Agile надає пріоритет гнучкості (що добре), але це може призвести до швидкої послідовності швидких змін, що полегшує втрату сліду за документацією процесу.

Коли ви втрачаєте контроль над документацією процесу, ви не можете гарантувати дотримання всіх протоколів безпеки, оскільки довідкової документації може не існувати, або її зберігання в узгодженому вигляді не було пріоритетом. Для забезпечення безпечної розробки додатків ідеально мати певну довідкову документацію, незалежну від продукту. У цьому випадку підвищена гнучкість, пов'язана з меншою кількістю документації, може збільшити вашу вразливість до порушень безпеки.

Щоб зменшити проблеми безпеки, пов'язані з браком документації, зосередьтеся на більш тісному впровадженні безпеки в процес розробки у формі «чемпіонів безпеки» в команді розробників або шляхом автоматизації деяких форм документації для створення історичного запису, до якого можна буде звертатися пізніше. Однією з головних проблем, з якими сьогодні стикаються керівники інформаційних систем (CISO) та їхні команди безпеки, є розуміння процесів розробки додатків, які їм доручено захистити, оскільки в організації немає документації щодо того, які системи використовуються розробниками. Зараз існують сучасні інструменти безпеки, такі як SaaS-платформа Legit Security, яка може автоматично виявляти та інвентаризувати активи SDLC – автоматично створюючи документацію, до якої команди безпеки можуть отримати доступ за потреби.

Цикл швидкого вивільнення

Гнучка методологія допомагає створити середовище для швидких релізів, але оскільки великий пріоритет надається забезпеченню цінності продукту протягом спринту, безпека часто відходить на другий план порівняно з розробкою основної функціональності продукту на ранніх етапах життєвого циклу розробки програмного забезпечення (SDLC). На жаль, це виявилось антипаттерном. Знижуючи пріоритет безпеки на ранніх етапах розробки програмного забезпечення, ви створюєте борг безпеки, який буде вирішено пізніше, коли для усунення цієї помилки безпеки буде набагато більше ресурсомістких ресурсів. Крім того, бізнес взяв на себе більшу відповідальність за ризик протягом цього часу, якщо помилка безпеки стане використаною вразливістю. Прагніть інтегрувати безпеку в гнучкі методи розробки.

Замість того, щоб просто пріоритезувати випуск коду, зосередьтеся на забезпеченні дотримання протоколів тестування вразливостей безпеки. Це може допомогти впровадити

підхід «безпека понад усе» до гнучкої розробки та уникнути потенційних ризиків для безпеки. У дусі «гнучкої безпеки» докладайте всіх зусиль для автоматизації перевірок безпеки та програмної оцінки дотримання протоколів безпеки.

Поява нових загроз

Оскільки гнучка розробка зосереджена на постійному вдосконаленні та невеликих обсягах роботи, релізи можуть створювати нові ризики безпеки, яких можна було б уникнути, якби ми продумали це наперед. Крім того, гнучкі методології іноді використовуються як привід для уникнення ретельного планування та підготовки. Команди, які недалекоглядно зосереджені лише на розробці наступного нового релізу, можуть не враховувати, як може змінитися ландшафт загроз з новим релізом (тобто розробники не є експертами з безпеки). В результаті такого сценарію зловмисники можуть легше використовувати будь-які приховані вразливості в гнучкому середовищі розробки.

Одним із поширених прикладів цього в сучасній індустрії програмного забезпечення є використання жорстко закодованих секретів у вихідному коді. Ця практика не викликала великого занепокоєння десять років тому, коли концепція хмарного програмного забезпечення, що надається як послуга, перебувала на ранніх стадіях впровадження на ринку. Однак протягом останнього десятиліття більшість гнучких розробників програмного забезпечення не зробили жодного кроку назад, щоб оцінити вплив SaaS та жорстко закодованих секретів. Це створило новий вектор атаки, де зловмисники прагнуть отримати доступ до систем управління вихідним кодом та вихідного коду, щоб отримати подальший доступ до інших систем (наприклад, серверів збірки), крадучи жорстко закодовані секрети. Короткозоро зосереджуючись на кожному спринті. Програмна галузь в цілому пропустила кричущу проблему безпеки, яка тепер стала головною проблемою.

Коли виникають нові загрози, вирішуйте їх двома способами:

Аудит вашої існуючої поверхні атаки, щоб оцінити поточний ризик і визначити пріоритети виправлень безпеки.

Вбудовуйте методи для ітеративного аудиту поверхні атаки, що постійно та автоматично відповідає вашому існуючому процесу розробки, щоб запобігти подальшому ризику.

Щоб впоратися з появою нових загроз за допомогою цього двостороннього підходу, організаціям необхідно впровадити стратегію внутрішніх команд для покращення безпеки та безперервного навчання.

Недостатня обізнаність та навчання з питань безпеки

Загальновідомо, що безпека часто відходить на другий план як з боку внутрішніх команд, так і з боку клієнтів та сторонніх ресурсів на користь більш безпосередньої діяльності, що «генерує дохід». В епоху атаки на ланцюги поставок програмного забезпечення. Однак таке мислення небезпечно застаріло. Простіше кажучи, атака SolarWinds чітко показала, що існує новий тип загрози, яка безпосередньо призведе до втрати клієнтів, оскільки зловмисники тепер прагнуть атакувати ваших клієнтів *через вас*. Ось чому важливо підкреслювати та сприяти підвищенню обізнаності та навчанню з питань безпеки для всіх сторін.

Замість того, щоб зосереджуватися лише на швидкості та термінах виконання, виділіть спеціальний час для навчання з питань безпеки та протоколів безпеки. Прагніть досягти гнучку безпеку. Використовуйте сучасні інструменти безпеки ланцюга постачання програмного забезпечення, які надають агрегований «оцінку безпеки» за лінійкою продуктів та командою розробників. Таким чином, ви можете застосовувати більше навчання з безпеки до команд розробників, які цього найбільше потребують, не обтяжуючи при цьому вже безпечні команди розробників. Завдяки гейміфікації практик безпеки за допомогою оцінок безпеки за лінійкою продуктів, організації можуть перейти до фази посилення гнучкої безпеки.

Необмежений доступ до репозиторіїв вихідного коду та конвеєрів CI/CD

Нерідко трапляється просто надавати загальні дозволи та авторизації великим групам команди розробників, особливо в невеликих організаціях з менш розвиненими практиками безпеки. Більша кількість користувачів з доступом до репозиторіїв коду, систем керування вихідним кодом (SCM), серверів збірки, реєстрів артефактів та конвеєрів CI/CD означає більший ризик для вашого SDLC. Кожен користувач із надмірними привілеями являє собою ще одне слабе місце у вашому захисті, яке стає мішенню для зловмисників. Крім того, команди розробників програмного забезпечення часто передають певну частину розробки зовнішнім, контрактним командам розробників на проєктній основі. Часто ці підрядники зберігають свої дозволи ще довго після завершення проєкту. Ризики для гнучкої розробки програмного забезпечення особливо критичні, коли привілеї адміністративного рівня надаються занадто вільно.

Підвищте свою гнучку безпеку, дотримуючись найкращих практик гнучкої розробки. Перегляньте дозволи та протоколи авторизації для вашої команди розробників та систем, які вони використовують для швидкої розробки програмного забезпечення. Використовуйте принцип найменших привілеїв, щоб кожен користувач мав лише ті дозволи, які необхідні для виконання його роботи.

Якщо кількість розробників, які мають доступ до ваших конвеєрів розробки, коливається від 0 до 50 осіб, ручний підхід може бути можливим і бажаним; однак для команд, що налічують понад 50 розробників, найкраще використовувати такий інструмент, як платформа Legit Security, щоб допомогти вам визначити поточні ризики доступу, присутні у ваших конвеєрах розробки, перш ніж зловмисник скомпрометує застарілі облікові записи, які, як ви помилково вважали, більше не мають доступу до ваших конвеєрів.

Невміння керувати конфіденційними даними

Багато команд розробників розуміють основні принципи безпеки, але більшість із них не дуже добре обізнані з тим, як інтегрувати практики безпеки навколо управління даними таким чином, щоб це відповідало найкращим практикам гнучкої розробки.

Повний перелік ризиків безпеки, пов'язаних з управлінням конфіденційними даними, є довгим і виходить за рамки цього блогу, але деякі з найбільших викликів у DataOps – це (1) впровадження проактивного управління даними, (2) маркування конфіденційних даних та (3) навчання команд прийнятним практикам роботи з даними.

Ось кілька порад щодо кращого управління конфіденційними даними: Централізувати управління ідентифікацією; Визначення прав доступу на основі ролей; Маскування конфіденційних даних; Відмовтеся від ручного захисту даних та *автоматизуйте його*, коли це можливо; Постійно скануйте код на наявність конфіденційних даних.

Оскільки команди безпеки та розробки стають більш узгодженими, вигідно мати «чемпіона безпеки» або когось у команді розробників, хто виступає за покращення загальної ситуації та наполягає на цьому. поза безпеки та управління конфіденційними даними. Врахування безпеки як частини розробки допомагає всім командам долати перешкоди у сфері безпеки.

Погане управління сторонніми розробниками та відкритим кодом

Сторонні та з відкритим кодом. Код може відігравати важливу роль для більшості команд розробників, звільняючи багато ресурсів від необхідності створювати кожен аспект коду власними силами. Однак це не означає, що сторонній код та код з відкритим вихідним кодом не потребують підтримки. Весь цей зовнішній код поєднується з власним кодом, створюючи частину вашого ланцюжка постачання програмного забезпечення, яка є дуже вразливою до атак.

Прості способи управління програмним забезпеченням з відкритим кодом та сторонніми розробниками у вашому ланцюжку поставок включають: Встановлення політики щодо використання програмного забезпечення з відкритим вихідним кодом; Створення ради управління відкритим кодом; Створення взаємопов'язаних відносин з вашими постачальниками, щоб у разі виникнення проблем вони швидко реагували та вживали

необхідних заходів для їх усунення; Регулярно запускайте сканування за допомогою аналізу складу програмного забезпечення (SCA).

Інвентаризуйте свій SDLC, щоб зрозуміти, які конвеєри є найважливішими для бізнесу.

Скануйте свої конвеєри розробки на наявність SCA-сканувань.

Важливо зазначити, що ваш ланцюжок постачання програмного забезпечення – це не лише зовнішній код, який тут використовується. Ваш ланцюжок постачання програмного забезпечення також складається з інструментів розробника та конвеєрів у вашому SDLC, а також будь-якого додаткового коду, бібліотек та ресурсів, що використовуються під час розгортання вашого програмного забезпечення або інструменту, що передаються у ваше робоче середовище.

Невикористання стороннього коду на свою користь

Багато команд надають великого значення розробці внутрішніх рішень безпеки, але розробка власного коду та рішень має кілька недоліків. Через це іноді нове, неперевірене, незахищене внутрішнє рішення використовується *за звичкою*, замість того, щоб просто оцінити сторонні рішення, які вирішують проблему більш нестандартним та менш ресурсоемним способом порівняно з саморобним підходом.

Один гібридний підхід полягає в інвестуванні в low-code та no-code рішення для безпеки та автоматизації, щоб інтегрувати безпеку в гнучкі методи розробки. Такі інструменти допомагають усунути вузькі місця, пов'язані з обмеженнями потужностей команди розробників. Власники гнучких продуктів не завжди по-справжньому розуміють наслідки для безпеки своїх основних функцій, тому важко планувати заздалегідь під час розробки вимог. І не всі команди здатні формулювати вимоги, що стосуються проблем безпеки, не диктуючи потім занадто багато елементів рішення, що може призвести до значного розширення обсягу робіт під час спроби створення внутрішніх рішень.

Коротше кажучи, не бійтеся використовувати надійний та безпечний сторонній код і рішення на свою користь, оскільки ці рішення добре перевірені та значно скорочують час розгортання.

Нездатність визначити пріоритети служби безпеки

Підхід, що ставить безпеку на перше місце, може здаватися суперечливим темпам типової гнучкої розробки для багатьох гнучких команд. Тестування та процедури безпеки часто розглядаються як перешкоди та лежачі поліцейські на шляху до швидшої доставки готового продукту членами гнучкої команди, зосередженими на дотриманні останнього дедлайну спринту.

Один зі способів підвищити безпеку в гнучкій розробці – це спричинити культурні зміни, які зроблять безпечну розробку невід'ємним пріоритетом. Приділіть час переосмисленню процедур безпеки, щоб члени команди розуміли, чому певна практика безпеки є важливою. Інтегруйте команди безпеки та розробки, щоб безпека могла бути інтегрована на ранніх етапах процесу експертом у цій галузі. Обговоріть та встановіть розумну частоту та процедури тестування, щоб допомогти перейти до культури «гнучкої безпеки». Існує тісний зв'язок між додаванням занадто великої кількості необґрунтованих перевірок безпеки в процес та часом розробки, який витрачається на винахід способів обійти складні процеси. Наприклад, може бути безпечніше вимагати понад 2 рецензентів коду під час просування коду, але це створює більш ніж удвічі більше труднощів, ніж вимога лише одного рецензента коду. Відділи безпеки повинні враховувати вплив на досвід розробника під час запровадження політики, якої необхідно дотримуватися.

Вибір самостійної безпеки

Нерідко багато команд намагаються вирішувати всі свої потреби в безпеці самостійно. Існує поширена помилкова думка, що повністю внутрішня команда може заощадити вам час і гроші (особливо враховуючи те, що компанії відчайдушно потребують експертів з кібербезпеки.) Часто внутрішнім командам бракує всебічної експертизи, необхідної для забезпечення безпеки всього SDLC – саме тут і знадобляться експерти.

Зовнішня експертиза буває двох форм: Постачальники послуг кібербезпеки.

Постачальники продуктів кібербезпеки; Використання зовнішньої експертизи з безпеки для управління вашою безпекою дає деякі помітні переваги: Звільняє внутрішні ресурси, щоб зосередитися безпосередньо на завданнях, які можуть виконати тільки вони; Заповнює прогалини в спеціалізації, для забезпечення яких було б надто важко найняти внутрішній ресурс.

Тепер, коли розробка дедалі більше кодифікується, у індустрії програмного забезпечення спостерігається поява принципу «політика як код». SaaS-рішення, такі як Легітимна платформа безпеки. Зараз існують стандарти, які кодифікували сотні найкращих практик у вузькоспеціалізованих сферах безпеки, таких як безпека ланцюга постачання програмного забезпечення. Замість того, щоб вимагати внутрішнього експерта з предметної області, ви можете використовувати знання, кодифіковані в продукті. Крім того, SaaS краще підходить для контролю того, чи порушують команди розробників необхідні політики, порівняно з внутрішнім ресурсом безпеки. Зрештою, це допомагає досягти більшої безпеки-орієнтованої розробки.

Гнучка розробка допомагає компаніям-розробникам програмного забезпечення впроваджувати легкі, ітеративні цикли розробки. Методологія розробки робить акцент на невеликих, керованих командах з міжфункціональною співпрацею для частих оновлень та випусків.

Хоча Agile залежить від масштабних культурних змін у розробці та тестуванні коду, ця модель також вимагає нового підходу до впровадження безпеки в Agile.

У цьому розділі обговорюються відповідні ризики, що виникають внаслідок неправильного впровадження методів безпеки, а також заглиблюються в найкращі практики забезпечення циклу Agile-розробки.

Ризики неврахування безпеки у вашій гнучкій розробці

Гнучкі процеси зазвичай відкривають виробниче та розробницьке середовища для розподілених команд, що призводить до витoku важливої інформації через поступове збільшення кількості авторизацій. Хоча гнучкі методології розвивалися, щоб враховувати інновації та терміни виконання, безпека часто відходить на другий план, оскільки оцінки безпеки уповільнюють розробку.

Практики безпеки особливо складно впроваджувати однаково протягом усього життєвого циклу розробки програмного забезпечення. Цикл збірки є безперервним, і тести безпеки необхідно проводити поза робочим процесом розробки. Це створює різні ризики для безпеки організації, зокрема:

Недостатня політика, що регулює використання компонентів з відкритим кодом

Основний принцип Agile полягає в тому, щоб не винаходити велосипед. Крім того, командам рекомендується використовувати рішення з відкритим кодом та комерційні власні рішення для скорочення життєвого циклу розробки. Однак, хоча такі інтеграції з відкритим кодом пропонують різні переваги, вони також створюють значні ризики безпеки, які можуть вплинути на розробку.

Типовий сценарій – це коли розробники не знають про залежності модулів та кількість бібліотек коду, які вони імпортують. Як наслідок, відстеження змін у відкритому коді є складним завданням, що ускладнює забезпечення надійної та безпечної роботи програмного забезпечення.

Залежність від інтеграцій з відкритим кодом також ускладнює отримання інформації про конкретні вразливості та виправлення, виявлені спільнотою учасників. За відсутності чітко визначених політик, що регулюють інтеграції з відкритим кодом, вибір інструментів та управління технологічним стеком, виявляють проблеми для зменшення загроз.

Необмежений доступ до процесів розробки та репозиторіїв вихідного коду

Agile сприяє ефективній співпраці між міжфункціональними, розподіленими командами, які дотримуються ітеративного підходу до розробки. Щоб забезпечити роботу

команд з єдиним джерелом достовірної інформації, організації покладаються на публічні та приватні репозиторії вихідного коду для підтримки, обміну та версіонування коду.

Хоча репозиторії забезпечують безперебійний контроль версій, команди часто не можуть інтерпретувати версію вихідного коду, що використовується, що ускладнює виявлення конкретних вразливостей та застосування заходів щодо їх усунення.

Крім того, коли приватне створення коду потрапляє до репозиторіїв вихідного коду, він розкриває вразливі точки входу. Зловмисники націлюються на такі відкриті репозиторії, щоб виявити приховані функції, а потім поєднують їх з розвідувальними тактиками для організації атак.

Небезпечне управління конфіденційними даними

Сучасний процес гнучкої розробки інтегрує численні джерела для аналітики та операцій з даними в масштабах всієї організації. Складна інтеграція вимагає систематичної та точної класифікації даних для контролю рівня доступу до конфіденційних даних організації.

Крім того, фрагменти тестових даних, створені командою тестувальників, часто є значною часткою реальних даних. Хоча такі дані використовуються внутрішньо для цілей тестування, відсутність належної санітарної обробки даних сприяє зловживанню вразливостями з боку векторів атак.

Більшість Agile-організацій не мають політик захисту своїх даних від внутрішніх зловмисників. Через відсутність суворих політик класифікації даних, члени команди зазвичай не знають про комплексні вимоги безпеки, чутливість даних та свою відповідальність за їх захист. Рівень співпраці, необхідний для безперебійної роботи, також ускладнює для команди безпеки впровадження заходів безпеки.

Методології безпеки в Agile-розробці

Гнучка розробка програмного забезпечення запроваджує культурні зміни в масштабах усієї організації, зосереджуючись на модульних, більш керованих, міжфункціональних командах. Хоча ці зміни забезпечують дуже гнучку розробку, яка реагує на мінливі вимоги, організаціям потрібне впровадження спеціальних методів для захисту коду та середовищ розгортання.

Нижче наведено деякі з найкращих практик для захисту застосунків у гнучкому середовищі:

Захист гнучких конвеєрів доставки

Методологія Agile робить акцент на конвеєрах безперервної інтеграції (CI) та безперервної доставки (CD), щоб забезпечити швидше розгортання. Щоб мінімізувати ризики безпеки, команди Agile повинні розглянути інтеграцію автоматизованих механізмів тестування на кожному етапі SDLC. Крім того, всі коміти, зроблені командою розробників, повинні проходити через експертів з безпеки, щоб гарантувати безпеку розробленого застосунку.

Окрім ручних перевірок коду, також повинні бути статичні аналізатори коду, інтегровані з конвеєром неперервної інтеграції (CI), та автоматизовані модульні тести для запуску запланованих перевірок. Також рекомендується проводити активні аудити безпеки та автоматичні перевірки безпеки під час процесу CI/CD, щоб допомогти виявити вразливості безпеки, перш ніж код перейде у продакшн.

Вартість виявлення вразливості безпеки на ранній стадії значно менша порівняно з пошуком її у виробництві, що може призвести до серйозних наслідків, включаючи крадіжку конфіденційних даних, неякісну продуктивність програм та втрату репутації.

Забезпечити безперервну участь усієї організації

Порівняно з традиційними практиками, Agile-процес представляє собою зсув у практиках розробки, який повинен супроводжуватися змінами в організаційній культурі в бік практик безпеки. Рекомендується, щоб фахівці з безпеки співпрацювали з розробниками для формування затвердженого керівництва щодо стандартів кодування, шаблонів проектування та рішень щодо проектування.

Організаціям також слід проводити ретельне моделювання загроз, одночасно розробляючи безперервне навчання з безпеки, яке зосереджується на зміні поведінки, а не лише на обізнаності. Фахівці з безпеки також повинні документувати критерії безпечної розробки на спільних платформах, щоб інші організації могли посилатися на них у своїх процесах.

Фірми також можуть впроваджувати гнучкі методи безпеки, впроваджуючи політики безпеки в нещодавно розроблені мікросервіси, додатки, інтеграції та API.

Впроваджуйте пасивні огляди

Методологія гнучкої розробки характеризується коротшими ітераціями, швидкими збірками та частими випусками нових функцій. Тому необхідно переглянути всі зміни в додатку, які потребують ітерацій, та як вони впливають на безпеку системи, перш ніж їх впроваджувати.

Пасивний огляд коду допомагає фахівцям з контролю якості розуміти додатки, не скануючи кожен рядок вихідного коду. Натомість, фахівці з контролю якості можуть переглядати код, а системи огляду коду відстежують їхні переміщення в кодовій базі та пропонують своєчасну, відповідну додаткову інформацію для вихідного коду. Деякі інструменти безпеки пасивного огляду також генерують схеми моделей, які візуалізують логіку, реалізовану кодом, спрощуючи усунення несправностей.

Забезпечення проактивного контролю для команд Agile-розробників

Організація повинна підтримувати розробників у впровадженні заходів контролю, що сприяють безпечній практиці розробки коду. OWASP перераховує різні методи безпеки, які забезпечують побудову всіх рівнів програми, з акцентом на безпеці. Деякі з цих методів включають:

Визначення вимог безпеки – Гнучкі методи повинні бути побудовані на галузевих стандартах, минулих вразливостях та чинному законодавстві, щоб гарантувати, що продукт відповідає всім властивостям безпеки.

Використання бібліотек та фреймворків безпеки – ці бібліотеки та фреймворки мають вбудовані заходи безпеки для захисту коду від недоліків проектування та реалізації, які призводять до недоліків безпеки.

Безпека сховищ даних – команди повинні забезпечити безпеку як NoSQL, так і реляційних баз даних за допомогою безпечних запитів, автентифікації, налаштування та зв'язку.

Кодування та екранування даних – Кодування та екранування даних використовуються для запобігання вразливостям, пов'язаним з ін'єкціями. Ескейпінг передбачає використання спеціальних символів, щоб уникнути неправильної інтерпретації рядків, тоді як кодування стосується перетворення символів на однакові значення з різними форматами, що робить їх недоступними для зловмисних інтерпретаторів.

Інші проактивні засоби контролю для комплексної Agile-безпеки включають перевірку вхідних даних, керування ідентифікацією та доступом (IAM), обробку помилок та винятків, а також ведення журналу та моніторингу безпеки.

Хоча Agile та традиційна методи безпеки спираються на впровадження подібних політик безпеки, реалізація функцій безпеки значно відрізняється. У Agile-методах швидкі цикли випуску передбачають часті тести безпеки, що означає, що детальний аналіз коду може зрештою уповільнити розробку та реалізацію.

Щоб вирішити цю проблему, індикатори ризиків безпеки слід встановити відповідно до швидкості виконання, що дозволить Agile-командам проводити перевірки безпеки, одночасно справляючись з частими змінами. Agile-практики безпеки також слід класифікувати на ті, що виконуються на початку розробки, та ті, що впроваджуються під час кожного спринту, залежно від того, чи потрібно їх виконувати одноразово чи постійно.

Найпоширенішою помилкою Agile-команд, які намагаються захистити конфіденційну інформацію, є неправильна класифікація даних. Більшість команд не вказують дані, які

потребують спеціального захисту, що ускладнює впровадження ефективної політики класифікації даних.

Крім того, команди розробників програмного забезпечення не можуть оптимально шифрувати конфіденційні дані під час передачі або зберігання, що робить їх легкодоступними для зловмисників. Ще один момент для занепокоєння виникає, коли команди неправильно використовують платформи хмарного зберігання даних, зберігаючи облікові дані та дані конфігурації без правильного тлумачення політик безпеки постачальника. Це ускладнює впровадження комплексної стратегії з точки зору безпеки.

Розроблене програмне забезпечення дозволяє забезпечити захист переданої по мережі інформації, строго взаємну автентифікацію користувачів і серверів, гнучке розмежування доступу. Для реалізації цих функцій у системі використовуються SSL/TLS протоколи й X.509 цифрові сертифікати, тобто універсальні, що стали стандартом де-факто, механізми, підтримувані практично всіма розповсюдженими Веб-агентами.

За допомогою розробленого програмного забезпечення легко забезпечуються вимоги по інформаційній безпеці, запропоновані різними Інтернет додатками, такими як:

- сервера платіжних систем;
- інтернет-магазини;
- багатопрофільні корпоративні Веб-сервера, що містять інформацію з різним рівнем конфіденційності;
- B2B системи;
- системи захищеного документообігу;
- системи обміну електронною поштою;
- й багато які інші.

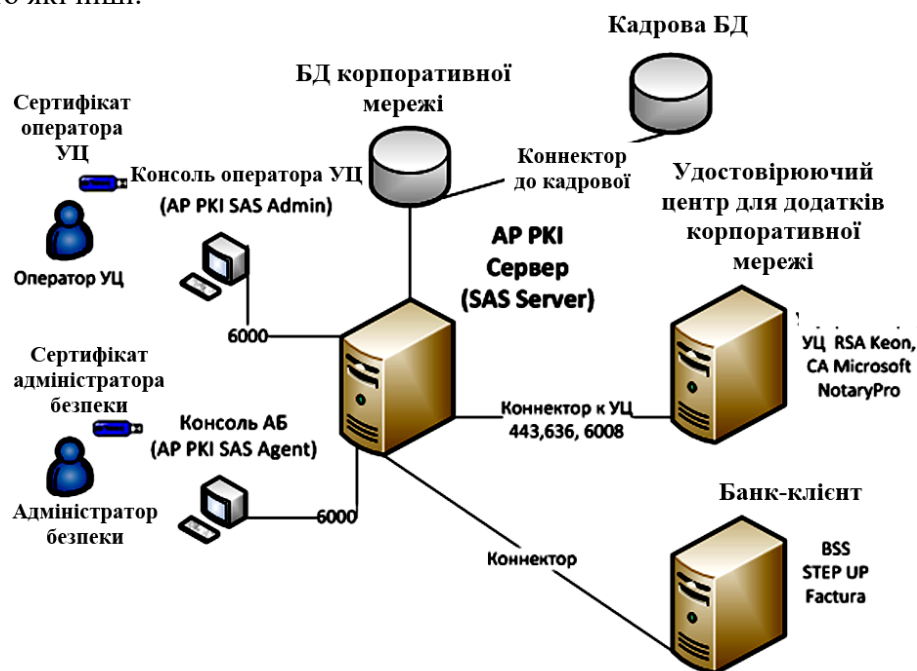


Рисунок 1 – Структурна схема системи

На рисунку 1 представлена структурна схема розробленої системи. Для поняття роботи системи введені наступні позначення:

- ЕЦП – електронний цифровий підпис;
- УЦ – удостоверяющий центр.
- ЦС – цифровий сертифікат;
- PKI – інфраструктура відкритих ключів;
- DVCS – Data Validation and Certification Server Protocols – протокол підтвердження даних та сертифікації серверу;

- OSCP – Online Certificate Status Protocol – онлайн протокол статусу сертифікату;
- TSP – Time-Stamp Protocol – протокол часових міток;
- TLS – криптографічний протокол, що забезпечує захищену передачу даних між вузлами в мережі Інтернет;
- RFC – документ, у якому описується той або інший стандарт.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів захисту корпоративних додатків, які розробляються за допомогою методології Agile. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем захисту корпоративних додатків, які розробляються за допомогою методології Agile.
- Досліджена система захисту корпоративних додатків, які розробляються за допомогою методології Agile.
- На основі отриманих результатів досліджень створена програмна реалізація системи захисту корпоративних додатків, які розробляються за допомогою методології Agile. Розроблені алгоритми дозволяють успішно вирішувати завдання захисту корпоративних додатків, які розробляються за допомогою методології 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. 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. – 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., Neskordieva A., Neskordieva 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 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.
 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.

УДК 004

Є.Завірюха, магістр гр. КІ-24М,

Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ ПРОГРАМНО-АПАРАТНОГО КОМПЛЕКСУ МОНІТОРИНГУ ЖИТТЄВИХ ПОКАЗНИКІВ ПАЦІЄНТІВ ІЗ ПЕРЕДАЧЕЮ ДАНИХ НА РОБОЧЕ МІСЦЕ ЛІКАРЯ

У статті розроблено програмне забезпечення, яке призначено для програмно-апаратного комплексу моніторингу життєвих показників пацієнтів із передачею даних на робоче місце лікаря. Метою розробки є дослідження та реалізація програмно-апаратного комплексу моніторингу життєвих показників пацієнтів із передачею даних на робоче місце лікаря. Об'єктом дослідження є процес моніторингу життєвих показників пацієнтів із передачею даних на робоче місце лікаря. Предметом дослідження є методи моніторингу життєвих показників пацієнтів із передачею даних на робоче місце лікаря. Методи дослідження базуються на методах теорії обробки інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – реалізація програмно-апаратного комплексу моніторингу життєвих показників пацієнтів із передачею даних на робоче місце лікаря. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

програмно-апаратний комплекс, моніторинг життєвих показників пацієнтів

Постановка проблеми. У роботі запропоновано метод організації структурної схеми апаратно-програмного медичного комплексу, в якому основна увага була приділена: методу побудови архітектури біомедичної системи для реєстрації та обробки фізіологічних сигналів, що підвищує функціональність комплексу та його технологічність; математичній моделі розподілу та фізичного представлення даних для вирішення задачі ідентифікації паралельних процесів; методика забезпечує функції реєстрації, зберігання, обробки, аналізу ряду фізіологічних сигналів: пульсу, температури тіла, електрокардіограм; високій надійності та стійкості до перешкод; розробці оригінального схемотехнічного рішення з метою зменшення обсягу телеметричних даних та великого обсягу переданої інформації, а також збільшення швидкості бездротової передачі даних. Моніторинг життєво важливих показників за допомогою апаратно-програмного медичного комплексу покращує якість життя пацієнта під час обстеження та дозволяє кількісно оцінити реакцію серцево-судинної системи пацієнта на стрес-тести, встановити ефективність режиму стимуляції та терапії у пацієнтів з імплантованими кардіостимуляторами та багатьма іншими патологіями.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні дослідження та реалізація програмно-апаратного комплексу моніторингу життєвих показників пацієнтів із передачею даних на робоче місце лікаря.

Мета й завдання дослідження. Метою роботи є дослідження та реалізація програмно-апаратного комплексу моніторингу життєвих показників пацієнтів із передачею даних на робоче місце лікаря.

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

- Огляд існуючих систем моніторингу життєвих показників пацієнтів із передачею даних на робоче місце лікаря.

- Дослідження програмно-апаратного комплексу моніторингу життєвих показників пацієнтів із передачею даних на робоче місце лікаря.

- Реалізація програмно-апаратного комплексу моніторингу життєвих показників пацієнтів із передачею даних на робоче місце лікаря.

Об'єктом дослідження є процес моніторингу життєвих показників пацієнтів із передачею даних на робоче місце лікаря.

Предметом дослідження є методи моніторингу життєвих показників пацієнтів із передачею даних на робоче місце лікаря.

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

Виклад основного матеріалу. У сучасному середовищі охорони здоров'я потреба в надійному, масштабованому та доступному моніторингу пацієнтів ще ніколи не була такою великою. Урбанізація, зростання тягаря хронічних захворювань, нестача лікарів та застаріла інфраструктура – все це разом створює значний тиск на лікарні в регіонах по всьому світу, особливо в країнах із середнім рівнем доходу.

Однак, за допомогою правильних інструментів системи охорони здоров'я можуть подолати традиційні бар'єри моніторингу та покращити як безпеку пацієнтів, так і ефективність роботи клініцистів, одночасно підтримуючи довгострокову стійкість. Одним із критично важливих інструментів для подолання цих бар'єрів є платформа моніторингу пацієнтів: гнучке рішення для всієї лікарні, розроблене для масштабування, адаптації та роботи в реальних умовах, де складність, терміновість та обсяг є щоденними реальностями.

Хоча лікарні із середнім рівнем доходу поділяють багато потреб більш усталених лікарень, таких як зростання рівня хронічних захворювань, включаючи серцеві захворювання, діабет та ожиріння, ці проблеми є поєднаними з іншими, такими як:

- існуючі інфекційні захворювання: це включає спалахи нових, повторно з'являючихся та ендемічних патогенів.

- обмеженість ресурсів: застаріла інфраструктура, ненадійне електропостачання та обмежений доступ до сучасного обладнання – це проблеми, з якими стикаються багато систем охорони здоров'я.

- нестача персоналу: поширеними є ротація персоналу, недостатня кваліфікація клініцистів та вигорання.

- фрагментована технологія: різні постачальники та несумісні системи порушують безперервність медичного обслуговування.

- прогалини в нормативному регулюванні: непослідовні стандарти медичного обслуговування дозволяють неякісному обладнанню потрапляти на ринок, що додає ризиків для лікарняних процесів та знижує рівень медичного обслуговування.

Через ці потреби керівникам охорони здоров'я необхідно враховувати кілька дуже важливих питань, розглядаючи будь-яку платформу моніторингу: Чи зменшить ця система навантаження на персонал, чи збільшить його? Чи може це працювати в різних сферах догляду з мінімальним навчанням? чи може це допомогти спростити роботу та покращити процес прийняття рішень? Чи будуть сигнали тривоги точними, чи вони відволікатимуть увагу?

Не кожен монітор життєво важливих показників зроблений однаково. На ринку доступні численні монітори життєво важливих показників з безліччю функцій та можливостей. Моніторинг пацієнта передбачає безперервне або періодичне спостереження та вимірювання фізіологічних функцій та життєво важливих показників пацієнта. Це включає відстеження частоти серцевих скорочень, артеріального тиску, частоти дихання, температури та рівня насичення крові киснем.

Мета полягає в тому, щоб швидко виявити будь-які відхилення від нормальних значень, які можуть свідчити про погіршення стану пацієнта, щоб мати змогу вжити відповідних заходів.

Якщо основи технології моніторингу пацієнтів є надійними, вихідний сигнал моніторингу буде точним та надійним для процесу прийняття клінічних рішень. Як наслідок, робота медичних працівників буде покращена та спрощена, наприклад, зі значно меншою кількістю хибних тривог або переміщення датчиків.

Які ключові основи лежать в основі надійного рішення для моніторингу?

Отримання сигналу: стосується процесу захоплення та перетворення життєво важливих сигналів пацієнта у формат, який можна обробляти та аналізувати за допомогою алгоритмів. На отримання сигналу впливають не лише якість та конструкція датчиків, прикріплених до пацієнта (чи датчик занадто вільно прилягає? чи не впливає на нього артефакт руху?), але й фільтри шумоподавлення, підсилення сигналу, кількість вхідних каналів, швидкість дискретизації тощо.

Монітори повинні працювати з перевіреними датчиками, адаптованими до вимог застосування, забезпечуючи точні показники та задовольняючи очікування щодо продуктивності.

Обробка сигналів: зосереджена на аналізі, модифікації та синтезі отриманих сигналів для оптимізації передачі, корекції спотворених сигналів, що забезпечує точну клінічну інтерпретацію. В основі цього лежать точні алгоритми.

Наскільки досконалі алгоритми, визначають загальну якість інформації, що відображається на моніторі. Зокрема, чутливість та специфічність відіграють ключову роль відповідно для виявлення якомога більшої кількості справжніх подій та відкидання хибних.

Точні алгоритми можуть виконувати: покращити здатність розрізняти артефакти від справжніх життєво важливих показників; дозволяють безперервний моніторинг навіть за наявності артефакту, тим самим зменшуючи переривання догляду; мають високу чутливість, особливо на порогових значеннях для діагностики гіпотензії та гіпертензії; мають високу точність вимірювання за низьких та дуже низьких порогів перфузії; зменшити затримку між отриманням сигналу та відображенням інформації на моніторі. Навіть затримка в кілька секунд між діями хірурга та візуальним зворотним зв'язком на моніторі може поставити під загрозу результат лікування пацієнта.

Монітори та алгоритми також повинні бути ретельно протестовані компанією та сертифіковані незалежною лабораторією.

Конфігурованість: коли монітор пацієнта є гнучким з точки зору налаштування апаратного та програмного забезпечення (тобто додавання нових параметрів «на місці», можливості налаштування трендів та відображення, розширене керування тривогами та інструменти візуальної підтримки), тоді посилюються ефективніші протоколи та генеруються дієві клінічні сповіщення.

Основні можливості платформи моніторингу, готової до майбутнього

Для оцінки платформи моніторингу з точки зору безпеки пацієнтів, ефективності клініцистів та довгострокової стійкості, слід враховувати такі області:

1. Простота використання: розроблено для швидкого навчання та гнучкості.

У завантажених та складних клінічних умовах рішення, яке бере на себе частину навантаження, спростить життя. Наприклад, рішення для моніторингу, яке включає: великі, читабельні дисплеї з висококонтрастним зображенням; зрозумілий інтерфейс користувача, що зменшує потребу у офіційному навчанні; стандартизовані робочі процеси для госпіталізації, виписки та ескалації пацієнтів; налаштування за зоною догляду (відділення інтенсивної терапії, відділення невідкладної допомоги, операційна, відділення пониженої терапії); інструменти візуалізації, які збирають та поєднують клінічні дані з різних джерел (за різними параметрами) та спрощують обробку складної інформації для ефективного процесу прийняття рішень.

Про що мені потрібно обов'язково подумати? Чи може персонал з обмеженою підготовкою працювати з монітором пацієнта під тиском або під час кризи? Скільки кліків потрібно для виконання функції? Чи адаптується інтерфейс користувача до різних клінічних середовищ і дозволяє операторам інтуїтивно знаходити необхідну інформацію або налаштування? Чи може надмірність у інтерфейсі користувача допомогти доглядачам знаходити інформацію, що надходить з різних точок навігації?

2. Клінічна досконалість: надійна, перевірена, розумна.

Рішення для моніторингу пацієнтів повинні надавати медичним працівникам точні дані, необхідні для прогнозування, виявлення та лікування гостроти захворювання пацієнтів протягом усього періоду догляду. Від шкіри до екрана: датчики, розроблені для зменшення кількості хибних тривог та забезпечення цілісності сигналу, завдяки чому дані, що зчитуються на екрані, відображають те, що відбувається в організмі. Перевірені та ретельно протестовані алгоритми, що обробляють дані життєво важливих показників для отримання клінічно корисних результатів (наприклад, інтелектуальне керування сигналізацією, виявлення аритмії, точність артеріального тиску).

Доступ до даних пацієнтів у режимі реального часу в усіх зонах догляду. Оптимізація сигналізації, що підтримує «тихе» середовище. Розширені інструменти візуалізації, що підтримують швидке та ефективне прийняття клінічних рішень. Про що мені потрібно обов'язково подумати? Чи клінічно перевірені та доведена їхня ефективність в умовах високого тиску алгоритми та датчики? Як система запобігає втомі від тривоги та підтримує швидке прийняття рішень?

3. Масштабованість: одна платформа, багато зон догляду.

Клінічні робочі процеси відрізняються в різних сферах медичного обслуговування. Відповідно, рішення має бути адаптоване до конкретної галузі медичного обслуговування, в якій ми працюємо, а також має забезпечувати гнучкість використання певних параметрів за потреби. Модульна конструкція з повноцінними компонентами plug-and-play, що розширюються на льоту (не обмежується конфігурацією моніторингу, обраною під час покупки). Можливість масштабування від базових життєво важливих показників до більш спеціалізованих параметрів. Транспортні монітори, що стикаються та безперешкодно інтегруються з центральними системами (наприклад, електронним медичним звітом, якщо він доступний).

Однаковий користувацький досвід у всіх відділеннях, по всій лікарні – скорочення часу на навчання. Про що мені потрібно обов'язково подумати? Чи можу я розгорнути таку саму систему по всій лікарні? Чи буде він зростати разом із клінічними потребами моєї лікарні протягом наступних десятиліть?

4. Мобільність та внутрішньолікарняне транспортування: безперервність без компромісів. Під час переміщення пацієнта між зонами догляду спостереження та втручання повинні бути такими ж, як і в початковій установі, щоб підтримувати винятковий рівень безпеки пацієнтів: Транспортні монітори з тривалим часом роботи від батареї та міцним корпусом; Безперебійна передача даних пацієнтів з однієї області до іншої; Живлення від батареї для середовищ з коливаннями напруги живлення;

Про що мені потрібно обов'язково подумати? Чи втрачає монітор дані під час транспортування пацієнта? Чи витримує пристрій удари під час транспортування, падіння та електричну нестабільність? Чи дозволяє монітор вимірювати всі критичні параметри для рівня гостроти стану пацієнта (інтубовані пацієнти, пацієнти з нестабільною гемодинамікою)?

5. Доступність: розроблено для довгострокової цінності.

Як рішення для моніторингу широкого спектру закупівель може відповідати довгостроковим цілям фінансової стабільності лікарні? Слід враховувати багато аспектів, а не лише одноразове придбання. Нещодавно придбане рішення для моніторингу повинно мати: Варіант початкового рівня з можливістю оновлення в майбутньому; Сумісність з усіма підприємствами, що зменшує потребу в установці кількох систем; Цифровий робочий

процес, який зменшує використання паперу та рівень помилок; Обмежене поточне технічне обслуговування та низькі витрати на навчання.

Про що мені потрібно обов'язково подумати? Чи можемо ми оновити встановлений парк обладнання, чи нам потрібно замінити все рішення? Яка загальна вартість володіння протягом 5–7 років, включаючи навчання, обслуговування та витратні матеріали?

6. Надійність, якій ви можете довіряти. Опора на компетенцію партнера, його великий досвід у моніторингу охорони здоров'я та відданість спільним цілям є основою для довгострокової співпраці: Підтверджений досвід роботи як у передових, так і в загальних медичних закладах; Сильна присутність для післяпродажної підтримки, а також для безперервності обслуговування; Спадщина клінічних інновацій у моніторингу пацієнтів; Відсутність прихованих витрат на обслуговування та довгострокова доступність запчастин.

Про що мені потрібно обов'язково подумати? Чи має цей постачальник досвід довгострокових партнерських відносин на ринках, подібних до мого? Чи визнано цього постачальника інноваційною та клінічно бездоганною компанією? Чи буде цей партнер продовжуватися протягом усього терміну служби моєї платформи моніторингу?

Більшість закладів охорони здоров'я у світі не лише обмежені в ресурсах, вони мають потенціал перетворитися на центр, багатий на інновації. Лікарні, які роблять мудрий вибір сьогодні, можуть забезпечити собі позиції для майбутнього зростання, розумніших робочих процесів та кращих результатів лікування пацієнтів завтра. Правильна платформа моніторингу не лише вимірює життєво важливі показники – вона захищає пацієнтів, полегшує навантаження на клініцистів та забезпечує майбутні інвестиції в лікарні.

Короткий огляд: на що звернути увагу при виборі рішення для моніторингу:

- Простота використання: мінімальне навчання, інтуїтивно зрозумілі операції, стандартизовані робочі процеси.
- Клінічна точність: перевірені алгоритми, якість сигналу, інтелектуальні тривоги.
- Масштабованість: модульна конструкція, підтримка кількох гострот, додаткові параметри.
- Готовність до транспортування: міцні, з живленням від батареї, безперешкодна передача.
- Доступність: низька загальна вартість володіння, платформа з можливістю оновлення, зменшені витрати на обслуговування.
- Надійний партнер з глобальним досвідом, регіональна підтримка.
- Системи моніторингу пацієнтів використовуються в низці застосувань.
- З інноваціями в бездротовому, портативному та дистанційному моніторингу пацієнтів, різноманітність та тип застосування зростають.

У стінах лікарень та клінік – історичного центру інновацій у сфері моніторингу пацієнтів – системи моніторингу пацієнтів мають вирішальне значення для будь-якої хірургічної операції.

Під час операції хірург(и) повинен(и) мати постійний доступ до життєво важливих показників пацієнта, щоб зменшити ризик виникнення негативних наслідків.

В операційній зазвичай є термометр для відстеження температури пацієнта, пульсоксиметр для вимірювання рівня кисню, капнограф для контролю рівня CO₂ та сфігмоманометр для вимірювання артеріального тиску.

Після операції багато з цих самих пристроїв моніторингу використовуються лікарями, медсестрами та іншими медичними працівниками, щоб забезпечити безперебійне післяопераційне відновлення.

Окрім клінічних умов, системи дистанційного моніторингу пацієнтів використовуються в різних сферах застосування, таких як догляд за діабетиками.

Прилади для моніторингу рівня глюкози використовуються пацієнтами з діабетом поза лікарнею вже багато років, дозволяючи як пацієнту, так і його лікарю запобігати небезпечним подіям для здоров'я.

Хоча цей розділ містить лише кілька прикладів застосувань, де системи моніторингу пацієнтів допомагають медичним працівникам та пацієнтам покращувати результати, одне має бути зрозумілим: інновації на ринку моніторингу пацієнтів продовжуватимуть стимулювати зростання нових застосувань.

Які компоненти системи моніторингу пацієнтів?

Кожна система моніторингу пацієнта унікальна – ЕКГ не складається з тих самих компонентів, що й глюкометр.

Немає жодного нормативного акту, який би стверджував, що кожна система моніторингу пацієнтів повинна мати певну кількість друкованих плат, датчиків, провідників тощо.

З огляду на це, ми групуємо компоненти системи моніторингу пацієнта на три загальні категорії: пристрій моніторингу пацієнта, капітальне обладнання та програмне забезпечення.

Пристрій моніторингу пацієнта

Хоча термін «пристрій моніторингу пацієнта» зазвичай використовується для позначення всієї системи моніторингу пацієнта, у цій публікації блогу ми використовуватимемо його для опису частини системи моніторингу пацієнта, яка контактує з пацієнтом або вводиться в нього.

Загалом, пристрій моніторингу пацієнта зазвичай містить датчик для збору важливої інформації про пацієнта (наприклад, частоти серцевих скорочень) та рішення для з'єднання (наприклад, друковані плати, роз'єми, проводку тощо), яке може передавати інформацію до основного обладнання.

Використовуючи пульсоксиметр як приклад, деталь, яка кріпиться до вашого пальця та вимірює ваш пульс, а також передає його на основне обладнання, є прикладом компонента пристрою для моніторингу пацієнта.

Капітальне обладнання

Дані, зібрані пристроєм моніторингу пацієнта, марні, якщо до них немає доступу.

Це робить капітальне обладнання важливим компонентом системи моніторингу пацієнтів.

Оскільки пристрій моніторингу пацієнта сам збирає життєво важливі дані про пацієнта, ці дані потім надсилаються (іноді бездротовим способом) на основне обладнання, де вони обробляються, зберігаються та відображаються.

Більшість основного обладнання, що використовується для моніторингу пацієнтів, використовують складну систему взаємоз'єднань, що складається з роз'ємів, друкованих плат та джгутів проводів, а також певний тип екрана/монітора, на якому дані передаються у зручному для використання форматі.

Деякі види основного обладнання для моніторингу пацієнтів містять комп'ютер із процесором та жорстким диском.

По суті, капітальне обладнання є центральною точкою, де дані з пристрою моніторингу обробляються, зберігаються та виводяться у вигляді корисної інформації.

Екран комп'ютера, на якому відображається зубець Р ЕКГ пацієнта, є прикладом капітального обладнання, що використовується в системі моніторингу пацієнта.

Програмне забезпечення

Після того, як дані пацієнта передаються з пристрою на основне обладнання, їх необхідно обробити.

Хоча апаратне забезпечення, яке збирає дані, є важливим, програмне забезпечення, яке робить ці дані корисними, часто ігнорується в обговореннях щодо інновацій у моніторингу пацієнтів.

Зрештою, програмне забезпечення відповідає за перетворення одиниць і нулів у формат, який медичні працівники можуть насправді зрозуміти.

Драйвери, програми та програми, які обробляють, зберігають та візуально перетворюють дані, є невід'ємними частинами будь-якої системи моніторингу пацієнтів –

збій або затримка в програмному забезпеченні системи моніторингу пацієнтів може призвести до плутанини та небезпеки для пацієнта.

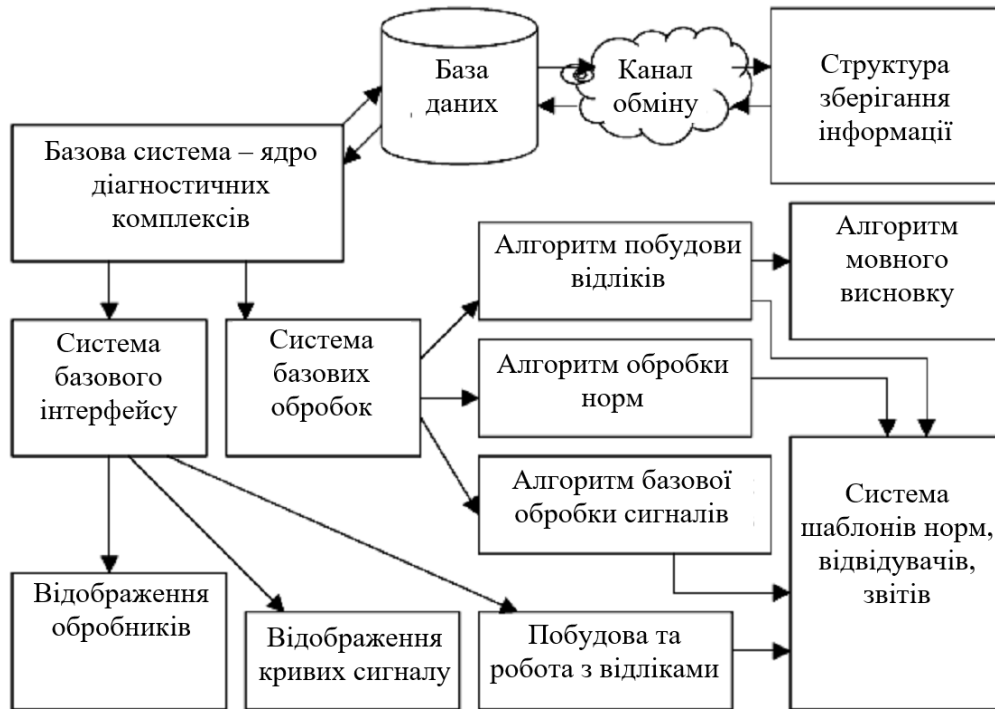


Рисунок 1 – Структурна схема системи

Завдання розробки пристроїв та обладнання для моніторингу пацієнтів

Як видно з наведеної вище інформації, системи моніторингу пацієнтів справді знаходяться на перетині інформаційних технологій та біомедичних наук.

Розробка пристроїв та обладнання для моніторингу пацієнтів вимагає глибоких знань технології датчиків, систем взаємоз'єднань, проектування пристроїв, розробки програмного забезпечення тощо.

Чи зберуть ваші датчики необхідну інформацію?

Чи може ваше рішення для взаємоз'єднання збирати та передавати дані з необхідною вам швидкістю?

Чи ваше програмне забезпечення точно перетворює ці дані на корисну інформацію?

Це лише деякі з багатьох точок потенційної несправності, які ви повинні враховувати під час розробки концепції вашого пристрою.

Інновації на ринку моніторингу пацієнтів продовжують покращувати результати лікування пацієнтів у всьому світі.

Розуміння загальних компонентів, що складають систему моніторингу пацієнтів, може допомогти вам краще підійти до процесу розробки з цілісної точки зору.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів моніторингу життєвих показників пацієнтів із передачею даних на робоче місце лікаря. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем моніторингу життєвих показників пацієнтів із передачею даних на робоче місце лікаря.

- Досліджена система моніторингу життєвих показників пацієнтів із передачею даних на робоче місце лікаря.

- На основі отриманих результатів досліджень створена реалізація програмно-апаратного комплексу моніторингу життєвих показників пацієнтів із передачею даних на робоче місце лікаря. Розроблені алгоритми дозволяють успішно вирішувати завдання моніторингу життєвих показників пацієнтів із передачею даних на робоче місце лікаря. 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.

УДК 004

М.Іванченко, магістр гр. КІ-24М,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ МЕРЕЖЕВОГО КОРПОРАТИВНОГО ЦЕНТРУ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ (SOC)

У статті розроблено програмне забезпечення, яке призначено для системи мережевого корпоративного центру управління інформаційною безпекою (SOC). Метою розробки є дослідження та принципи побудови системи мережевого корпоративного центру управління інформаційною безпекою (SOC). Об'єктом дослідження є процес мережевого корпоративного центру управління інформаційною безпекою (SOC). Предметом дослідження є методи мережевого корпоративного центру управління інформаційною безпекою (SOC). Методи дослідження базуються на методах захисту інформації у мережі, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи мережевого корпоративного центру управління інформаційною безпекою (SOC). В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

центр управління інформаційною безпекою (SOC)

Постановка проблеми. Центр операцій безпеки (SOC) – це централізований підрозділ, який займається питаннями безпеки на організаційному та технічному рівні. SOC оснащений командою аналітиків та інженерів з безпеки, а також сучасними технологіями виявлення та запобігання для моніторингу, аналізу та реагування на інциденти кібербезпеки.

Головною метою SOC є виявлення, оцінка, пом'якшення та звітування про кіберзагрози, забезпечення запобігання або раннього виявлення потенційних порушень безпеки та своєчасного реагування на них. Це включає постійний спостереження за ІТ-інфраструктурою організації, включаючи її мережі, пристрої, програми та дані, для захисту від загроз безпеці, починаючи від атак шкідливого програмного забезпечення до складного кібершпиунства.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи мережевого корпоративного центру управління інформаційною безпекою (soc).

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи мережевого корпоративного центру управління інформаційною безпекою (SOC).

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань: Огляд існуючих систем мережевого корпоративного центру управління інформаційною безпекою (SOC).; Дослідження системи мережевого корпоративного центру управління інформаційною безпекою (SOC).; Програмна реалізація системи мережевого корпоративного центру управління інформаційною безпекою (SOC).

Об'єктом дослідження є процес мережевого корпоративного центру управління інформаційною безпекою (SOC).

Предметом дослідження є методи мережевого корпоративного центру управління інформаційною безпекою (SOC).

Методи дослідження базуються на методах захисту інформації у мережі, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Центр операцій безпеки (SOC) – це команда експертів з інформаційної безпеки, які відповідають за моніторинг, виявлення, аналіз, запобігання та реагування на інциденти безпеки. Керований Центр операцій безпеки зазвичай надає консультації, розробку послуг та підтримку організаціям, яким потрібна зовнішня експертиза для захисту від загроз безпеці.

Окрім реагування на вторгнення, SOC також моніторить мережі на предмет незвичайної активності, такої як моделі трафіку, поведінка користувачів або зміни в обмеженнях доступу. Якщо щось здається підозрілим, SOC досліджує це, переглядаючи журнали та файли конфігурації на комп'ютерах і серверах, щоб з'ясувати, що сталося.

Центр кібербезпеки (SOC) можна розглядати як центральну нервову систему мережі, оскільки цей відділ відповідає за постійний моніторинг систем та проведення аналізу для виявлення та запобігання інцидентам кібербезпеки. Мета полягає в тому, щоб діяти до того, як станеться інцидент, але при цьому слід бути готовим до відновлення після інциденту, що складається з нової загрози.

SOC повинна швидко виявляти проблеми та встановлювати їхню серйозність, а також пропонувати рішення для запобігання атакам та припинення будь-яких поточних загроз.

Як працює Центр операцій безпеки

Центр безпеки (SOC) надає критично важливу інформацію про безпеку, щоб команди могли швидко реагувати на кіберінциденти. SOC збирають, співвідносять та аналізують дані з усіх різних комп'ютерів та мереж в організації. Це включає моніторинг у режимі реального часу, виявлення та реагування на оцінку вразливостей, виявлення вторгнень, аналіз та запобігання шкідливому програмному забезпеченню, мережеву криміналістику, а також технічне обслуговування та усунення несправностей.

Центри безпеки (SOC) найчастіше керуються спеціалізованим членом команди безпеки, який працює цілодобово, щоб контролювати активність у кількох системах та сегментах мережі. Член SOC розробляє звіти, використовуючи інформацію, отриману з журналів, для відстеження атак. Інформація, надана SOC, може бути використана для визначення пріоритетів реагування, визначення найбільш критичних вразливостей у середовищі та швидкої оцінки загального стану безпеки.

SOC має доступ до всіх різних компонентів безпеки в мережі, включаючи брандмауери, системи виявлення вторгнень (IDS), брандмауери додатків, балансувальники навантаження та веб-проксі. Член SOC може об'єднати ці різноманітні фрагменти інформації в одну цілісну картину того, що відбувається в середовищі. Крім того, член SOC може використовувати цю інформацію для швидкої оцінки всіх аспектів середовища, включаючи аномалії в трафіку та даних, нові оцінки вразливостей, незвичайну поведінку відомих інструментів та скриптів шкідливого програмного забезпечення, незвичайну активність веб-додатків, результати тестування на проникнення та інші події.

SOC не замінюють традиційні команди безпеки; радше вони забезпечують їм критичний рівень для покриття прогалин, які команди безпеки не можуть безпосередньо усунути.

Чому SOC такий важливий для бізнесу

Безпека – це дуже важливо. Якщо ви не захищаєтеся від зловмисників, ваша компанія може зазнати масової втрати даних або іншої конфіденційної інформації. І саме тому Центри операцій безпеки такі важливі – вони допомагають великим компаніям контролювати свою безпеку та захищатися від хакерів цілодобово, щодня.

Раніше компанії просто мали когось за столом, хто стежив за будь-якими потенційними загрозами. Але цього вже недостатньо. Зі зростанням компаній, а їхні процеси (і навіть їхні власні системи безпеки) ускладнювалися, вони виявили, що відстеження всього може бути мамонтовим завданням.

Атаки методом грубої сили на корпоративні мережі стають дедалі поширенішими. Вони можуть коштувати чимало грошей, і коли зловмисник намагається зламати захист однієї корпоративної мережі, стає зрозуміло, що витратити гроші на найм людей по суті

марно, коли справа доходить до визначення реального рівня загрози. Потрібен високотехнологічний моніторинг самих систем безпеки. Те, що починалося як проста ідея для Центрів операцій безпеки, тепер перетворилося на величезну галузь, яка спирається на висококваліфікованих фахівців, які стежать за всім одночасно, забезпечуючи безпеку та надійність корпоративних даних.

Ключові переваги SOC

Звісно ж, наявність SOC має довгий список переваг для бізнесу. Ось деякі з них: 1) Центр операцій безпеки дозволяє компаніям збирати відповідні дані в одному центральному місці. 2) Центр операцій безпеки покращує здатність компаній швидко та рішуче реагувати на нові загрози. 3) Компанії, які інвестують у центри безпеки, з більшою ймовірністю дотримуються правил, що регулюють кібербезпеку. 4) Компанії з центром безпеки мають легшу співпрацю з правоохоронними органами. 5) Центр операцій безпеки дозволяє компаніям швидше виявляти вторгнення та атаки й мінімізувати їх вплив. 6) Центр операцій безпеки дозволяє компаніям краще навчати своїх співробітників кіберризикам та способам їх уникнення. 7) Центр операцій безпеки покращує можливості компаній контролювати активність авторизованих користувачів у своїх системах, значно зменшуючи внутрішні загрози. 8) Наявність центру операцій безпеки покращує можливості компаній моніторити, реагувати та повідомляти про кіберзагрози. 9) Наявність центру операцій безпеки дозволяє компаніям централізувати моніторинг, скорочуючи час повідомлення про інцидент та забезпечуючи швидше вирішення проблем. 10) Центр операцій безпеки дозволяє компаніям надавати кращі послуги своїм клієнтам, дотримуючись галузевих стандартів та державних норм. 11) Центр операцій безпеки дозволяє компаніям бути проактивними, а не реактивними, у боротьбі з кіберзагрозами. 12) Компанії, які інвестують у центри безпеки, з меншою ймовірністю стануть мішенню кіберзлочинців. 13) Центр операцій безпеки дозволяє компаніям дотримуватися галузевих стандартів щодо найкращих практик кібербезпеки. 14) Інвестиції в центр операцій безпеки дозволяють компаніям бути проактивними та звітувати про свої заходи управління ризиками, покращуючи свою репутацію як серед клієнтів, так і серед акціонерів. 15) Центри операцій безпеки дозволяють компаніям уникати штрафів та судових позовів, що виникають унаслідок витоків даних.

Які найбільші проблеми центрів безпеки операцій?

Відстеження загроз та мінімізація їхнього впливу на підприємство є постійним викликом для компаній, але цей виклик став легшим з розвитком технологій. Центри операцій безпеки є критично важливими для інформаційної безпеки. Вони відповідають за моніторинг, оцінку та захист ІТ-активів.

Ця відповідальність вимагає значного планування та знань як ІТ-інфраструктури, так і принципів кібербезпеки для успішного виконання. Постійно зростаюча мережева інфраструктура, старіюче обладнання, величезна площа атак та скорочення бюджетів ускладнюють їхню роботу.

Щоб подолати ці проблеми, центри операцій безпеки повинні впроваджувати інновації та автоматизацію для централізації своїх даних. Це означає перехід від розрізненої, ізольованої інформації до централізованої платформи, де їхні дані доступні та використовуються для спільного використання. Цей крок може бути особливо важливим для компаній з центрами операцій фізичної безпеки (SOC), оскільки вони мають найбільшу потребу в прозорості та більших засобах захисту від фізичних загроз.

Майбутнє державних операційних компаній

У світі, де кіберзлочинці стають дедалі витонченішими, Центри операцій безпеки повинні мати можливість швидко адаптуватися та розвиватися, щоб залишатися на крок попереду конкурентів. Це означає, що їм необхідно мати ресурси та підтримку ІТ-відділу своєї компанії, а також інструменти, доступні для успішної роботи команд безпеки. Майбутнє центрів операцій безпеки буде рухомим, реагуючи на загрози в режимі реального часу за допомогою автоматизації та машинного навчання. Однак вони ніколи не зможуть

замінити кваліфікованих та відданих фахівців з безпеки, яким доводиться виконувати складну роботу.

У складному та швидкозмінному ландшафті сучасних кіберзагроз організації стикаються з безпрецедентним викликом у захисті своїх цифрових активів, конфіденційних даних та забезпеченні безперервності операційної діяльності. Величезний обсяг та складність кібератак вимагають централізованого, проактивного та вузькоспеціалізованого підходу до безпеки. Саме тут Центр операцій безпеки (SOC) стає невід'ємним компонентом загальної стратегії кібербезпеки організації.

Центр операцій безпеки (SOC) – це централізована функція в організації або послуга, що надається третьою стороною, яка займається постійним моніторингом та аналізом стану безпеки організації. Його основна мета – виявляти, запобігати, розслідувати та реагувати на кіберінциденти та загрози цілодобово. SOC – це набагато більше, ніж просто набір інструментів безпеки, це нервовий центр, де люди, процеси та технології сходяться для забезпечення комплексних операцій безпеки. Він являє собою фундаментальний перехід від реактивних заходів безпеки до проактивного, заснованого на розвідці захисного механізму, призначеного для захисту організації від безлічі потенційних загроз, що ховаються в цифровому світі.

Основна роль Центру операцій безпеки (SOC): понад базовий захист

Роль SOC виходить далеко за рамки простого реагування на сповіщення; вона втілює стратегічний імператив підтримки цифрової стійкості. В епоху, коли кіберзагрози є постійними та дедалі складнішими, багато організацій усвідомлюють, що надійна система безпеки вимагає цілеспрямованого експертного нагляду. Команда операцій безпеки в SOC має головне завдання: забезпечити конфіденційність, цілісність та доступність (тріада ЦПУ) інформаційних активів організації.

Центр безпеки (SOC) діє як центральний розвідувальний центр, постійно збираючи та зіставляючи інформацію про безпеку з усього ІТ-середовища. Це включає дані з мереж, серверів, кінцевих точок, програм, баз даних та різних інструментів безпеки. Консолідуючи цей величезний обсяг інформації, аналітики SOC отримують цілісне уявлення про ландшафт безпеки, що дозволяє їм виявляти підозрілу активність, яка в іншому випадку могла б залишитися непоміченою. Така всебічна видимість має вирішальне значення для ефективного виявлення загроз, розслідування та швидкого реагування на інциденти. Стратегічна цінність SOC полягає в його здатності перетворювати необроблені дані безпеки на дієву інформацію, що дозволяє командам безпеки не лише виявляти та стримувати загрози, але й розуміти їх походження та запобігати майбутнім випадкам.

Ключові функції та обов'язки SOC

Щоденна діяльність SOC охоплює широкий спектр функцій, кожна з яких є критично важливою для створення та підтримки надійної системи безпеки. Ці функції виконує спеціальна команда аналітиків та фахівців з безпеки, використовуючи передові рішення безпеки та чітко визначені процеси.

Безперервний моніторинг безпеки та сортування за тривогами

Одним з основоположних обов'язків SOC є постійний моніторинг усіх систем, мереж та програм у режимі реального часу в інфраструктурі організації. Ця цілодобова пильність спрямована на виявлення будь-яких ознак аномальної поведінки або потенційних загроз. Процес моніторингу генерує велику кількість сповіщень від різних інструментів безпеки, таких як брандмауери, системи виявлення/запобігання вторгненням (IDS/IPS), рішення для виявлення та реагування на мережу (NDR), рішення для виявлення та реагування на кінцеві точки (EDR) та системи управління інформацією та подіями безпеки (SIEM).

Аналітики SOC відповідають за початкове сортування цих сповіщень, розрізняючи справжні інциденти безпеки та хибнопозитивні результати. Це вимагає глибокого розуміння нормальної поведінки мережі та законної системної активності. Ефективне сортування значно знижує втому від сповіщень, дозволяючи команді зосередити свою увагу та ресурси

на критичних подіях, які становлять реальний ризик. Мета полягає в тому, щоб швидко виявити підозрілу активність, перш ніж вона переросте в повноцінну кібератаку.

Виявлення та аналіз загроз

Після того, як сповіщення класифікується як потенційно шкідливе, команда SOC розпочинає глибше розслідування виявленої загрози. Це включає детальний аналіз журналів, даних мережевого трафіку, телеметрії кінцевих точок та іншої відповідної інформації безпеки, щоб зрозуміти природу, масштаб та потенційний вплив інциденту безпеки. Аналітики використовують розширену аналітику, моделювання поведінки та можливості машинного навчання, часто інтегровані в їхні інструменти безпеки, щоб зіставити, здавалося б, різноманітні фрагменти інформації та виявити закономірності, що вказують на кіберзагрозу.

Використання актуальної інформації про загрози є надзвичайно важливим на цьому етапі. Канали інформації про загрози надають інформацію про відомі вразливості, нові вектори атак, тактику, методи та процедури зловмисників (TTP), а також індикатори компрометації (IoC). Зіставляючи внутрішні спостереження із зовнішньою інформацією про загрози, аналітики SOC можуть точніше ідентифікувати загрози, розуміти їхні характеристики та прогнозувати їх потенційний розвиток, що дозволяє проводити більш ефективні та цілеспрямовані операції безпеки.

Реагування на інциденти та їх усунення

Кінцева мета виявлення загроз полягає в забезпеченні швидкого та ефективного реагування на інциденти. Коли виявляється підтверджений інцидент безпеки, команда SOC негайно запускає план реагування на інцидент. Цей критичний процес зазвичай включає кілька фаз: Ідентифікація: Підтвердження інциденту та збір початкової інформації; Стимування: Вжиття негайних заходів для ізоляції уражених систем або мереж, щоб запобігти подальшому поширенню інциденту. Це може включати відключення пристроїв, блокування IP-адрес або карантин шкідливого програмного забезпечення; Викорінення: Усунення першопричини інциденту, наприклад, видалення шкідливого програмного забезпечення, виправлення вразливостей або видалення шкідливих конфігурацій; Відновлення: Відновлення уражених систем і даних до нормального стану, що може включати відновлення з резервних копій, перебудову систем або переналаштування засобів безпеки; Аналіз після інциденту (вивчені уроки): Вирішальний крок, під час якого команда аналізує, що сталося, чому це сталося та як запобігти подібним інцидентам у майбутньому. Цей цикл зворотного зв'язку зміцнює загальний рівень безпеки організації.

Швидкість і точність реагування на інциденти є життєво важливими для мінімізації збитків, скорочення простоїв та підтримки довіри в організації. Фахівці з реагування на інциденти SOC співпрацюють, часто з іншими IT-відділами, для ефективного усунення загроз.

Управління вразливостями та оцінка ризиків

Проактивний SOC виходить за рамки реагування на активні загрози; він активно працює над зменшенням поверхні атаки організації. Це передбачає постійне управління вразливостями, яке включає виявлення, оцінку та визначення пріоритетів слабких місць безпеки в системах, додатках та мережевій інфраструктурі. Команди SOC часто проводять регулярне сканування вразливостей, тести на проникнення та аудити безпеки, щоб виявити потенційні точки входу для зловмисників.

Після виявлення вразливостей, SOC співпрацює з командами IT-операцій, щоб забезпечити своєчасне встановлення виправлень, посилення конфігурації та впровадження політик безпеки, розроблених для зменшення цих ризиків. Проактивно усуваючи слабкі місця, SOC допомагає зміцнити загальний рівень безпеки та зменшити ймовірність успішних кібератак. Оцінка ризиків – це безперервний процес, який оцінює потенційний вплив виявлених вразливостей та загроз на бізнес-операції та дані.

Полювання на загрози: проактивний захист

Хоча постійний моніторинг та автоматичні сповіщення є важливими, вони часто реагують на відомі загрози або заздалегідь визначені правила. З іншого боку, полювання на

загрози – це проактивний та ітеративний процес, у якому аналітики безпеки, яких часто називають мисливцями за загрозами, активно шукають невідомі або невиявлені загрози, що ховаються в мережі організації. Це передбачає використання глибокого контекстуального розуміння середовища, розвідки загроз та розслідувань на основі гіпотез.

Мисливці за загрозами працюють, виходячи з припущення, що організація вже була скомпрометована або зазнає малопомітної атаки. Вони шукають аномальну поведінку, малопомітні індикатори компрометації (IoC) та відхилення від нормальних базових показників, які автоматизовані інструменти можуть пропустити. Ця вузькоспеціалізована функція вимагає розширених аналітичних навичок, глибоких знань методологій зловмисників та доступу до багатих, детальних джерел даних, особливо до мережових пакетних даних. Мета полягає у виявленні складних, прихованих кіберзагроз, таких як передові постійні загрози (APT), перш ніж вони зможуть завдати значної шкоди.

Інтеграція з управлінням інформацією та подіями безпеки (SIEM)

Система управління інформацією та подіями безпеки (SIEM) є базовою технологією майже для кожної SOC. Рішення SIEM агрегує та централізує дані журналів і подій практично з кожного пристрою та програми в IT-інфраструктурі організації. Це включає дані з брандмауерів, серверів, операційних систем, мережових пристроїв, інструментів безпеки та програм.

Потім SIEM нормалізує ці різноманітні дані, роблячи їх узгодженими та зручними для пошуку. Найголовніше, що SIEM використовує правила кореляції та аналітичні механізми для виявлення закономірностей та зв'язків у даних, які вказують на підозрілу активність або потенційні інциденти безпеки. Наприклад, він може співвіднести невдалу спробу входу на одному сервері з успішним входом з того ж облікового запису користувача на іншому сервері в незвичному місці, позначаючи це як потенційну компрометацію.

Ключова відмінність між SIEM та SOC полягає в тому, що SIEM є потужним інструментом, який використовується SOC. SOC – це операційна команда та об'єкт, який використовує SIEM (разом з багатьма іншими інструментами та процесами) для досягнення своїх цілей моніторингу, виявлення, аналізу та реагування на загрози. Без SIEM здатність SOC отримувати повну видимість та співвідносити події була б серйозно обмежена, що зробить виявлення загроз, розслідування та реагування на інциденти набагато складнішими та трудомісткішими.

Автоматизація та оркестрація безпеки (SOAR)

Щоб впоратися зі зростаючим обсягом та складністю інцидентів безпеки, багато сучасних центрів охорони безпеки (SOC) інтегрують платформи оркестрації, автоматизації та реагування на безпеку (SOAR). Технології SOAR дозволяють командам SOC стандартизувати, автоматизувати та оркеструвати робочі процеси операцій безпеки.

Автоматизація передбачає автоматичне виконання завдань і процесів, таких як блокування шкідливої IP-адреси, виявленої за допомогою сповіщення SIEM, ізоляція зараженої кінцевої точки або збагачення інциденту даними розвідки про загрози. Оркестрація означає координацію кількох інструментів та систем безпеки для безперебійної спільної роботи в межах визначеного робочого процесу, часто ініційованого сповіщенням. Можливості реагування в SOAR надають інструменти для управління інцидентами, співпраці та створення звітів.

Впровадження автоматизації та оркестрації значно підвищує ефективність та швидкість роботи SOC. Це зменшує ручне навантаження на аналітиків безпеки, дозволяючи їм зосередитися на складних розслідуваннях та стратегічному пошуку загроз, а не на повторюваних завданнях. Це також призводить до швидшого реагування на інциденти, мінімізуючи вікно можливостей для зловмисників та зменшуючи потенційний вплив кібератаки.

Відповідність та звітність

Окрім безпосереднього зменшення загроз, SOC відіграє вирішальну роль у забезпеченні дотримання організацією різних нормативних вимог та галузевих стандартів.

Багато організацій підпадають під дію таких вимог щодо дотримання, як GDPR, HIPAA, PCI DSS та SOX, які вимагають суворого контролю безпеки та надійних механізмів звітності. SOC постійно контролює системи, щоб забезпечити їх відповідність цим правилам та внутрішнім політикам безпеки. Вони генерують детальні звіти про стан безпеки, виявлені інциденти, вразливості та зусилля з усунення наслідків, надаючи необхідну документацію для аудитів та демонструючи належну перевірку. Ця звітність не лише служить регуляторним цілям, але й надає вищому керівництву цінну інформацію щодо стану безпеки організації та поточних ризиків, допомагаючи приймати стратегічні рішення та розподіляти ресурси для рішень безпеки.

Неперевершена потужність пакетних даних у SOC

Хоча журнали та сповіщення надають цінну інформацію про те, що сталося в системі, вони часто пропонують узагальнений або відфільтрований огляд подій. Для справді повного розуміння мережевої активності та найдеталізованішого рівня деталізації, необхідного для розширеного виявлення та пошуку загроз, SOC значною мірою покладається на дані мережевих пакетів. Цей необроблений, нефільтрований потік інформації, що проходить мережею, забезпечує неперевершений рівень видимості, виступаючи головним джерелом достовірної інформації в розслідуваннях кібербезпеки.

Чому саме пакетні дані? Нефільтрована правда та глибока прозорість

Мережеві пакетні дані представляють собою кожен фрагмент інформації, що передається мережею, включаючи джерело, пункт призначення, протокол і корисне навантаження кожного зв'язку. На відміну від журналів, які генеруються певними програмами або системами і можуть не фіксувати всі деталі або навіть бути підроблені зловмисниками, пакетні дані пропонують незмінний запис мережевого трафіку. Це «істина», яка точно показує, що відбувалося в мережі.

Ця глибока видимість є критично важливою, оскільки: Відсутність сліпих зон: Пакетні дані фіксують усі мережеві комунікації, незалежно від того, чи генерують вони запис у журналі, чи їх бачать інші засоби безпеки. Це означає, що можна виявити приховані канали командування та управління (C2), спроби прихованого витоку даних або складні горизонтальні переміщення, що обходять засоби контролю безпеки кінцевих точок; Незаперечні докази: Для криміналістики та реагування на інциденти пакетні дані надають переконливі докази зловмисної діяльності. Вони можуть реконструювати цілі шляхи атаки, показати послідовність подій та точно визначити момент компрометації або витоку даних; Поза межами сигнатур: Хоча системи виявлення на основі сигнатур спираються на відомі шкідливі шаблони, аналіз пакетів може виявити аномальну поведінку, навіть для загроз нульового дня або варіацій відомого шкідливого програмного забезпечення, для яких ще не існує сигнатури. Поведінковий аналіз пакетних даних може виявити незвичне використання протоколу, шаблони зв'язку або розміри передачі даних.

Практичні висновки: від фрагментів до порушень

Здатність захоплювати, зберігати та аналізувати мережеві пакетні дані трансформувє можливості SOC ефективно виявляти, розуміти, виявляти та видаляти загрози.

Ідентифікація: Точне виявлення аномалій та вторгнень. Пакетні дані дозволяють аналітикам SOC швидко виявляти аномалії, які можуть сигналізувати про кібератаку. Це включає:

Незвичайні мережеві потоки: виявлення підключень до підозрілих IP-адрес, нетипового використання портів або обсягів трафіку, що суттєво відхиляються від встановлених базових значень.

Зв'язок командування та управління (C2): Виявлення закономірностей, що вказують на канали C2, таких як активність маяків, використання нестандартних протоколів або зв'язок з відомими шкідливими доменами.

Витік даних: розпізнавання передачі великих обсягів даних до зовнішніх, несанкціонованих місць призначення або надсилання незвичайних типів файлів, що може свідчити про крадіжку даних.

Внутрішні загрози: моніторинг внутрішнього мережевого трафіку на предмет несанкціонованого доступу до конфіденційних систем, незвичайного переміщення даних привілейованими користувачами або порушень політик, що свідчать про зловмисну інсайдерську діяльність.

Аналізуючи пакетні дані в режимі реального або майже реального часу, команди SOC можуть отримати негайне уявлення про підозрілу активність, що дозволяє швидко виявляти потенційні інциденти безпеки до їх ескалації.

Полювання на загрози: слідування цифровим хлібним крихтам

Для проактивного пошуку загроз пакетні дані є незамінними. Мисливці за загрозами використовують пакетні дані для:

Реконструкція шляхів атаки: Відстежуючи потік мережевого трафіку, мисливці можуть відстежувати горизонтальне переміщення зловмисника в мережі, розуміти, як він отримав доступ, та ідентифікувати скомпрометовані системи. Це забезпечує повну картину ланцюжка знищення кібератаки.

Виявлення прихованих загроз: Досвідчені зловмисники часто використовують легітимні інструменти та протоколи, щоб зливатися зі звичайним мережевим трафіком, що ускладнює їх виявлення за допомогою традиційних заходів безпеки. Аналіз пакетів може виявити ці тонкі індикатори, такі як незвичне використання протоколів, зашифровані тунелі або приховані канали, що використовуються для зв'язку.

Перевірка гіпотез: Коли мисливець за загрозами підозрює певний тип атаки або наявність індикатора компрометації (IoC) у мережі, він може використовувати пакетні дані для перевірки своєї гіпотези. Наприклад, якщо відомо, що певне шкідливе програмне забезпечення зв'язується через певний порт, пакетні дані можуть підтвердити, чи справді будь-які внутрішні хости здійснюють такі з'єднання.

Розуміння масштабу: Пакетні дані допомагають визначити повний масштаб порушення, ідентифікуючи всі уражені системи та дані, що має вирішальне значення для комплексного стримування.

Видалення та відновлення: цілеспрямована та науково обґрунтована відповідь

Коли інцидент підтверджено, пакетні дані надають незаперечні докази, необхідні для цілеспрямованого стримування та ліквідації:

Точне стримування: Визначивши точне джерело та пункт призначення шкідливого трафіку, команди SOC можуть впроваджувати високоточні заходи стримування, такі як блокування певних з'єднань або ізоляція скомпрометованих хостів, мінімізуючи порушення законних операцій.

Ефективне знищення: Пакетні дані розкривають методи, що використовуються зловмисниками, спрямовуючи зусилля з знищення. Наприклад, якщо витік даних стався через певний протокол, команда точно знає, на чому зосередити свої зусилля для очищення та запобігання.

Криміналістика після інциденту: Для ретельного аналізу після інциденту пакетні дані є безцінними. Вони дозволяють судовим слідчим відтворювати мережеву активність, аналізувати корисні навантаження та розуміти повний вплив порушення, сприяючи покращенню політик та практик безпеки.

Аналіз першопричин: Розуміння того, «як» і «чому» відбувається атака, є надзвичайно важливим. Пакетні дані дозволяють провести глибокий аналіз першопричин, визначити початкову точку проникнення та використати вразливості, що життєво важливо для запобігання повторенню.

За межами реактивності: проактивна безпека з пакетними даними

Стратегічна інтеграція пакетних даних в операції SOC перетворює безпеку з виключно реактивної моделі, що керується сповіщеннями, на проактивний захист, що керується розвідкою. Забезпечуючи нефільтрований, комплексний огляд мережевої активності, це дає командам безпеки можливість виявляти, виявляти та усувати загрози з неперевершеною точністю та швидкістю. Ця можливість є основою для досягнення

справжньої кіберстійкості, дозволяючи організаціям випереджати складних супротивників та захищати свої найважливіші активи. Сучасні рішення для виявлення та реагування на мережі (NDR) спеціально розроблені для використання можливостей пакетних даних, пропонуючи глибоку видимість та поведінкову аналітику для розширення можливостей SOC.

Ключові ролі в команді SOC

Високоєфективна SOC спирається на міждисциплінарну команду, кожен член якої вносить свій спеціалізований внесок у зусилля з колективної безпеки. Хоча конкретні посади та рівні можуть відрізнятися, основні функції загалом однакові:

Менеджер/керівник SOC: Ця особа здійснює стратегічний нагляд та керівництво всім SOC. Вона відповідає за визначення бачення SOC, встановлення операційних цілей, управління персоналом, забезпечення дотримання політик безпеки та ескалацію критичних інцидентів вищому керівництву. Менеджер SOC також відіграє ключову роль в ініціативах щодо постійного вдосконалення та сприяння культурі досконалості в команді.

Аналітики безпеки (рівень 1, 2, 3): це захисники на передовій, які формують ядро команди SOC. Їхні ролі зазвичай розподіляються на рівні залежно від досвіду та складності інцидентів, з якими вони працюють:

Аналітики 1-го рівня: часто їх називають «спеціалістами з сортування сповіщень», ці аналітики відповідають за початковий моніторинг сповіщень безпеки, фільтрацію хибнопозитивних результатів та проведення попередніх розслідувань. Вони дотримуються встановлених методичних рекомендацій для ескалації підтверджених інцидентів на вищий рівень. Їхні обов'язки зазвичай включають цілодобовий моніторинг, перевірку початкових сповіщень та збір базових даних.

Аналітики 2-го рівня: це більш досвідчені аналітики, які проводять глибші розслідування інцидентів, що ескалирували з 1-го рівня. Вони виконують детальний аналіз, використовують передові інструменти безпеки (включаючи SIEM та NDR) та працюють над стратегіями стримування. Вони вміють розуміти тактику зловмисників та розробляти дії негайного реагування.

Аналітики 3-го рівня: Найстарші та найкваліфікованіші аналітики безпеки, також відомі як «мисливці за загрозами» або «судові слідчі». Вони обробляють найскладніші та найсучасніші загрози, виконують проактивне полювання на загрози, проводять поглиблений судово-медичний аналіз та розробляють власні правила виявлення. Вони часто мають досвід у зворотному проектуванні, аналізі шкідливих програм та передових методологіях боротьби з постійними загрозами (APT).

Мисливці за загрозами: Хоча вони часто є підгрупою аналітиків 3-го рівня, деякі організації присвячують певні ролі пошуку загроз. Ці фахівці є проактивними, керованими гіпотезами слідчими, які активно шукають невідомі загрози, що обійшли існуючі засоби контролю безпеки. Вони використовують складні методи та величезні набори даних, включаючи мережеві пакетні дані, для виявлення прихованих супротивників.

Реагування на інциденти: Ці фахівці спеціалізуються на фазах стримування, ліквідації та відновлення після інцидентів. Хоча всі аналітики SOC беруть участь у реагуванні на інциденти, спеціалізовані фахівці з реагування на інциденти часто керують повним життєвим циклом серйозного порушення, координуючи зусилля кількох команд та забезпечуючи швидке повернення до нормальної роботи. Вони вміють аналізувати та звітувати про інциденти після інциденту.

Фахівці з управління вразливостями: Ці члени команди зосереджуються на виявленні, оцінці та визначенні пріоритетів вразливостей в інфраструктурі організації. Вони проводять сканування, аналізують результати та співпрацюють з IT-командами, щоб забезпечити усунення вразливостей, тим самим зменшуючи поверхню атаки.

Інженери/архітектори безпеки: Хоча інженери безпеки не завжди входять до безпосередньої операційної команди SOC, вони часто тісно співпрацюють з SOC. Вони відповідають за проектування, впровадження та підтримку інфраструктури та інструментів

безпеки (SIEM, EDR, NDR, брандмауери тощо), на які покладається SOC. Вони надають експертизу в оптимізації рішень безпеки та інтеграції нових технологій.

Спільний характер цих ролей є важливим для ефективної роботи SOC, що забезпечує постійний моніторинг, захист та вдосконалення всіх аспектів кібербезпеки організації.

Типи моделей SOC

Організації можуть впроваджувати Центр операцій безпеки кількома способами, кожен з яких має свої переваги та міркування, залежно від таких факторів, як бюджет, внутрішні можливості та конкретні вимоги безпеки.

Внутрішній SOC: Ця модель передбачає створення та функціонування SOC повністю всередині організації.

Переваги: Забезпечує повний контроль над операціями, процесами та даними безпеки. Дозволяє глибоку інтеграцію з внутрішніми бізнес-процесами та конкретними політиками безпеки. Команда отримує глибокі знання про унікальне середовище та ризики організації.

Недоліки: Вимагає значних початкових інвестицій у технології, інфраструктуру та кваліфікований персонал. Укомплектування цілодобової операції експертами-аналітиками безпеки може бути складним та дорогим через нестачу фахівців з кібербезпеки. Поточні операційні витрати, включаючи навчання та обслуговування інструментів, можуть бути високими.

Аутсорсинг SOC (SOC-as-a-Service / SOCaaS): У цій моделі організація укладає договір зі стороннім постачальником керованих послуг безпеки (MSSP) для виконання функцій SOC. SOC-as-a-Service (SOCaaS) – це популярна пропозиція, коли постачальник керує моніторингом, виявленням загроз, попереднім розслідуванням та реагуванням на інциденти з власних потужностей.

Переваги: Економічно ефективний, оскільки дозволяє уникнути капітальних витрат та проблем із персоналом, пов'язаних із внутрішньою SOC. Забезпечує негайний доступ до спеціалізованих експертів з кібербезпеки, часто з цілодобовим покриттям. Пропонує масштабованість та може надавати інформацію про загрози, що перевищує ту, яку може зібрати одна організація. Швидке розгортання рішень безпеки.

Недоліки: Менший прямий контроль над операціями безпеки та даними. Організації повинні ретельно перевіряти постачальників, щоб забезпечити довіру та дотримання вимог відповідності. Потенційні проблеми щодо суверенітету даних та того, як конфіденційна інформація безпеки обробляється третьою стороною.

Гібридний SOC: Ця модель поєднує елементи як внутрішнього, так і аутсорсингового підходів. Наприклад, організація може підтримувати менший внутрішній SOC для критичних систем та реагування на основні інциденти, одночасно передаючи цілодобовий моніторинг та первинне сортування сповіщень постачальнику послуг з управління операційною службою (MSSP).

Переваги: Поєднує контроль з економічною ефективністю та доступом до спеціалізованих експертів. Дозволяє організації зосередитися на своїх найбільш чутливих активах, використовуючи зовнішні ресурси для ширшого охоплення.

Недоліки: Потрібна ретельна координація та чіткий розподіл обов'язків між внутрішньою командою та зовнішнім постачальником, щоб уникнути прогалин або дублювання.

Кероване виявлення та реагування (MDR): Хоча MDR часто надається постачальниками послуг з управління загрозами (MSSP), це окрема послуга, яка зосереджена саме на розширеному виявленні загроз, розслідуванні загроз, пошуку загроз та швидкому реагуванні на інциденти. На відміну від традиційного SOCaaS, який може більше зосереджуватися на моніторингу безпеки та базовому оповіщенні, MDR йде глибше, пропонуючи проактивне виявлення загроз та управління інцидентами під керівництвом експертів.

Переваги: Забезпечує більш проактивний та практичний підхід до управління загрозами. Пропонує спеціалізованих мисливців за загрозами та реагування на інциденти, які

активно виявляють та усувають загрози. Може доповнити існуючу внутрішню команду безпеки.

Недоліки: Може бути дорожчим за базовий SOCaaS. Вимагає високого рівня довіри з постачальником, враховуючи його глибокий доступ до середовища організації.

Вибір моделі SOC значною мірою залежить від унікального профілю ризиків організації, наявності ресурсів та стратегічних цілей безпеки.

Побудова ефективної SOC: найкращі практики

Створення та функціонування ефективного Центру операцій безпеки вимагає не лише придбання передових інструментів безпеки; воно вимагає стратегічного підходу, що охоплює людей, процеси та технології. Дотримання найкращих практик може значно покращити здатність Центру операцій безпеки захищати організацію від кіберзагроз.

Визначте чіткі цілі та показники: Перш ніж створювати або оптимізувати SOC, вкрай важливо визначити його цілі. Які конкретні ризики він враховуватиме? Як буде вимірюватися його успіх? Цілі повинні відповідати загальним бізнес-цілям та дотриманню нормативних вимог. Ключові показники ефективності (KPI) та показники, такі як середній час виявлення (MTTD), середній час отримання знань (MTTK), середній час реагування (MTTR), кількість хибнопозитивних результатів та серйозність інцидентів, є важливими для постійного вдосконалення та демонстрації цінності.

Інвестуйте в правильний технологічний стек: Потужний SOC спирається на надійний набір рішень безпеки. Зазвичай це включає SIEM для агрегації та кореляції журналів, Endpoint Detection and Response (EDR) або Extended Detection and Response (XDR) для видимості кінцевих точок, Network Detection and Response (NDR) для глибокої видимості мережі (особливо пакетних даних), Security Orchestration, Automation, and Response (SOAR) для ефективності, а також платформи розвідки загроз. Ключем є інтеграція та сумісність між цими інструментами для створення єдиної екосистеми безпеки.

Формуйте кваліфіковану команду: лише технологій недостатньо. Ефективність SOC залежить від досвіду її аналітиків та спеціалістів з безпеки. Інвестуйте в постійне навчання та професійний розвиток, щоб підтримувати навички в актуальному стані з урахуванням кіберзагроз та технологій, що розвиваються. Сприяйте культурі безперервного навчання, обміну знаннями та співпраці в командах SOC. Розгляньте можливість перехресного навчання для розвитку резервних можливостей та стійкості.

Встановлення надійних процесів та інструкцій: Чіткі, добре задокументовані процеси є основою ефективних операцій SOC. Розробіть комплексні інструкції реагування на інциденти для різних типів інцидентів безпеки, що окреслюють покрокові процедури виявлення, аналізу, стримування, ліквідації та відновлення. Впроваджуйте стандартизовані робочі процеси для сортування тривог, управління вразливостями та звітності. Регулярні навчання та симуляції (навчання «Червона команда» проти «Синьої команди») допомагають удосконалити ці процеси та забезпечити готовність команди до реальних сценаріїв.

Інтеграція інформації про загрози: Щоб випереджати розвиток кіберзагроз, SOC повинен постійно отримувати та інтегрувати відповідну інформацію про загрози. Це включає інформацію про нові вразливості, нові вектори атак, групи зловмисників та індикатори компрометації (IoC). Інтеграція цієї інформації в правила SIEM, запити на пошук загроз та процеси управління вразливостями дозволяє SOC проактивно виявляти та пом'якшувати ризики.

Впровадження автоматизації та оркестрації: для боротьби зі втомою від сповіщень та покращення часу реагування використовуйте автоматизацію для повторюваних завдань (наприклад, блокування шкідливих IP-адрес, ізоляція кінцевих точок, збагачення сповіщень). Платформи SOAR можуть оркеструвати складні робочі процеси, забезпечуючи послідовне та швидке виконання дій реагування, звільняючи аналітиків безпеки для зосередження на складніших аналітичних та пошукових заходах.

Постійне вдосконалення: SOC не є статичною структурою; вона повинна постійно адаптуватися та вдосконалюватися. Регулярно переглядайте дані про інциденти, проводите

аналіз після інцидентів для виявлення отриманих уроків та вдосконалюйте процеси та технології на основі цих даних. Збирайте відгуки від команди SOC та інших зацікавлених сторін для оптимізації операцій та покращення загального стану безпеки. Регулярно оцінюйте нові рішення безпеки та коригуйте стратегію для реагування на нові кіберзагрози.

Ретельно впроваджуючи ці найкращі практики, організації можуть створити та вдосконалити високоефективний Центр операцій безпеки, який забезпечує надійні, проактивні можливості кіберзахисту від сучасного складного ландшафту загроз.



Рисунок 1 – Структурна схема системи

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів мережевого корпоративного центру управління інформаційною безпекою (SOC). Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем мережевого корпоративного центру управління інформаційною безпекою (SOC).
- Досліджена система мережевого корпоративного центру управління інформаційною безпекою (SOC).
- На основі отриманих результатів досліджень створена програмна реалізація системи мережевого корпоративного центру управління інформаційною безпекою (SOC). Розроблені алгоритми дозволяють успішно вирішувати завдання мережевого корпоративного центру управління інформаційною безпекою (SOC). 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. 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.
4. 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.
5. 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.
6. 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.
7. 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.
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. 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.
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. Akhalaia, G., Iavich, M., Iashvili, G., Prisyazhnyy, D., Smirnova, T. «Secure Encrypted Connection on Georgian Website». CEUR Workshop Proceedings, 2023, 3550, pp. 313-320.
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., Yenchov, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». CEUR Workshop Proceedings, Volume 3530, 2023, pp. 256-265.
15. 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.
16. 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.
17. 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.
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. 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,
23. 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.
24. 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.
 25. 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.
 26. 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.
 27. 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.
 28. 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
 29. 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.
 30. 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.
 31. 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.
 32. 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.

УДК 004

Н.Касьянов, магістр гр. КІ-24М,

Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ВИЗНАЧЕННЯ МІСЦЕЗНАХОДЖЕННЯ ЗА ДОПОМОГОЮ ПРОТОКОЛУ APPLE LOCATION SERVICES PROTOCOL

У статті розроблено програмне забезпечення, яке призначено для системи визначення місцезнаходження за допомогою протоколу Apple Location Services Protocol. Метою розробки є дослідження та принципи побудови системи визначення місцезнаходження за допомогою протоколу Apple Location Services Protocol. Об'єктом дослідження є процес визначення місцезнаходження за допомогою протоколу Apple Location Services Protocol. Предметом дослідження є методи визначення місцезнаходження за допомогою протоколу Apple Location Services Protocol. Методи дослідження базуються на методах теорії геопозиціонування, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи визначення місцезнаходження за допомогою протоколу Apple Location Services Protocol. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

система визначення місцезнаходження, Apple Location Services Protocol

Постановка проблеми. Програми для геолокаційних послуг (LBS) поширюються та підтримують транспорт, розваги тощо. Сучасні мобільні платформи, яскравим прикладом яких є смартфони, покладаються на наземну та супутникову інфраструктуру (наприклад, глобальну навігаційну супутникову систему (GNSS) та краудсорсингові бази даних Wi-Fi, Bluetooth, стільникового зв'язку та IP) для правильного позиціонування. Однак вони вразливі до атак, які маніпулюють позиціями для контролю та підриву функціональності LBS, що дозволяє шахрайство з користувачами або сервісами. Наша робота показує, що атаки зі спуфінгом GNSS успішні, навіть якщо смартфони мають кілька джерел інформації про позиціонування. Більше того, атаки зі спуфінгом Wi-Fi з глушінням GNSS є напоручд ефективними. Більше занепокоєння викликають докази того, що складні, скоординовані атаки зі спуфінгом є дуже ефективними. Атаки можуть бути спрямовані на GNSS у поєднанні з іншими методами позиціонування, тому захист, який припускає, що атакується лише GNSS, не може бути ефективним. Більше того, стійкі приймачі GNSS та антени спеціального призначення неможливі на смартфонах.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи визначення місцезнаходження за допомогою протоколу apple location services protocol.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи визначення місцезнаходження за допомогою протоколу Apple Location Services Protocol.

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

- Огляд існуючих систем визначення місцезнаходження за допомогою протоколу Apple Location Services Protocol.
- Дослідження системи визначення місцезнаходження за допомогою протоколу Apple Location Services Protocol.

– Програмна реалізація системи визначення місцезнаходження за допомогою протоколу Apple Location Services Protocol.

Об'єктом дослідження є процес визначення місцезнаходження за допомогою протоколу Apple Location Services Protocol.

Предметом дослідження є методи визначення місцезнаходження за допомогою протоколу Apple Location Services Protocol.

Методи дослідження базуються на методах теорії геопозиціонування, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. **A-GPS (Assisted GPS)** система застосовується для прискорення початку роботи GPS у мобільному пристрої або безпосередньо визначення координат мобільного пристрою без одержання даних безпосередньо від супутників. Можна виділити два основних режими роботи з A-GPS.

– Перший – основний, коли всю роботу з визначення координат пристрою виконує інфраструктура провайдеру стільникового зв'язку.

– Другий – допоміжний, прискорювальний запуск основного GPS пристрою, шляхом відновлення через базу оператора мобільного зв'язку інформації об альманах, ефемеридах і списку видимих супутників. У цьому випадку убудований GPS приймач сам приймає й обробляє інформацію для визначення координат. Особливістю A-GPS є її підвищена чутливість і велика швидкодія. На відкритих просторах A-GPS дозволяє одержати точність у визначенні координат до 15м.

Дослідження протоколу Apple Location Services Protocol (ALSP)

Звичайний спосіб дослідження трафіку за допомогою ланцюжків із проксі серверів не працював, оскільки в macOS є функція SIP.

Під час роботи бібліотекою Whereami мене зацікавило, як насправді працюють сервіси від Apple, пов'язані з виявленням місцезнаходження. Я знаю, що цей протокол зв'язаний locationd, оскільки в Little Snitch ця служба залишається заблокованою. Звичайний спосіб дослідження трафіку за допомогою ланцюжків із проксі серверів не працював, оскільки в macOS є функція SIP (System Integrity Protection; Захист цілісності системи).

Альтернативний шлях: установка Charles у якості проміжного проксі-сервера на iOS-пристрої. Після просікання трафіку, в основному пов'язаного з оповіщеннями великого брата (device phoning home), я одержав інформацію про запит служб, пов'язаних з визначенням місцезнаходженням.

Я думаю, що Apple вивантажує тристоронні виміри клієнтові. Замість ресурсомістких розрахунків вертається набір координат точок доступу.

Якщо як мінімум три точки доступу видні клієнтові, Фреймворк core location може використовувати рівень сигналу як відстань. Коли в нас є координати трьох точок доступу й відстань до мети, ми можемо розрахувати місцезнаходження мети із прийнятною точністю.

Якщо в нас є інформація про сотню точок доступу навколо, знижується необхідність у повторному з'єднанні із сервером служб, пов'язаних з місцезнаходженням. Оскільки в core location є координати трьох видимих точок доступу, можна обчислити місцезнаходження нашої точки. Подібні розрахунки можуть бути зроблені навіть оффлайн, оскільки Wi-Fi включений.

Як використовувати цю можливість?

Ви можете написати підтримку Core location на рівні користувача для тих мов програмування, де подібний функціонал відсутній. Хоча є більше прості способи вирішити те ж саме завдання.

Більше цікаве завдання – розгорнути свій власний сервер служб, пов'язаних з місцем розташування з метою полегшення налагодження додатків.

Індустрія GPS-трекінгу стрімко розвивається завдяки технологічному прогресу та зростаючому попиту на більш ефективні та безпечні рішення для відстеження. З наближенням 2025 року захопливі тенденції революціонізують використання систем GPS-

трекінгу окремими особами та підприємствами. Від штучного інтелекту до інтеграції Інтернету речей, ці інновації підвищують точність, зв'язок та функціональність.

У цьому розділі ми розглянемо провідні тенденції GPS-відстеження.

Найпопулярніші тенденції GPS-відстеження, за якими варто стежити у 2025 році.

1) Інтеграція штучного інтелекту (ШІ)

Штучний інтелект покращить системи GPS, аналізуючи великі обсяги даних відстеження для прогнозування закономірностей, оптимізації маршрутів та покращення прийняття рішень. Приклад: треки на базі штучного інтелекту можуть пропонувати найефективніший маршрут з точки зору витрати палива на основі дорожнього руху та погодних умов.

2) Підключення до Інтернету речей (IoT)

Інтеграція Інтернету речей дозволить GPS-пристроєм підключатися до інших розумних пристроїв, створюючи мережу взаємопов'язаних систем. Приклад: GPS-трекер, підключений до діагностики автомобіля, може надсилати сповіщення про проблеми з технічним обслуговуванням, такі як низький тиск у шинах. GPS-пристрої на базі 5G розгортання мереж 5G значно покращить швидкість і точність відстеження в режимі реального часу. Перевага: Швидша передача даних дозволяє швидше відстежувати навіть у ситуаціях з високим навантаженням, таких як управління автопарком.

3) Покращений час роботи від батареї

Досягнення в технології акумуляторів призведуть до створення пристроїв з більшим терміном служби, що зменшить потребу в частій підзарядці або заміні. Приклад: Сонячні треки для дистанційного моніторингу активів у внутрішніх районах Гайани.

4) Посилена безпека даних

Зі зростанням занепокоєння щодо конфіденційності даних, системи GPS-стеження впроваджуватимуть сильніші протоколи шифрування та безпечні рішення для зберігання даних. Перевага: Користувачі можуть бути впевнені, що дані про їхнє місцезнаходження захищені від несанкціонованого доступу.

5) Інтеграція доповненої реальності (AR)

Доповнена реальність (AR) забезпечить інноваційні способи візуалізації даних відстеження, що полегшить користувачам взаємодію з картами та відстеження переміщень. Приклад: Менеджер автопарку використовує окуляри доповненої реальності, щоб бачити місцезнаходження всіх транспортних засобів у режимі реального часу на динамічній карті.

6) Екологічно чисті пристрої

7) Виробники зосередяться на створенні екологічно чистих трекерів з використанням матеріалів, що підлягають переробці, та енергоефективних компонентів.

8) Прогнозна аналітика

Треки використовуватимуть історичні дані для прогнозування майбутніх рухів, що дозволить підприємствам та приватним особам приймати проактивні рішення. Приклад: Прогнозування заторів та пропонування альтернативних маршрутів.

Розширення багатосузір'євих та багаточастотних GNSS-приймачів

У супутниковій навігації терміни GPS і GNSS часто вживаються тотожними, проте вони позначають різні системи. GPS, створена у США, є лише однією з багатьох супутникових навігаційних систем, тоді як GNSS охоплює кілька типів супутників, таких як GPS, Galileo, що забезпечує більш широке покриття та вищу точність.

Розширення використання багатосузір'євих та багаточастотних GNSS-приймачів є однією з найцікавіших тенденцій 2025 року. Ці приймачі можуть отримувати доступ до сигналів від різних глобальних супутникових систем, включаючи GPS, Galileo та BeiDou, значно підвищуючи точність та надійність. Ця технологія дозволяє вашим GNSS-системам отримувати дані позиціонування від ширшого масиву супутників, покращуючи доступність сигналу та зменшуючи ризик втрати сигналу або перешкод, особливо в міських каньйонах або віддалених районах.

Завдяки інтеграції кількох частот, ці приймачі також можуть фільтрувати поширені джерела перешкод, що ще більше покращує цілісність даних. Наприклад, двочастотні приймачі можуть отримувати доступ до частот L1 та L2, що дозволяє їм зменшити помилки, спричинені іоносферними збуреннями. Результатом є надійніше позиціонування, що має вирішальне значення в таких застосуваннях, як геодезія, точне землеробство та автономні транспортні засоби, де висока точність є важливою для успіху. З розвитком цієї технології ви помітите більшу гнучкість та кращу продуктивність навіть у складних умовах.

Інтеграція штучного інтелекту та машинного навчання

Штучний інтелект (ШІ) та машинне навчання (МН) все частіше інтегруються в технології GNSS, прокладаючи шлях для створення розумніших та адаптивніших систем. ШІ та МН можна використовувати для покращення обробки сигналів, що дозволяє приймачам GNSS ефективніше інтерпретувати дані із супутників у режимі реального часу. Це означає, що замість того, щоб покладатися лише на попередньо запрограмовані алгоритми, система може навчатися з навколишнього середовища та динамічно коригувати свою продуктивність.

Для автономних транспортних засобів, робототехніки та дронів ця можливість дозволяє системам GNSS адаптуватися до змінних умов у режимі реального часу. Чи то коригування перешкод сигналу, зміна рельєфу чи непередбачувані фактори навколишнього середовища, приймачі GNSS на базі штучного інтелекту можуть забезпечити оптимальну продуктивність вашої системи. Ці досягнення зроблять системи GNSS ще надійнішими та ефективнішими, допомагаючи таким галузям, як транспорт, логістика та геодезія, отримувати вигоду від безперебійної технології позиціонування в режимі реального часу, незалежно від перешкод.

Розробка стійких систем PNT

З розвитком технології GNSS зростає потреба в системах позиціонування, навігації та синхронізації (PNT), які можуть протистояти зовнішнім загрозам, таким як глушіння та спуфінг. Ці загрози можуть порушити точність та надійність сигналів GNSS, що робить надзвичайно важливим для галузей промисловості, особливо в оборонній, автономній та критично важливій інфраструктурі, впровадження більш стійких систем PNT.

Щоб усунути ці вразливості, у приймачі GNSS інтегруються вдосконалені технології шифрування сигналів, протоколи безпечного зв'язку та вдосконалена корекція помилок. Це гарантує, що навіть у середовищах з високим ризиком перешкод ваші системи зможуть підтримувати цілісність даних позиціонування. Розробка цих стійких систем особливо важлива для таких секторів, як автономні транспортні засоби та дослідження космосу, де безперебійні та точні дані є важливими для безпеки та успіху місій. Випереджаючи ці інновації, ви можете забезпечити безпеку та надійність вашого обладнання GNSS, незалежно від зовнішніх загроз.

Мініатюризація та низьке енергоспоживання

Тенденція до мініатюризації та низького енергоспоживання в технології GNSS є ще одним важливим досягненням на 2025 рік. Оскільки пристрої стають більш компактними та портативними, зростає попит на GNSS-приймачі, які забезпечують високу точність без шкоди для енергоефективності чи розміру. Це особливо актуально для зростаючого ринку Інтернету речей (IoT), носимих та мобільних пристроїв, де простір та час роботи від батареї часто обмежені.

Ці менші, малопотужні приймачі GNSS все ще можуть досягати високого рівня точності, що дозволяє використовувати їх у таких сферах застосування, як пристрої відстеження, моніторинг навколишнього середовища та портативні геодезичні інструменти. Завдяки покращеному терміну служби батареї та можливостям обробки, ці пристрої дозволяють працювати протягом тривалішого часу без частого перезарядження або громіздкого обладнання. Це значний крок вперед у доступності технології GNSS для ширшого кола галузей та варіантів використання, особливо в мобільних або віддалених сценаріях. Впроваджуючи ці досягнення, ви можете скористатися перевагами високопродуктивної технології GNSS у більш зручному та екологічному форм-факторі.

Інтеграція з мережами 5G

Однією з ключових тенденцій технології GNSS у 2025 році є її інтеграція з мережами 5G. У міру поширення технології 5G у всьому світі, синергія між GNSS та 5G розширить можливості позиціонування, особливо в міських умовах, де супутникові сигнали часто перешкоджають. 5G забезпечить швидшу та надійнішу мережу зв'язку, яка зможе працювати разом із системами GNSS, пропонуючи точні послуги на основі місцезнаходження з меншою затримкою.

Для таких галузей, як логістика, автономні транспортні засоби та розумні міста, ця інтеграція призведе до покращення навігації в режимі реального часу, управління дорожнім рухом та моніторингу інфраструктури. Дані GNSS у поєднанні з підключенням 5G можуть забезпечити безперебійне відстеження транспортних засобів, людей та активів, що дозволить швидше приймати рішення та ефективніше працювати. Завдяки широкій пропускну здатності 5G та низькій затримці передачі, приймачі GNSS можуть передавати дані про місцезнаходження з мінімальною затримкою, забезпечуючи безперебійну роботу програм, що залежать від позиціонування в режимі реального часу, навіть у щільних міських районах або складних умовах.

Досягнення у високоточній GNSS для комерційного використання

Високоточні приймачі GNSS стають більш доступними для комерційного використання у 2025 році, забезпечуючи промисловість доступними та надійними рішеннями для таких застосувань, як геодезія, сільське господарство, будівництво та картографування. Інтеграція передових методів корекції, таких як RTK (кінематика в реальному часі) та PPP (точне позиціонування точок), допомагає комерційним користувачам досягати точності на сантиметровому рівні без необхідності використання дорогого обладнання або складних налаштувань.

Для таких секторів, як сільське господарство, це означає можливість впроваджувати методи точного землеробства, які підвищують врожайність сільськогосподарських культур і зменшують відходи. У будівництві високоточні GNSS забезпечують точність вимірювань на місці, зменшуючи ризик помилок і дорогої переробки. Зростаюча доступність цих технологій дозволяє компаніям будь-якого розміру скористатися точністю, яка колись була зарезервована для спеціалізованих застосувань, роблячи GNSS більш невід'ємною частиною повсякденних комерційних робочих процесів. Використовуючи ці досягнення, ви можете покращити якість та ефективність своїх проєктів, зрештою заощаджуючи як час, так і ресурси.

Розширення застосування GNSS у космічних дослідженнях

З розвитком технології GNSS її використання починає поширюватися за межі Землі, зі зростанням застосування в дослідженнях космосу. Приймачі GNSS зараз адаптуються для використання в місячних місіях, супутникових операціях та інших космічних програмах. Ці досягнення забезпечують точнішу та автономнішу навігацію космічних апаратів, зменшуючи залежність від наземних систем стеження.

Наприклад, системи на основі GNSS інтегруються в космічні кораблі для забезпечення точного позиціонування під час міжпланетних подорожей. У найближчі роки ми можемо очікувати використання GNSS-приймачів у місіях на дослідження Місяця та Марса, підтримуючи автономні марсоходи та інші транспортні засоби. Ці системи матимуть вирішальне значення для точної посадки, навігації та зв'язку в космосі, виводячи технологію GNSS на нові висоти. Зі зростанням космічної галузі технологія GNSS відіграватиме вирішальну роль у забезпеченні безпечнішої та ефективнішої роботи за межами орбіти Землі.

У 2025 році системи GPS-стеження вже не призначені лише для менеджерів автопарку чи шпигунських фільмів; тепер вони є важливими інструментами для щоденної безпеки, розумнішої логістики та контролю в режимі реального часу. Завдяки досягненням у сфері штучного інтелекту, 5G та супутникових технологій, ці трекери стали точнішими, доступнішими та зручнішими у використанні, ніж будь-коли.

Система GPS-стеження – це пристрій або програмне забезпечення, яке дозволяє вам контролювати місцезнаходження транспортних засобів, людей або активів у режимі реального часу за допомогою глобальних супутникових мереж. Незалежно від того, чи ви відстежуєте автомобіль, керуєте автопарком доставки чи стежите за близькими, технологія GPS відіграє життєво важливу роль.

У цій статті ви дізнаєтеся, що таке система GPS-стеження, як працює GPS-стеження та чому воно важливе у 2025 році, на які нові функції варто звернути увагу, хто їх використовує та чому вони стали таким революційним інструментом у сфері особистої та бізнес-безпеки.

Ключові висновки:

- Системи GPS-стеження використовують супутники та мережі для моніторингу місцезнаходження в режимі реального часу.

- У 2025 році GPS-трекери стали розумнішими, швидшими та доступнішими, ніж будь-коли.

- Сповіщення на основі штучного інтелекту, геозонування та інтеграція додатків тепер є стандартними функціями.

- GPS використовується в особистих, бізнес- та логістичних програмах.

- Для законного використання потрібне право власності або згода – закони про конфіденційність все ще застосовуються.

- Вибір правильного трекера залежить від того, що і кого ви відстежуєте.

- Зростає попит на екологічно чисті GPS-пристрої, що працюють на сонячних батареях, та GPS-навігатори.

- Сумісність з мобільними пристроями та комп'ютерами забезпечує легкий доступ до GPS-відстеження в будь-який час.

Система GPS-трекінгу – це технологія, яка використовує супутники для визначення та моніторингу місцезнаходження людини, транспортного засобу або активу в режимі реального часу в будь-якій точці Землі.

Він працює, підключаючись до мережі GPS-супутників, які надсилають сигнали на пристрій відстеження. Потім цей пристрій передає дані про місцезнаходження, часто використовуючи стільникові мережі або мережі Wi-Fi, на мобільний додаток або веб-платформу, де користувачі можуть переглядати поточне місцезнаходження, історію маршруту та сповіщення про рух.

Існують різні типи систем GPS-трекінгу залежно від їхнього призначення. Наприклад:

- Персональні трекери використовуються для дітей, людей похилого віку або самотніх працівників.

- Трекери для транспортних засобів допомагають власникам автомобілів або операторам автопарків контролювати водіння та запобігати крадіжкам.

- Системи відстеження активів призначені для цінного обладнання, причепів або посилок під час перевезення.

Сучасні системи GPS-стеження 2025 року поєднують супутникове позиціонування з передовими мобільними мережами та інтелектуальними технологіями, щоб надавати швидші та надійніші дані про місцезнаходження, ніж будь-коли раніше.

Сучасні трекери використовують як супутникові сигнали, так і стільникові мережі (4G/5G) для оновлення місцезнаходження в режимі реального часу. Таке подвійне з'єднання забезпечує плавніше відстеження навіть у віддалених районах, густонаселених містах або під час швидкого руху.

Щойно трекер збере дані про місцезнаходження, він надсилає їх у мобільний додаток або хмарну панель керування, дозволяючи користувачам бачити рух, швидкість, зупинки та історію маршрутів – і все це зі свого телефону або комп'ютера.

Завдяки інтеграції Інтернету речей та штучного інтелекту, GPS-трекери тепер можуть виявляти закономірності, запускати інтелектуальні сповіщення (наприклад, про небезпечне водіння або незвичайний рух) та оптимізувати використання акумулятора. Порівняно з 2020 роком, сучасні системи пропонують:

- Швидше фіксування GPS.
- Ширше покриття завдяки глобальним SIM-карткам.
- Довший час роботи від батареї.
- Розумніші сповіщення завдяки штучному інтелекту.

Вибір правильної системи GPS-трекінгу у 2025 році означає знання того, які функції дійсно мають значення у щоденному використанні. Нижче наведено основні функції, на які слід звернути увагу, незалежно від того, чи купуєте ви для особистої безпеки, чи для ведення бізнесу:

– Відстеження в режимі реального часу: отримуйте оновлення місцезнаходження з точністю до секунди, щоб ви завжди знали, де знаходиться ваш автомобіль, близька людина або майно.

– Сповіщення про геозони: встановлюйте власні зони на карті та отримуйте миттєві сповіщення, коли трекер входить у ці зони або виходить з них, що ідеально підходить для безпеки або водіння підлітками.

– Відтворення історії маршруту: переглядайте минулі маршрути руху, швидкості та час зупинок, щоб проаналізувати поведінку водія або перевірити активність.

– Варіанти батареї та живлення: Вибирайте з довговічних акумуляторних батарей, сонячної зарядки або дротових налаштувань залежно від ваших потреб відстеження.

– Сумісність із додатками та комп'ютерами: доступ до даних відстеження з мобільних додатків або веб-панелей керування, що безперешкодно синхронізуються на всіх пристроях.

– Екстрені сповіщення SOS: Деякі трекери мають кнопку SOS, яка надсилає миттєве сповіщення з місцезнаходженням у режимі реального часу контактам у разі надзвичайної ситуації.

– Водонепроникний та міцний дизайн: Міцний, захищений від атмосферних впливів трекер забезпечує надійну роботу в суворих умовах, будь то під автомобілем чи на вуличному обладнанні.

Ці основні функції не лише забезпечують щоденну зручність, але й підвищують безпеку, відповідальність та душевний спокій.

У 2025 році системи GPS-стеження важливіші, ніж будь-коли, не лише для відстеження місцезнаходження, але й для видимості в режимі реального часу, безпеки та прийняття більш розумних рішень у особистому та професійному житті.

Ось чому вони є критично важливими сьогодні, і хто отримує від цього найбільшу користь:

– Власники автомобілів: GPS-трекери діють як потужні засоби захисту від крадіжок та допомагають батькам контролювати водіння підлітків, забезпечуючи душевний спокій та швидше повернення автомобіля у разі викрадення.

– Автопарки для бізнесу: Для служб доставки, компаній з технічного обслуговування та транспортних компаній GPS-відстеження підвищує ефективність маршрутів, зменшує витрати палива та забезпечує відповідальність водіїв.

– Сім'ї та опікуни: Від дітей, які повертаються додому зі школи, до літніх членів сім'ї з проблемами пам'яті, GPS-пристрої забезпечують миттєве оновлення місцезнаходження та екстрені сповіщення, коли це найбільше потрібно.

– Логістика та оператори ланцюгів поставок: У галузях, де терміни та захист активів є критично важливими, GPS допомагає контролювати кожне відправлення та зменшує ризик втрати або затримки.

– Користувачі, орієнтовані на безпеку: Люди, які працюють у сфері високого ризику або проживають у нестабільних районах, використовують трекери для обміну місцезнаходженням у надзвичайних ситуаціях, сповіщень SOS та особистої безпеки.

Незалежно від того, чи ви турботливий батько, власник бізнесу чи автолюбитель, використання системи GPS-стеження пропонує реальні, вимірювані переваги у 2025 році. Ось як вона створює цінність:

– Спокій та безпека: Завжди знайте, де знаходиться ваш автомобіль, близька людина чи актив. Відстеження в режимі реального часу, сповіщення про геозони та функції SOS допомагають запобігти втраті, пошкодженню або крадіжці.

– Покращене управління транспортними засобами та активами: GPS-відстеження надає вам кращий контроль над вашими транспортними засобами та обладнанням. Ви можете відстежувати їх використання, виявляти несанкціоновану діяльність та планувати технічне обслуговування на основі фактичних даних про використання.

– Економія коштів: заощаджуйте гроші завдяки паливній ефективності, оптимізації маршрутів та зниженню страхових внесків. Багато страховиків зараз пропонують знижки на автомобілі, обладнані GPS. Відшкодування збитків після крадіжки також відбувається швидше та є більш імовірним, якщо встановити GPS.

– Підзвітність: Незалежно від того, чи це співробітники, які користуються службовими транспортними засобами, чи підлітки, які керують сімейним автомобілем, GPS створює прозорість та заохочує відповідальну поведінку.

– Дотримання законодавства: Для комерційних автопарків системи GPS допомагають виконувати вимоги ELD, відстежувати години роботи водія та інші нормативні вимоги, які відрізняються залежно від штату чи галузі.

На схемі представлена геопараметрична сітка з поточним місцем розташування об'єкта й система супутників, що забезпечує визначення місця розташування. При поганому зв'язку із супутниками (знаходження в приміщеннях) необхідно, принаймні 3 супутники, що знаходяться не на одній лінії для визначення поточного положення.

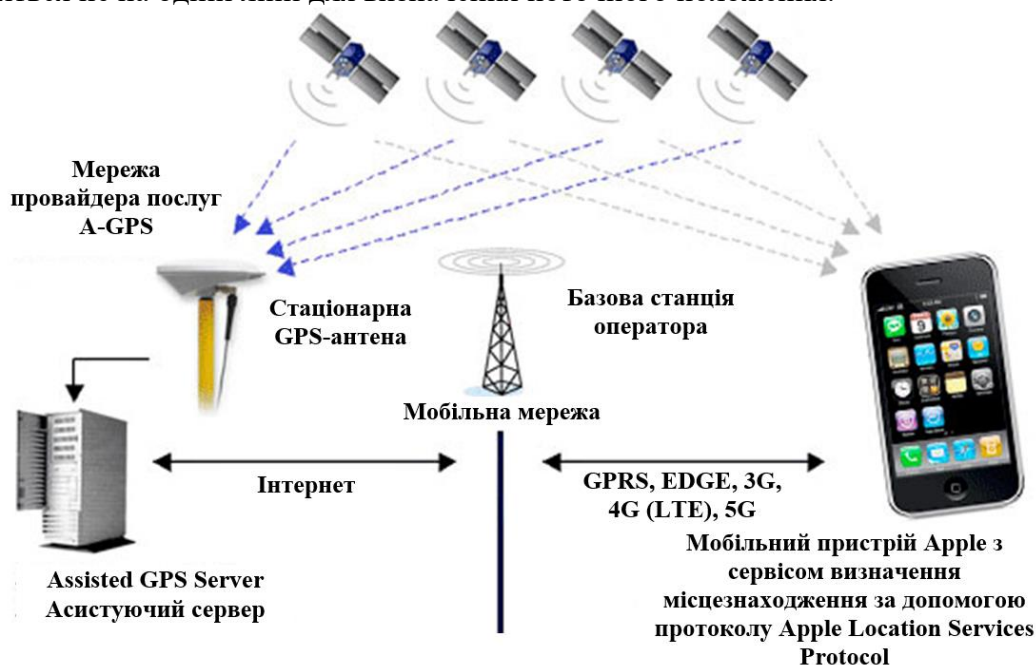


Рисунок 1 – Структурна схема роботи системи

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів визначення місцезнаходження за допомогою протоколу Apple Location Services Protocol. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем визначення місцезнаходження за допомогою протоколу Apple Location Services Protocol.
- Досліджена система визначення місцезнаходження за допомогою протоколу Apple Location Services Protocol.
- На основі отриманих результатів досліджень створена програмна реалізація системи визначення місцезнаходження за допомогою протоколу Apple Location Services Protocol. Розроблені алгоритми дозволяють успішно вирішувати завдання визначення місцезнаходження за допомогою протоколу Apple Location Services Protocol. 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. Malyukov V., Bebeshko 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.
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., 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. 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.
7. 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.
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. 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.
10. 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.
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., 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
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., 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., 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., 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.
 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., 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. 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.
 24. 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.
 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. 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.
 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., Дреєва Г.М., Дреєв О.М., Смірнова Т.В. «Фрактальний аналіз генератора самоподібного трафіку на основі ланцюга Маркова». Центральноукраїнський науковий вісник. Технічні науки. № 2(33). с. 161-172, 2019.
 30. 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).
 31. Смірнова Т.В., Солових Є.К., Смірнов О.А., Дреєв О.М. Побудова хмарних інформаційних технологій оптимізації технологічного процесу відновлення та зміцнення поверхонь деталей. Центральноукраїнський науковий вісник. Технічні науки. № 1(32). с. 184-194, 2019.
 32. Смірнов О.А., Котелянець В.В. Стійкі до колізій стохастичні моделі функціонування безпроводових сенсорних мереж. Вісник інженерної академії України, №3, с. 145-152, 2018

УДК 004

Д.Кашпуровський, магістр гр. КІ-24М,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ МЕРЕЖЕВОГО МОНІТОРИНГУ ТА КОНТРОЛЮ СТАНУ ІТ

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

мережевий моніторинг, контроль стану ІТ

Постановка проблеми. Інструменти моніторингу мережі – це програмні рішення для контролю, аналізу та управління продуктивністю та станом мережі. Ці інструменти постійно контролюють різні мережеві компоненти, такі як маршрутизатори, комутатори, сервери та програми, щоб забезпечити їх правильне функціонування.

Відстежуючи такі показники, як трафік, затримка та час безвідмовної роботи, вони допомагають ІТ-командам виявляти та вирішувати проблеми, перш ніж вони переростуть у серйозні проблеми. Основною метою інструментів моніторингу мережі є підтримка доступності, надійності та безпеки мережі. Вони забезпечують видимість мережевої активності, дозволяючи організаціям виявляти неефективність, збої або загрози безпеці.

Крім того, ці інструменти підтримують планування потужностей, оптимізацію продуктивності та дотримання угод про рівень обслуговування (SLA). Сучасні інструменти моніторингу мережі часто інтегрують такі функції, як аналітика в режимі реального часу, аналітика на основі штучного інтелекту та підтримка хмарної інфраструктури.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи мережевого моніторингу та контролю стану ІТ.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи мережевого моніторингу та контролю стану ІТ.

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

- Огляд існуючих систем мережевого моніторингу та контролю стану ІТ.
- Дослідження системи мережевого моніторингу та контролю стану ІТ.
- Програмна реалізація системи мережевого моніторингу та контролю стану ІТ.

Об'єктом дослідження є процес мережевого моніторингу та контролю стану ІТ.

Предметом дослідження є методи мережевого моніторингу та контролю стану ІТ.

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

Виклад основного матеріалу. Сформулюємо поради, які допоможуть вам вибрати, розгорнути та максимізувати цінність інструментів моніторингу мережі:

1. Пріоритет гібридної та багатохмарної сумісності: оскільки гібридні та багатохмарні середовища стають нормою, обирайте інструменти моніторингу, які пропонують безперешкодну інтеграцію з постачальниками публічних хмарних послуг (наприклад, AWS, Azure, Google Cloud) та інфраструктурою приватних хмар. Це забезпечує видимість на різних мережних рівнях.

2. Впроваджуйте поетапний підхід до розгортання: уникайте розгортання інструментів моніторингу по всій мережі одночасно. Натомість розгортайте рішення поетапно, починаючи з критичної інфраструктури, щоб мінімізувати перебої та точно налаштувати конфігурації під час масштабування.

3. Інтеграція з платформами SIEM та SOAR: підключіть інструменти моніторингу до рішень SIEM або SOAR для централізації аналізу даних, покращення виявлення загроз та забезпечення автоматизованих робочих процесів реагування на інциденти. Така інтеграція допомагає створити єдину екосистему безпеки.

4. Використовуйте виявлення аномалій на основі штучного інтелекту: використовуйте інструменти, що включають штучний інтелект та машинне навчання, для виявлення незначних відхилень від нормальної поведінки мережі. Такий підхід зменшує залежність від статичних порогів та покращує виявлення загроз нульового дня або повільних атак.

5. Встановлення базового профілю продуктивності: Проведення комплексного базового дослідження показників продуктивності мережі (наприклад, затримки, пропускну здатності та пропускну здатності) під час нормальної роботи. Це допоможе швидко виявити аномалії та оцінити майбутні покращення продуктивності.

Як вибрати правильний інструмент для моніторингу мережі

Ось деякі основні фактори, які слід враховувати під час оцінки рішень для моніторингу мережі.

Міркування щодо масштабованості

Зі зростанням організацій їхні мережі стають складнішими, що вимагає інструментів, здатних обробляти збільшений обсяг даних та складність мережі. Масштабоване рішення для моніторингу може враховувати додаткові пристрої, користувачів та робочі навантаження без шкоди для продуктивності чи точності.

Вибір інструменту з опціями масштабованості дозволяє організаціям адаптуватися до змінних вимог мережі. Інструменти, що пропонують механізми горизонтального та вертикального масштабування, забезпечують безперебійний моніторинг під час зростання мережі.

Можливості інтеграції

Сучасні IT-середовища часто включають різноманітні технології та системи. Інструмент, який добре інтегрується з іншими програмами та платформами, може забезпечити комплексне уявлення про стан та продуктивність мережі. Така інтеграція дозволяє автоматизувати робочі процеси та обмін даними.

Обираючи інструменти моніторингу з потужними функціями інтеграції, організації можуть спростити IT-операції та зменшити ручну роботу. Інтегровані системи забезпечують централізований моніторинг та управління, пропонуючи єдину платформу для всіх мережних дій.

Інтерфейс користувача та зручність використання

Інтерфейс користувача (UI) інструменту моніторингу мережі суттєво впливає на його зручність використання та ефективність. Добре розроблений інтерфейс дозволяє IT-фахівцям легко орієнтуватися в інструменті, налаштовувати конфігурації та інтерпретувати дані. Простота використання гарантує, що команди можуть швидко реагувати на проблеми та приймати обґрунтовані рішення на основі чіткої візуалізації продуктивності мережі.

Вибір інструменту з інтуїтивно зрозумілим інтерфейсом скорочує криву навчання та підвищує продуктивність. Зручні функції, такі як панелі інструментів з функцією перетягування елементів та автоматизована звітність, покращують впровадження та ефективність використання користувачами.

Моделі вартості та ліцензування

Організаціям необхідно враховувати початкові витрати, поточні платежі та потенційні приховані платежі. Моделі ліцензування різняться, включаючи варіанти на основі підписки, безстрокові або freemium, кожна з яких має свої власні витрати та переваги залежно від бюджету та потреб організації.

Оцінка загальної вартості володіння допомагає організаціям збалансувати бюджетні обмеження з вимогами до функціональності. Розуміння умов ліцензування та майбутніх витрат на масштабованість гарантує, що інвестиції задовольняють як поточні потреби, так і майбутнє зростання.

Інструменти моніторингу мережі є важливими для підтримки продуктивності, надійності та безпеки сучасних мереж. Вибираючи рішення, яке відповідає конкретним потребам організації, враховуючи такі фактори, як масштабованість, інтеграція, зручність використання та вартість, IT-команди можуть забезпечити оптимальну роботу мережі та проактивно вирішувати проблеми. Інвестування в правильний інструмент моніторингу не лише покращує стан мережі, але й підтримує безперервність бізнесу та операційну ефективність.

Моніторинг мережі включає спостереження та аналіз продуктивності та стану мережі за допомогою різних пристроїв та програмних інструментів. Цей процес спрямований на забезпечення безперебійної роботи мережевої інфраструктури шляхом відстеження потоків даних, станів пристроїв та потенційних несправностей, які можуть порушити роботу сервісу.

Мережеві адміністратори часто використовують ці дані для керування пропускнуою здатністю, виявлення аномалій та забезпечення проактивного обслуговування, зменшуючи час простою та пом'якшуючи ризики, пов'язані з проблемами мережі.

Інструменти моніторингу мережі збирають дані за допомогою таких протоколів, як SNMP (простий протокол керування мережею) та ICMP (протокол керування інтернет-повідомленнями), що дозволяє адміністраторам оцінювати стан мережі в режимі реального часу. Ці інструменти часто надають графічні інтерфейси, які відображають такі показники, як втрата пакетів, затримка та час безвідмовної роботи, що спрощує розуміння стану мережі.

Важливість моніторингу мережі

Існує кілька причин, чому організації повинні впроваджувати стратегії моніторингу мережі.

Раннє виявлення проблем з мережею

Раннє виявлення мережевих проблем передбачає постійне сканування мережевої активності для виявлення порушень. Ці порушення можуть включати незвичайні обсяги трафіку, неочікувані простої або несправності обладнання. Мережеві адміністратори можуть швидко втрутитися, виявивши ці проблеми на ранній стадії та усунувши першопричину, перш ніж вони порушать роботу мереж. Це заощаджує час і ресурси, необхідні для тривалого усунення несправностей.

Раннє виявлення може запобігти порушенням безпеки, виявляючи потенційні загрози в міру їх виникнення. Наприклад, раптові сплески передачі даних можуть свідчити про спроби несанкціонованого доступу або витоку даних. Завдяки сповіщенням та звітам у режимі реального часу системи моніторингу мережі можуть повідомляти адміністраторів про ці аномалії, що дозволяє швидко реагувати та негайно зменшувати ризики безпеки.

Забезпечення продуктивності та доступності мережі

Відстежуючи ключові показники продуктивності, такі як використання пропускнуої здатності та затримка, мережеві адміністратори можуть забезпечити ефективне використання ресурсів та уникнути потенційних вузьких місць. Постійний моніторинг надає уявлення про стан мережі, що дозволяє своєчасно оновлювати або перерозподіляти ресурси для підтримки зв'язку в організації.

Крім того, моніторинг мережі підтримує високу доступність, оперативно сповіщаючи команди про збої або погіршення стану мережевих компонентів. Ці сповіщення дозволяють швидко діяти, мінімізуючи час простою та підтримуючи доступність послуг.

Моніторинг відповідності та безпеки

Відповідність вимогам та безпека є важливими питаннями, на які звертають увагу системи моніторингу мережі. Ці системи відстежують журнали доступу, дії користувачів та передачу даних, забезпечуючи відповідність використання мережі нормативним стандартам та політикам організації. Моніторинг може допомогти виявити прогалини у відповідності, що дозволяє компаніям оперативно вживати коригувальних заходів, щоб уникнути штрафів.

Моніторинг безпеки зосереджений на виявленні та реагуванні на потенційні загрози, такі як несанкціонований доступ та проникнення шкідливого програмного забезпечення. Моніторинг мережі в режимі реального часу виявляє відхилення від встановлених норм безпеки, запускаючи сповіщення для негайного реагування. Це посилює захист організації від кіберзагроз, захищаючи конфіденційні дані.

Ключові компоненти систем мережевого моніторингу**Методи збору даних**

Збір даних включає збір інформації про мережевий трафік, стан пристроїв та показники продуктивності. Традиційні методи включають SNMP, який збирає та впорядковує дані про мережеві пристрої, та ICMP-зонди, які вимірюють час підключення та відгуку. Ці інструменти працюють разом, щоб створити детальний огляд мережі, допомагаючи адміністраторам приймати обґрунтовані рішення щодо оптимізації продуктивності або усунення несправностей.

Методи збору даних також використовують технології на основі потоків, такі як NetFlow та sFlow, які пропонують детальну видимість моделей мережевого трафіку та використання пропускної здатності. Ці методи надають безцінну інформацію про продуктивність програм та поведінку користувачів, допомагаючи виявляти вузькі місця або несанкціоноване використання даних.

Топологія та відображення мережі

Топологія мережі та картографування є критично важливими компонентами мережевого моніторингу, що забезпечують візуальне уявлення про те, як пристрої та з'єднання організовані в мережі. Таке графічне зображення дозволяє мережевим адміністраторам краще зрозуміти, як трафік передається між пристроями, виявляти потенційні точки збою та оцінювати вплив перебоїв у роботі мережі.

Точне картографування топології допомагає ефективно виявляти несправності та оптимізувати мережеві шляхи. Інструменти картографування мережі автоматично виявляють та документують зміни в мережевому середовищі, підтримуючи актуальність топологічних представлень. У міру розвитку мереж з появою нових пристроїв та технологій динамічне картографування підтримує інтеграцію та прозорість.

Механізми оповіщення та звітності

Механізми сповіщень та звітності є незамінними для моніторингу мережі, надаючи сповіщення про аномалії або збої в режимі реального часу. Сповіщення налаштовуються на спрацьовування за певних порогових значень, таких як збільшення затримки або відключення пристроїв. Коли ці умови виконуються, сповіщення надсилаються адміністраторам мережі, що спонукає до негайного розслідування та вирішення проблеми.

Функції звітності доповнюють системи сповіщень, надаючи інформацію про довгострокові тенденції та показники ефективності. Регулярно генеровані звіти допомагають виявити закономірності, які можуть свідчити про основні проблеми або можливості для оптимізації. Вони також підтримують дотримання вимог, документуючи мережеву активність та демонструючи дотримання нормативних стандартів.

Сформулюємо поради, які допоможуть вам оптимізувати стратегії моніторингу мережі для підвищення продуктивності та безпеки:

1. Використовуйте штучний інтелект та машинне навчання для прогнозу аналітики: використовуйте інструменти моніторингу на базі штучного інтелекту для аналізу історичних даних та прогнозування потенційних збоїв або вузьких місць. Такий підхід допомагає вирішувати проблеми до того, як вони вплинуть на продуктивність мережі.

2. Сегментація мереж для покращення видимості: розділіть мережу на логічні сегменти (наприклад, за відділами чи програмами), щоб зосередити зусилля моніторингу та швидше виявляти проблеми. Сегментація також підвищує безпеку, обмежуючи обсяг потенційних загроз.

3. Використовуйте моніторинг на основі потоку разом із традиційними метриками: інтегруйте такі інструменти, як NetFlow або sFlow, для аналізу потоків трафіку для глибшого розуміння використання пропускної здатності, продуктивності програм та аномальної поведінки. Це доповнює моніторинг на основі SNMP для отримання більш повного уявлення.

4. Впроваджуйте порогові значення для сповіщень на основі часу: встановлюйте динамічні порогові значення для показників продуктивності на основі тенденцій часу доби. Наприклад, налаштуйте вищі порогові значення пропускної здатності в години пікової зайнятості, щоб зменшити кількість хибних спрацьовувань та зосередитися на справді аномальній активності.

5. Поєднання локальних та хмарних інструментів моніторингу: використовуйте гібридні рішення для отримання видимості в традиційних та хмарних інфраструктурах. Інструменти, що інтегруються в різних середовищах, є важливими для моніторингу гібридних або багатохмарних мереж.

Метрики та протоколи моніторингу мережі

Загальні показники, що відстежуються

Ефективний моніторинг мережі залежить від відстеження показників, які показують стан, продуктивність та надійність мережі. Зазвичай моніторингові показники включають:

1. Використання пропускної здатності: Цей показник показує, яка частина доступної пропускної здатності мережі використовується в певний момент часу. Високий рівень використання може свідчити про перевантаження мережі, що вимагає перерозподілу ресурсів або оновлення.

2. Затримка: Затримка вимірює час, необхідний для передачі даних від джерела до місця призначення і назад. Висока затримка впливає на програми реального часу, такі як VoIP та відеоконференції, що вимагає своєчасного втручання для покращення взаємодії з користувачем.

3. Втрата пакетів: Втрата пакетів – це відсоток пакетів даних, які не досягають місця призначення. Навіть невелика кількість втрачених пакетів може порушити роботу програм, чутливих до доставки даних, таких як потокове передавання або онлайн-ігри.

4. Час безперебійної роботи та простої: Моніторинг часу безперебійної роботи пристроїв та послуг дає уявлення про надійність мережевих компонентів. Часті або тривалі простої можуть сигналізувати про несправне обладнання, неправильні конфігурації програмного забезпечення або ширші проблеми з інфраструктурою.

5. Коефіцієнт помилок: Цей показник відстежує кількість помилок у переданих даних, таких як колізії, втрачені пакети або повторні передачі. Високий коефіцієнт помилок часто вказує на такі проблеми, як збій обладнання або погане кабельне з'єднання.

6. Пропускна здатність: Пропускна здатність вимірює фактичну швидкість передачі даних по мережі. Розбіжності між пропускною здатністю та використанням пропускної здатності можуть сигналізувати про проблеми з продуктивністю, такі як вузькі місця або перешкоди.

7. Джиттер: Джиттер стосується варіації часу доставки пакетів. Цей показник особливо важливий для програм реального часу, оскільки надмірний джиттер може призвести до погіршення якості голосового та відеозв'язку.

8. Використання процесора та пам'яті на пристроях: моніторинг використання ресурсів на мережевих пристроях, таких як маршрутизатори, комутатори та сервери, допомагає запобігти зниженню продуктивності через перевантажене обладнання.

9. Стан з'єднання: Регулярна перевірка стану з'єднань між пристроями забезпечує працездатність усіх компонентів. Швидке виявлення несправних з'єднань мінімізує перебої в обслуговуванні.

SNMP (Простий протокол керування мережею)

SNMP – це критично важливий протокол для моніторингу мережі, який дозволяє збирати та керувати мережевими даними на різних пристроях. Він працює шляхом запиту інформації до пристроїв, такої як показники продуктивності та сповіщення, що забезпечує централізоване управління мережею. Завдяки широкому розповсюдженню та сумісності з багатьма пристроями, SNMP допомагає в зусиллях з моніторингу.

Архітектура SNMP, що складається з агентів, менеджерів та баз управлінської інформації (MIB), формує структурований підхід до пошуку та управління даними. Агенти SNMP працюють на мережових пристроях, звітуючи перед менеджерами SNMP, які обробляють та аналізують дані. MIB визначають структуру даних, забезпечуючи стандарти щодо того, яка інформація доступна та як до неї здійснюється доступ.

NetFlow та sFlow

NetFlow та sFlow – це технології, що використовуються для забезпечення видимості мережі та аналізу трафіку шляхом захоплення потоків пакетів. NetFlow, розроблений Cisco, збирає дані IP-трафіку та надає інформацію про джерело, пункт призначення, обсяг та шляхи, що проходять мережею. Така видимість дозволяє проводити поглиблений аналіз трафіку, виявляти тенденції, моделі використання та аномалії.

sFlow – це технологія вибірки пакетів, яка забезпечує статистичне представлення даних, що проходять мережею. Вона ефективна для моніторингу високошвидкісних мереж, де захоплення всіх пакетів може бути неможливим. sFlow пропонує аналітику трафіку як другого, так і третього рівня, що робить її універсальною для моніторингу мережі.

ICMP (Протокол керування інтернет-повідомленнями)

ICMP допомагає в діагностиці та моніторингу мережі, надаючи зворотний зв'язок про проблеми, пов'язані з підключенням. Він в основному використовується для звітування про помилки, що дозволяє обмінюватися повідомленнями між пристроями, щоб вказати на проблеми з підключенням до мережі, такі як недоступні пункти призначення. Утиліти, такі як «ping» та «traceroute», покладаються на ICMP для перевірки доступності хоста та трасування мережових шляхів.

Незважаючи на свою корисність, ICMP також може становити ризики для безпеки, якщо його використовувати для атак типу «відмова в обслуговуванні» або мережової розвідки. Тому, хоча ICMP є невід'ємною частиною моніторингу продуктивності, його використання в мережах має бути ретельно керованим та захищеним.

Типи мереж та пристроїв, що контролюються

Маршрутизатори, комутатори та концентратори

Маршрутизатори, комутатори та концентратори – це основні мережові пристрої, що забезпечують передачу даних. Маршрутизатори керують трафіком між різними мережами, що необхідно для підключення локальних мереж до Інтернету. Моніторинг маршрутизаторів забезпечує усунення потенційних вузьких місць та оптимізацію шляхів маршрутизації для ефективного потоку трафіку. Це включає відстеження таких показників, як пропускна здатність, затримка та коефіцієнт помилок, для підтримки зв'язку та продуктивності.

Комутатори забезпечують зв'язок у мережі, спрямовуючи дані на певні пристрої, забезпечуючи ефективний розподіл даних. Моніторинг комутаторів допомагає визначити стан портів, використання пропускної здатності та рівень колізій, щоб запобігти зниженню продуктивності. Концентратори, хоча й простіші за функціями, діють як основні з'єднувачі в мережах. Їх моніторинг є важливим для виявлення потенційних несправностей, що впливають на сегменти мережі.

Брандмауери та пристрої безпеки

Пристрої мережевої безпеки, включаючи брандмауери, утворюють критично важливий захист від кіберзагроз та несанкціонованого доступу. Моніторинг цих пристроїв гарантує їх ефективне функціонування у забезпеченні дотримання політик та блокуванні шкідливого трафіку. Ключові показники, такі як спроби атак, порушення доступу та моделі трафіку, ретельно перевіряються для швидкого виявлення інцидентів безпеки та реагування на них.

Крім того, рішення для моніторингу забезпечують дотримання вимог, реєструючи спроби доступу та зміни конфігурації на пристроях безпеки. Такий рівень видимості допомагає проводити судово-медичний аналіз після порушення безпеки, швидко виявляючи скомпрометовані системи або порушення політик.

Сервери та віртуальні машини

Моніторинг серверів і віртуальних машин допомагає підтримувати безперервність та продуктивність обслуговування. На серверах розміщено програми та дані, життєво важливі для бізнес-функцій, що вимагає ретельного моніторингу використання процесора, споживання пам'яті та обсягу дискового вводу/виводу. Ці показники виявляють потенційне перевикористання або збої обладнання, що допомагає своєчасно вживати заходів з технічного обслуговування, щоб запобігти незапланованим простоям.

Віртуальні машини потребують особливого моніторингу через свою масштабованість та тимчасовість. Такі показники, як розподіл ресурсів, завантаження віртуального процесора та використання мережі, стають критично важливими для оптимізації віртуального середовища. Забезпечуючи ефективний моніторинг віртуальних активів, організації можуть динамічно адаптувати ресурси відповідно до потреб.

Хмарна інфраструктура та послуги

Завдяки своїй розподіленій та масштабованій інфраструктурі, хмарні сервіси потребують рішень для моніторингу, які забезпечують видимість розподілу ресурсів, доступності та продуктивності в кількох регіонах. Ключові показники, такі як час відгуку, час безвідмовної роботи сервісу та журнали доступу, є вирішальними для забезпечення надійної роботи та безпеки хмарного середовища.

Моніторинг хмарних сервісів також дозволяє проактивно керувати ресурсами, забезпечуючи масштабування віртуальних екземплярів під час пікових навантажень без погіршення продуктивності. Крім того, моніторинг підтримує управління витратами, виявляючи недостатньо використані ресурси або непотрібні витрати.

Дротові та бездротові мережі

Дротові мережі вимагають моніторингу таких компонентів, як комутатори Ethernet та кабелі, зосереджуючись на цілісності з'єднання та пропускній здатності для запобігання перебоям. Бездротові мережі пов'язані з унікальними проблемами, такими як перешкоди сигналу, перевантаження каналів та оцінка зони покриття. Моніторинг цих аспектів має вирішальне значення для підтримки продуктивності бездротового зв'язку.

Моніторинг бездротової мережі збирає дані про пристрої користувачів і точки доступу, допомагаючи виявляти проблеми з підключенням або спроби несанкціонованого доступу. Аналізуючи силу сигналу та швидкість передачі даних, адміністратори можуть оптимізувати конфігурації бездротової мережі для покращення покриття та зручності використання.

Проблеми моніторингу мережі

Організації повинні знати про фактори, що ускладнюють моніторинг мережі.

Моніторинг у гібридних та багатохмарних середовищах

Гібридні та мультихмарні середовища вносять багаторівневу складність у моніторинг мережі, вимагаючи рішень, що відповідають різноманітним проблемам інфраструктури та інтеграції. Ці середовища охоплюють приватні та публічні хмарні екземпляри, а також локальні системи, що вимагає інструментів, здатних забезпечувати узгоджені дані про продуктивність усіх компонентів.

Динамічна природа хмарних середовищ означає, що рішення для моніторингу повинні адаптуватися до швидкого масштабування та змін, не порушуючи видимість. Це вимагає гнучких архітектур та функцій автоматизованого виявлення, щоб йти в ногу з розвитком інфраструктури.

Обробка великих обсягів даних

Величезний обсяг даних, що генеруються в сучасних мережах, може бути приголомшливим, що створює значні труднощі для систем моніторингу, які відповідають за обробку та аналіз цієї інформації. Ефективне управління та фільтрація величезних потоків даних є важливими для отримання корисної інформації без перевантаження системних ресурсів.

Забезпечення цілісності та точності даних має вирішальне значення для надійних результатів моніторингу. Неточні або неповні дані перешкоджають прийняттю рішень, що призводить до неправильних діагнозів або пропущених сповіщень.

Забезпечення безпеки мережі та відповідності вимогам

Ефективний моніторинг вимагає стратегій впровадження, які забезпечують дотримання політик безпеки та захищають дані під час передачі та зберігання. Розширене шифрування та засоби контролю доступу необхідні для захисту процесів моніторингу та забезпечення дотримання таких норм, як GDPR та HIPAA.

Також важливо мати записи, які підтверджують дотримання стандартів безпеки та нормативних вимог, що підтримують процеси аудиту.

Практики для ефективного моніторингу мережі

Ось деякі способи, за допомогою яких організації можуть забезпечити ефективний моніторинг своїх мереж.

1. Визначте чіткі цілі моніторингу

Цілі можуть бути зосереджені на підтримці безперебійної роботи, своєчасному виявленні аномалій або оптимізації використання ресурсів. Встановлюючи точні цілі, організації можуть адаптувати свої стратегії моніторингу для отримання змістовної аналітики та підтримки прийняття стратегічних рішень.

Така чіткість також забезпечує ефективний розподіл ресурсів і допомагає встановити реалістичні показники та контрольні показники ефективності. Завдяки чітко визначеним цілям моніторингу команди можуть визначити пріоритети ключових видів діяльності та розробити цільові плани дій.

2. Регулярно оновлюйте мережеву документацію

Постійне оновлення мережевої документації гарантує точне відображення всіх змін в інфраструктурі, що сприяє ефективному моніторингу та втручанню. Документація повинна детально описувати топологію, конфігурації пристроїв та залежності, надаючи довідник адміністраторам, які керують мережею. Регулярні оновлення дозволяють точно відстежувати активи, зміни конфігурації та зростання мережі з часом.

Вичерпна документація допомагає у вирішенні проблем, швидко виявляючи уражені ділянки під час інцидентів. Вона також підтримує зусилля з дотримання вимог, підтверджуючи дотримання політик і процедур безпеки.

3. Впроваджуйте проактивне оповіщення та реагування на інциденти

Проактивне оповіщення та реагування на інциденти дозволяють швидко діяти, коли виникають проблеми з продуктивністю або загрози безпеці. Налаштування порогів оповіщень на основі тенденцій історичних даних дозволяє адміністраторам виявляти аномалії до того, як вони переростуть у серйозні проблеми. Ці оповіщення підтримують гнучке реагування на інциденти, надаючи практичну інформацію, яка спрямовує цілеспрямовані зусилля з усунення наслідків.

Протоколи реагування на інциденти доповнюють проактивне оповіщення, детально описуючи кроки для діагностики, ескалації та вирішення. Ці протоколи гарантують оперативне вирішення проблем, мінімізуючи час простою та вплив на операції.

4. Виконуйте планові оцінки та аудити мережі

Регулярні оцінки та аудити мережі надають уявлення про продуктивність мережі та стан безпеки. Ці оцінки визначають області для покращення, виявляючи вразливості або неефективність, які можуть перешкоджати роботі. Аудити систематично перевіряють конфігурації мережі, політики та процедури, забезпечуючи відповідність передовим практикам та нормативним вимогам.

Регулярні оцінювання також допомагають вимірювати успішність стратегій моніторингу, що дозволяє постійно вдосконалювати інструменти та процеси.

5. Навчіть персонал інструментам та процедурам моніторингу

Навчання персоналу використанню інструментів та процедур моніторингу мережі має вирішальне значення для максимального використання можливостей систем моніторингу. Добре навчені команди можуть точно інтерпретувати дані, розпізнавати аномалії та вживати обґрунтованих заходів для оперативного вирішення проблем. Регулярне навчання гарантує, що персонал завжди в курсі нових функцій та методологій моніторингу.

Навчання також заохочує спільну роботу між ІТ-командами, сприяючи спільному розумінню цілей та практик моніторингу. Це покращує комунікацію та координацію під час реагування на інциденти, сприяючи більш ефективним та результативним процесам вирішення проблем.

На рисунку 1 зображена структурна схема системи.

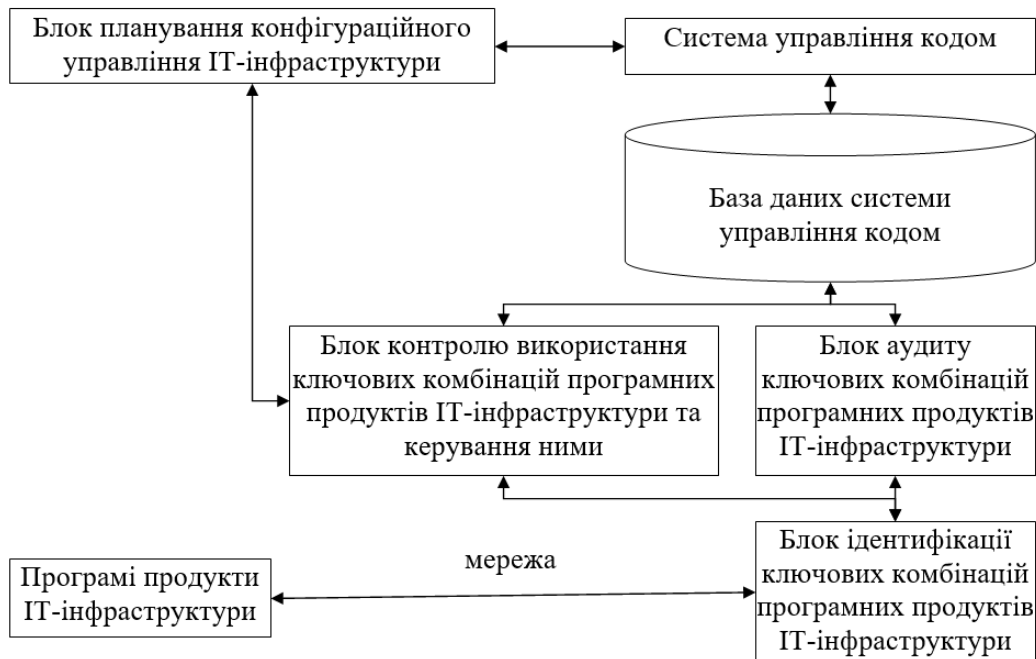


Рисунок 1 – Структурна схема системи

Зі структурної схеми видно, що система керування кодом підтримує програмні бібліотеки контролюючи доступ до елементів бібліотек, координує дії безлічі користувачів і допомагає в проведенні робочих процедур. Інші інструменти підтримують процес складання й випуску програмного забезпечення й документації на основі програмних елементів, що втримуються в бібліотеках. Інструменти для керування запитами на зміни програмного забезпечення використовуються для контрольованих системою конфігураційного керування програмних елементів. Інші інструменти можуть забезпечувати керування базою даних і необхідними менеджменту звітними засобами, а також діяльністю по розробці й забезпеченню якості.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів мережевого моніторингу та контролю стану ІТ. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем мережевого моніторингу та контролю стану ІТ.
- Досліджена система мережевого моніторингу та контролю стану ІТ.
- На основі отриманих результатів досліджень створена програмна реалізація системи мережевого моніторингу та контролю стану ІТ. Розроблені алгоритми дозволяють успішно вирішувати завдання мережевого моніторингу та контролю стану ІТ. 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. 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.
5. 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.
6. 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.
7. 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.
8. 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.
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. 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.
12. 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.
13. Akhalaia, G., Iavich, M., Iashvili, G., Prysiazhnyy, D., Smirnova, T. «Secure Encrypted Connection on Georgian Website». *CEUR Workshop Proceedings*, 2023, 3550, pp. 313-320.
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. 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.
16. 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.
17. Smirnov, O., Lakhno, V., Akhmetov, B., Chubaievskiy, V., Khorolska, K., Bebashko, 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. 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.
 19. 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 (ПШПІТ-2023)» м.Черкаси 6 грудня 2023 року – Черкаси: ЧДТУ.– 2023. – С.251-252.
 20. 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.
 21. 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.
 22. 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.
 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.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.
 25. 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.
 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. 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
 30. 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.
 31. 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.
 32. 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.

УДК 004

І.Кіблик, магістр гр. КІ-24М,

Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ ТА АУДИТУ ДІЙ ПРИ РОБОТІ З МЕРЕЖЕВОЮ БАЗОЮ ДАНИХ

У статті розроблено програмне забезпечення, яке призначено для системи контролю доступу та аудиту дій при роботі з мережевою базою даних. Метою розробки є дослідження та принципи побудови системи контролю доступу та аудиту дій при роботі з мережевою базою даних. Об'єктом дослідження є процес контролю доступу та аудиту дій при роботі з мережевою базою даних. Предметом дослідження є методи контролю доступу та аудиту дій при роботі з мережевою базою даних. Методи дослідження базуються на методах побудови баз даних та захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи контролю доступу та аудиту дій при роботі з мережевою базою даних. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

система контролю доступу, аудит дій, мережева база даних

Постановка проблеми. Контроль доступу до бази даних, або контроль доступу до БД – це метод, що дозволяє доступ до конфіденційної інформації компанії лише групам користувачів, яким дозволено доступ до таких даних, та обмежує доступ неавторизованим особам для запобігання витокам даних у системах баз даних. Контроль доступу до бази даних у СУБД включає два основні компоненти: автентифікацію та авторизацію.

Автентифікація – це спосіб підтвердження особи особи під час доступу до вашої бази даних. Важливо пам'ятати, що автентифікації користувача недостатньо для забезпечення безпеки даних. Авторизація, яка встановлює, чи є рівень доступу користувача або контроль доступу до даних відповідним, є додатковим рівнем захисту. Зрештою, без автентифікації та авторизації немає безпеки даних.

Кожна компанія сьогодні, у якій є співробітники, що взаємодіють з даними, а отже, кожна організація, повинна встановити контроль доступу до даних.

Після того, як ми розглянули питання «Що таке контроль доступу?», важливо зазначити, що ці засоби контролю впроваджуються для захисту ресурсів від несанкціонованого, незаконного доступу та забезпечення того, щоб суб'єкти могли отримувати доступ до об'єктів лише за допомогою безпечних, попередньо затверджених процедур.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи контролю доступу та аудиту дій при роботі з мережевою базою даних.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи контролю доступу та аудиту дій при роботі з мережевою базою даних. Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем контролю доступу та аудиту дій при роботі з мережевою базою даних.
- Дослідження системи контролю доступу та аудиту дій при роботі з мережевою базою даних.

– Програмна реалізація системи контролю доступу та аудиту дій при роботі з мережевою базою даних.

Об'єктом дослідження є процес контролю доступу та аудиту дій при роботі з мережевою базою даних.

Предметом дослідження є методи контролю доступу та аудиту дій при роботі з мережевою базою даних.

Методи дослідження базуються на методах побудови баз даних та захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Найвідоміші приклади контролю доступу до бази даних включають:

– Дискреційний контроль доступу (DAC). Власник даних надає доступ до моделей DAC. DAC – це метод призначення прав доступу на основі правил, визначених користувачем.

– Обов'язковий контроль доступу (MAC). У MAC людям дозволено доступ на основі дозволу на доступ до інформації, розробленого з використанням недискреційної парадигми. MAC позначає політику, яка призначає дозволи доступу на основі правил центрального органу влади.

– Контроль доступу на основі ролей (RBAC). RBAC використовує фундаментальні принципи безпеки, такі як «мінімальні привілеї» та «розділення привілеїв», щоб надавати доступ залежно від ролі користувача. Як результат, той, хто хоче отримати доступ до інформації, може отримати доступ лише до даних, необхідних для виконання його функції.

– Контроль доступу на основі атрибутів (ABAC). Кожен ресурс і користувач в ABAC отримує набір атрибутів. Цей динамічний підхід визначає доступ до ресурсів на основі порівняння характеристик користувача, таких як час доби, місцезнаходження та місцезнаходження.

Як працюють системи контролю доступу до баз даних

Системи контролю доступу до баз даних працюють з трьох сторін: користувача, адміністратора та інфраструктури:

– Користувач: Коли співробітник бажає увійти до зони обмеженого доступу, він повинен надати свої облікові дані. Запит на розблокування подається на зчитувач карток, який надсилає інформацію до блоку контролю доступу, що згодом авторизує користувача та відкриває двері.

– Адміністратор: Система контролю доступу має панель керування або портал на адміністративній стороні. Адміністратори офісу, IT-менеджери та керівники служби безпеки можуть використовувати портал керування, щоб вказати, хто має доступ до приміщення та за яких умов.

– Системна інфраструктура: Інфраструктура системи контролю доступу включає електричні замки, зчитувачі карт, стан дверей для моніторингу руху та пристрої запитів на вихід, всі з яких повідомляють на панель керування та сервер.

Ось деякі з найкращих практик використання системи контролю доступу до бази даних:

– Зосередьтеся на доступі до конфіденційних даних. Однією з реалій управління великою компанією є збір величезних обсягів конфіденційних даних, які потім зберігаються та обробляються в базах даних. Як наслідок, бази даних є поширеною мішенню для кібератак. Як наслідок, критично важливо зосередитися на безпеці даних. Почніть із запиту до вашого IT-відділу про створення базового плану поточних рівнів доступу та політик. Завдяки цьому ви зможете виявити недоліки у ваших існуючих процесах та викрити будь-яких серйозних порушників, таких як той, хто керує бізнесом зі свого робочого місця.

– Шифрування даних. Дані під час передачі або дані в русі активно переміщуються з однієї області в іншу, наприклад, через Інтернет або приватну мережу. З іншого боку, дані в стані спокою – це інформація, яка не переміщується активно з одного пристрою на інший або

з однієї мережі в іншу, наприклад, інформація, що зберігається на жорсткому диску, ноутбучі, флеш-накопичувачі, або архівована чи збережена іншим способом. Сучасні підприємства повинні захищати конфіденційні дані як під час передачі, так і в стані спокою, оскільки кіберзлочинці розробляють нові способи компрометації систем та крадіжки даних. Шифрування є популярним інструментом для захисту даних під час передачі та в стані спокою, і воно відіграє важливу роль у захисті даних.

– Освіта для всіх зацікавлених сторін даних. Це може здатися несподіванкою, але співробітники організації несуть найбільші ризики для її кібербезпеки. Хоча співробітники компанії є найбільшими носіями ризиків, вони також мають найбільшу користь для кібербезпеки організації. Завдяки постійній освіті та комплексній програмі навчання з безпеки, співробітники можуть забезпечити додаткову безпеку, виступаючи в ролі ще одного рівня захисту.

– Застосовуйте доктрину найменших привілеїв. Гарною відправною точкою для встановлення контролю доступу є використання Доктрини найменших привілеїв, яка по суті базується на принципі, що людина не повинна мати доступу до чогось, якщо їй не потрібно з цим працювати.

– Аудит та моніторинг. Аудит та моніторинг – це гарні заходи для забезпечення безпеки контролю доступу до бази даних. Оскільки співробітники більш схильні перевіряти обмеження доступу, коли ніхто не спостерігає, компанії можуть нагадувати своїм співробітникам, що їхня діяльність з доступу до даних контролюється.

Можливі ризики й приклади реальних інцидентів

До баз даних постійно прикута пильна увага зловмисників, як внутрішніх, так і зовнішніх. Щодня в українських компаніях відбувається безліч інцидентів порушення політик безпеки.

Приклад атаки зсередини

Адміністратор безпеки у фінансовій організації, використовуючи свої права, здійснював переміщення коштів між рахунками. Операція виконувалася в самій базі даних, при цьому журнал реєстрації дій відключався, або вироблялося його чищення.

Приклад атаки ззовні

Дані при їхній передачі між підрозділами компанії не захищалися за допомогою криптографії, залишаючи можливість їхнього прослуховування й зняття копії з мережного встаткування.

Безпечне конфігурування

Створення автоматизованого середовища забезпечення безпечної роботи з базами даних повинне містити в собі: виявлення баз даних, сканування по профілях безпеки, фіксація конфігурацій і т.п.

Навіть у випадку якщо база даних пройшла процедуру налаштування параметрів безпеки, це не виключає постійного контролю її стану, через те, що користувачі своїми діями можуть знижувати захищеність, неусвідомлено відкриваючи можливості для проникнення зловмисника й експлуатації уразливостей.

Технічні засоби забезпечення безпеки баз даних

Забезпечення безпеки Web-додатків

Через те що Web-додатки є невід'ємною частиною практично будь-якої бази даних, заходи, спрямовані на їхній захист, дозволяють за порівняно короткий строк, без впливу на сам процес роботи з базами даних, підвищити їхня захищеність від проникнень із зовнішнього середовища.

Можливості дозволяють реалізувати практично будь-яку конфігурацію, у тому числі й для високонавантажених систем.

Фізичний поділ компонентів БД, контроль доступу на мережному рівні

Поділ компонентів баз даних на мережному рівні повинне вироблятися за допомогою міжмережевих екранів, що забезпечують контроль доступу з перевіркою стану сесії й бажано з перевіркою користувачів по їх обліковим даним (інтеграція з LDAP, Active Directory та ін.).

Крім реалізації функцій поділу, бажано щоб міжмережевий екран мав функціонала виявлення й запобігання вторгнень.

Наявність наочних засобів адміністрування й візуалізації подій у міжмережевих екранах, є безсумнівним плюсом через прямий вплив на операційні витрати, пов'язані з розслідуванням інцидентів. Як можливі варіанти для рішення даного завдання є продукти компанії Check Point Software Technologies, PaloAlto Networks, Cisco Systems, Інфотекс, Код Безпеки й т.п.

Контроль доступу й аудит дій користувачів і адміністраторів

Реалізація функцій по контролі доступу, поділу прав, і виконанню аудита всіх дій, може бути виконана убудованими засобами БД. Однак, слід зазначити, що включення функцій по убудованому аудиті, як того вимагають завдання по забезпеченню безпеки (тобто не тільки базовий набір команд), приводить до зростання навантаження на апаратні ресурси від 10 до 30% залежно від бази даних, що у свою чергу тягне неефективну розтрату дорогих апаратних ресурсів. Реалізація функцій аудита убудованими засобами БД, у кожному разі залишає можливість адміністраторові відключити цього аудита.

У зв'язку із цим найбільш раціональним шляхом є винесення завдань по аудиті на зовнішню систему, що забезпечує запис всіх дій, виконуваних у БД користувачами й адміністраторами.

У загальному виді, рішення зможе складатися з декількох компонентів різних функцій, що забезпечують реалізацію, зокрема:

Сервер керування – для керування й збору даних із всіх компонентів рішення;

Шлюз – який реалізує функції розмежування доступу й аудита для мережних обігів;

Агент – який реалізує функції розмежування доступу й аудита для операцій, виконуваних безпосередньо із БД (даний спосіб роботи повинен бути максимально обмежений).

Звичайний міжмережевий екран не дозволяє працювати з даними на рівні sql – запитів, розбираючи їх і вишиковуючи для них профіль захисту.

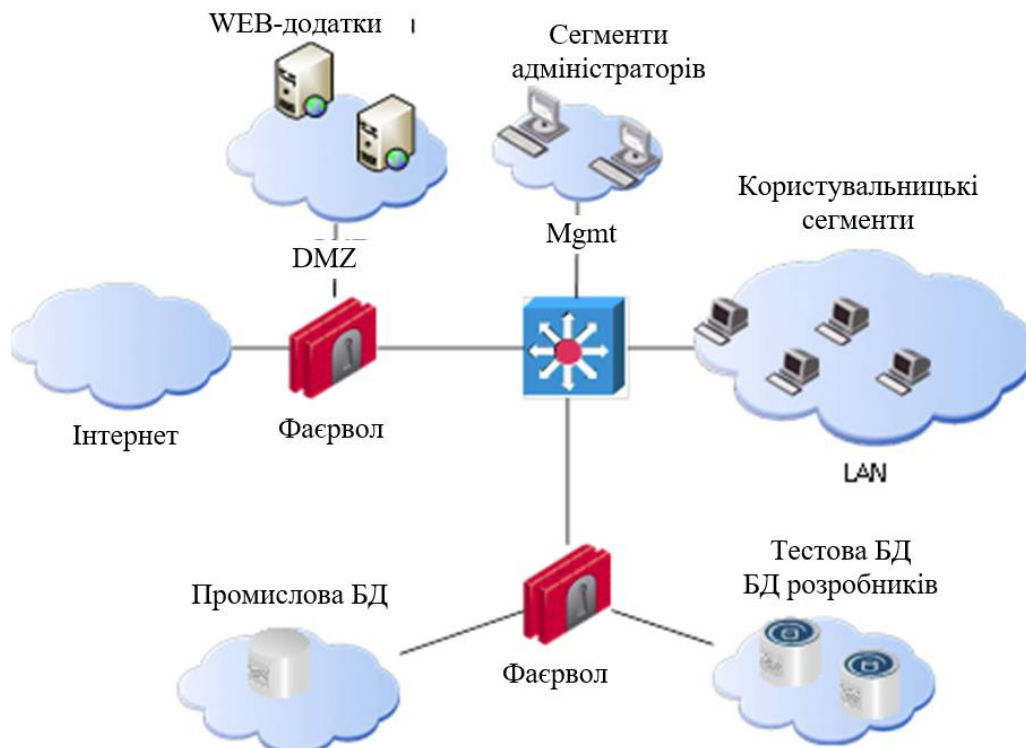


Рисунок 1 – Структурна схема системи

Поділ компонентів

Поділ бази даних на середовища розробки, тестування й промислове середовище, є обов'язковою вимогою й невід'ємною частиною всіх рекомендацій з безпеки. Однак це, у свою чергу народжує проблеми своєчасного одержання відновлень, даних із промислового середовища в тестову й розробки, швидкого відновлення й обслуговування декількох копій середовища розробки й тестування (через те, що ті самі відновлення можуть перевірятися як одночасно різними співробітниками й розроблювачами, так і для різних станів однієї й тої ж бази даних). Таким чином, швидке перенесення даних з одного середовища в інше, відновлення копій баз даних і їхнє адміністрування починає істотно впливати на операційні витрати.

Вирішити дані проблеми можна за допомогою розробленої програми, що також дозволяє паралельно вирішити завдання маскування даних у середовищі тестування й розробки.

Розроблена програма дозволяє віртуалізувати базу даних, швидко й ефективно працювати з копіями баз даних і інформацією в ній (відновлюючи/відкочуючи/видаляючи дані й стан бази даних на бажаний момент часу), а також забезпечити зміна даних стерпних із промислової бази даних у середовища розробки й тестування виконавши тим самим їх маскування.

Немаловажним завданням є перевірка встановлюваних на базу даних і її компоненти відновлень ПЗ. Необхідність постійного відновлення баз даних і її компонент із однієї сторони може бути викликана вимогами бізнесу (по додаванню нового функціонала), а з іншої сторони вимогами безпеки (усунення виявлених уразливостей). Вирішити дане завдання в тому числі можливо шляхом відпрацювання змін на віртуальних копіях бази даних.

Аналіз захищеності

Постійний контроль за змінами, що відбуваються з базами даних і їхніх компонентів, аналіз їхньої захищеності й схильності уразливостям повинен бути виділений в окремий процес, здійснюваний адміністраторами компанії, адміністраторами баз даних і розроблювачами. Для виявлення й аналізу уразливостей у базах даних варто використовувати сканери безпеки, при цьому їхнє застосування повинне виконуватися в строго погоджені технологічні "вікна" з дотриманням вимог по попередньому резервуванню поточних конфігурацій у базі даних. Сканування за допомогою технічного інструментарію повинне виконуватися по заздалегідь підготовлених профілях сканування актуальним для виконуваного завдання. Результати сканування повинні розбиратися й інтерпретуватися відповідними фахівцями, щоб з однієї сторони максимально точно настроїти профіль сканування, а з інший чітко позначити виявлені недоліки в конфігураціях баз даних, уразливості й відсутні відновлення.

Результатом проведеної роботи повинне з'явитися підтримка незмінності налаштувань безпеки в базах даних і її компонентів, виявлення відхилень від затверджених профілів безпеки й своєчасне усунення що виявляються уразливостей шляхом відновлення відповідних компонентів.

Виявлення відхилень у поведженні користувачів/адміністраторів

Рішення, що аналізують профіль поведження користувачів і адміністраторів, дозволяють у тому числі ефективно боротися із шахрайськими діями зловмисників навіть у тому випадку, якщо в них за якимись причинами виявилися легітимні облікові записи. Як подібні рішення можуть застосовуватися системи UBA (User Behavioral Analysis), принцип роботи яких будується на підставі складання профілю поведження для кожного контрольованого суб'єкта при його операціях з об'єктами доступу. При цьому варто враховувати факти спрацювання подібних систем у випадках появи додаткових повноважень у суб'єктів доступу, зміни їхніх прав і додавання нових об'єктів з якими здійснюється робота. Через вищесказаний найбільш доцільним є застосування систем UBA у

зв'язуванні з іншими системами, що фіксують правомірність зміни прав суб'єктів доступу, створення нових об'єктів доступу й т.п.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів контролю доступу та аудиту дій при роботі з мережевою базою даних. Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем контролю доступу та аудиту дій при роботі з мережевою базою даних.

– Досліджена система контролю доступу та аудиту дій при роботі з мережевою базою даних.

– На основі отриманих результатів досліджень створена програмна реалізація системи контролю доступу та аудиту дій при роботі з мережевою базою даних.

Розроблені алгоритми дозволяють успішно вирішувати завдання контролю доступу та аудиту дій при роботі з мережевою базою 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. 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. 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.
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. Akhalaia, G., Iavich, M., Iashvili, G., Prysiaznyy, D., Smirnova, T. «Secure Encrypted Connection on Georgian Website». CEUR Workshop Proceedings, 2023, 3550, pp. 313-320.
6. 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
7. 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.
8. 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.
9. 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.
10. 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.
11. 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.
12. 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.
13. 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.

14. 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.
15. Smirnov, O., Neskoriy, T., Fedorov, E., Rudakov, K., Neskoriy, A. «Method Detection Audit Data Anomalies on Basis Restricted Cauchy Machine» CEUR Workshop Proceedings, Volume 3187, 2022,
16. 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.
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 ґешування 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 ґешування 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 ґешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 1(67). С. 84-89.
21. 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
22. 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.
23. 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.
24. 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.
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., 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., Arischenko A., Chepurko I., Onikiychuk A., Kuznetsova T. «Pseudorandom sequences for spread spectrum image steganography». CEUR Workshop Proceedings Volume 2654, 2020, Pages 122-131.
29. 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.
30. 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.
31. 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.

УДК 004

Т.Кіріченко, магістр гр. КН-24М,

Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ НЕЙРОМЕРЕЖЕВИХ ЕКСПЕРТІВ БЕЗПЕЧНОЇ МАРШРУТИЗАЦІЇ У АНТИВІРУСИ

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

нейромережеві експерти, безпечна маршрутизація, антивірус

Постановка проблеми. Випереджати кіберзагрози з огляду на значне зростання кіберзлочинності – це постійний виклик. Зустрічайте хмарний антивірус, який змінює правила гри в кібербезпеці. Але що відрізняє його від традиційних антивірусних рішень і чому він стає вибором як для приватних осіб, так і для бізнесу?

Хмарний антивірус являє собою сучасний зсув у кібербезпеці, переносячи важку обробку даних з вашого пристрою на потужні віддалені сервери. На відміну від традиційного антивірусного програмного забезпечення, яке зберігає всі дані локально, хмарний антивірус працює переважно через сервери, підключені до Інтернету, що значно зменшує навантаження на вашу систему.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи нейромережевих експертів безпечної маршрутизації у антивіруси.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи нейромережевих експертів безпечної маршрутизації у антивіруси.

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

- Огляд існуючих систем нейромережевих експертів безпечної маршрутизації у антивіруси.
- Дослідження системи нейромережевих експертів безпечної маршрутизації у антивіруси.
- Програмна реалізація системи нейромережевих експертів безпечної маршрутизації у антивіруси.

Об'єктом дослідження є процес нейромережевих експертів безпечної маршрутизації у антивіруси.

Предметом дослідження є методи нейромережевих експертів безпечної маршрутизації у антивіруси.

Методи дослідження базуються на методах штучного інтелекту, методах комп'ютерних мереж, методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Алгоритми формування множини маршрутів передачі геш-файлу метаданих у хмарні антивірусні системи

Аналіз процесу функціонування телекомунікаційної системи, а також дослідження процесів формування, передачі й обробки метаданих у хмарних антивірусних системах [7, 9], дозволили визначити щільність розподілу ймовірностей часу передачі геш-файлу метаданих у хмарні антивірусні системи, а також обробки й доставки команд передачі керування, сформувати й математично формалізувати знання про зміни й характер поведінки основних ймовірнісно-часових показників якості обслуговування в телекомунікаційній системі.

Обмін метаданими між програмним клієнтом і сервером, у загальному випадку, здійснюється через транзитні маршрутизатори, послідовність яких на шляху від відправника до одержувача в рамках дипломної роботи визначимо як маршрут [13].

Нехай $\mathcal{R} = \{V_n | n \in 1, N\}$ – безліч маршрутизаторів у ТКС, V_n – n -й маршрутизатор, $N = |\mathcal{R}|$ – число маршрутизаторів, $\mathcal{Z} = \{\theta_\xi | \xi \in 1, \Theta\}$ – безліч каналів зв'язку в ТКС, де θ_ξ – ξ -й канал зв'язку, Θ – кількість каналів зв'язку в ТКС, $|Z|$ – потужність множини Z .

Інформаційні пакети метаданих для аналізу програмному серверу можуть бути передані по одному з маршрутів, що становлять безліч $\mathcal{S} = \{\eta_s | s \in 1, M\}$, де $\eta_s = \{\theta_{s,c} | \theta_{s,c} \in \mathcal{Z}; c \in 1, \Theta\}$ – s -й маршрут, $s \in 1, M$, $|\eta_s| = \Psi_s$, M – кількість маршрутів, $\theta_{s,c}$ – канал зв'язку з номером c , що належить s -му маршруту, Ψ_s – кількість каналів зв'язку на s -м маршруті.

Формування множини $\mathcal{S}$ маршрутів являє собою складний ітераційний процес, що складається у виконанні декількох алгоритмів:

- алгоритм пошуку найкоротших шляхів між вузлами в ТКС;
- алгоритм формування базової множини маршрутів передачі метаданих;
- алгоритм безпечної маршрутизації на базовій множини шляхів передачі метаданих у програмний сервер.

Початок роботи з хмарним антивірусом зазвичай простий. Ось загальний огляд кроків налаштування. Пам'ятайте, що точні кроки та інтерфейс можуть дещо відрізнятися залежно від обраного вами постачальника.

1. Встановлення:

– Завантаження: Відвідайте веб-сайт та завантажте інсталяційний файл. *Ніколи не завантажуйте програмне забезпечення з неофіційних джерел.*

– Запустіть інсталятор: знайдіть завантажений файл (зазвичай це.exe або.dmg) і двічі клацніть його, щоб розпочати інсталяцію.

– Налаштування облікового запису: Вам, ймовірно, буде запропоновано створити обліковий запис або увійти, якщо він у вас вже є. Це часто необхідно для керування підпискою та доступу до функцій.

2. Початкова конфігурація (зазвичай автоматична):

Більшість хмарних антивірусних рішень розроблені для ефективної роботи з налаштуваннями за замовчуванням. Зазвичай автоматично вмикаються такі параметри:

– Захист у режимі реального часу: цей захист постійно контролює вашу систему на наявність загроз.

– Хмарне сканування: це дозволяє програмному забезпеченню надсилати файли до хмари для аналізу.

– Автоматичні оновлення: це гарантує, що ваш антивірус завжди оновлений найновішими визначеннями загроз.

3. Додаткове налаштування (за потреби):

Після початкового налаштування ви можете ознайомитися з деякими додатковими параметрами:

– Планування сканування: налаштуйте регулярне сканування, щоб автоматично перевіряти систему на наявність загроз у певний час.

– Інтенсивність сканування: Деякі програми пропонують різні рівні сканування (наприклад, швидке сканування, повне сканування). Повне сканування перевіряє всі файли, але займає більше часу.

– Захист веб-сайту: налаштуйте параметри, пов'язані з блокуванням шкідливих веб-сайтів та спроб фішингу.

– Виключення файлів: Якщо у вас є певні файли або папки, яким ви довіряєте та не хочете, щоб їх сканували (наприклад, файли розробки), ви можете додати їх до списку виключень. *Використовуйте цю функцію обережно.*

4. Перевірка та тестування:

– Запустіть ручне сканування: виконайте повне сканування системи, щоб переконатися, що все працює правильно.

– Перевірте стан захисту: знайдіть видимий значок у системному треї або області сповіщень, який вказує на активність захисту в режимі реального часу.

– Тестування оновлень: Перевірте наявність оновлень вручну, щоб підтвердити, що функція оновлення працює.

Поради професіоналів для оптимальної продуктивності:

– Стабільне інтернет-з'єднання: Хмарний антивірус потребує інтернет-з'єднання для сканування. Переконайтеся, що у вас стабільне з'єднання для найкращої продуктивності.

– Час початкового сканування: Запуск повного сканування системи може зайняти деякий час, якщо ви активно не використовуєте комп'ютер.

Більшість хмарних антивірусних програм розроблені з урахуванням зручності використання та вимагають мінімального налаштування. Налаштування за замовчуванням часто забезпечують достатній захист для більшості користувачів. Якщо ви не впевнені щодо будь-яких налаштувань, зазвичай краще залишити їх як є. Зверніться до документації або ресурсів підтримки вашого постачальника антивірусної програми, якщо у вас є особливі потреби або виникли проблеми.

Хмарні антивірусні рішення – це ті, що зберігають інформацію про варіанти шкідливого програмного забезпечення в хмарі, а не на пристрої користувача. Традиційні, так звані «спискові» антивірусні рішення зберігають списки відомих шкідливих фрагментів коду на самому пристрої, що може негативно вплинути на продуктивність машини.

Щоб краще зрозуміти хмарне антивірусне програмне забезпечення, вам допоможе розуміння терміну «хмара». Хмара – це просто децентралізований простір для зберігання даних, до яких ваш комп'ютер має доступ через Інтернет.

Наше хмарне антивірусне програмне забезпечення захищає вас або ваш бізнес, взаємодіючи з базою даних загроз, яка зберігається не на вашому комп'ютері, а в хмарі.

Як працює хмарний антивірус

Зберігаючи визначення загроз (файли, класифіковані як шкідливі програми або небезпечні IP-адреси та URL-адреси) у хмарі, а не на самому пристрої, хмарне антивірусне програмне забезпечення не потребує зберігання всіх цих мільйонів визначень на власному жорсткому диску, звільняючи місце.

А оскільки оновлення можна надсилати до вашого антивірусного програмного забезпечення віддалено через хмару, ви не будете змушені мати статичний список загроз, від яких програмне забезпечення знає, що його потрібно захищати. Щойно нові загрози виявляються, наприклад, командою дослідників загроз, які підтримують ваше антивірусне програмне забезпечення, оновлення може бути розповсюджено на всі пристрої, які його використовують. Це забезпечує захист майже в режимі реального часу від постійно мінливого ландшафту загроз, що існує в Інтернеті.

Переваги хмарних антивірусних рішень:

- Доступ до більшої бази даних загроз без необхідності зберігати її на жорсткому диску
- Менший інсталяційний агент для вашого антивірусного програмного забезпечення, тому він займає менше місця
- Оновлення визначень майже в режимі реального часу на основі даних, зібраних з усієї мережі користувачів

Існуючий каталог поліморфного шкідливого програмного забезпечення, фішингу нульового дня та аналогічних загроз, що розвиваються, є величезним. Розміщення такої величезної кількості даних на одному комп'ютері знизить продуктивність до такої міри, що комп'ютер стане практично непрацездатним під час сканування.

На щастя, значні досягнення у хмарних обчисленнях відбулися на початку нового тисячоліття. Ті компанії, які змогли використати можливості хмари для антивірусного програмного забезпечення, чекали суттєвих покращень швидкості та продуктивності. Менші агенти встановлення означали менше часу та місця, що використовуються під час встановлення. Менша кількість визначень, що зберігаються на пристрої, почала означати менше або взагалі відсутність перерв для планового сканування.

Окрім зменшення навантаження на сховище окремих пристроїв, оновлення визначень – ці виправлення курсу, додані до програмного забезпечення для захисту від нещодавно виявлених загроз – займають лічені хвилини, а не дні чи тижні, які можуть знадобитися для створення тих самих оновлень без допомоги хмари. Якщо вам коли-небудь доводилося чекати, поки ваш комп'ютер оновиться, ви знаєте, як це розчаровує. Не кажучи вже про загрози, з якими ви могли зіткнутися в проміжку між оновленнями версій.

Хмарний антивірус для бізнесу

Хмарні антивірусні рішення не менш важливі для бізнесу, ніж для домашніх користувачів. Навпаки, під час встановлення засобів захисту кінцевих точок на велику кількість пристроїв, повільна інсталяція, спричинена великими агентами, характерними для традиційних антивірусних рішень, може значно збільшитися.

Крім того, хмарний антивірус для бізнесу гарантує, що кожен пристрій буде захищено від нових загроз лише за кілька хвилин після їх виявлення будь-якою захищеною кінцевою точкою, у всьому світі, без ручних оновлень чи інших перерв у роботі.

Структурна схема системи представлена на рис. 1.

Для нормального функціонування системи нейромережових експертів безпечної маршрутизації необхідно підготувати й систематизувати дані, на основі яких виробляється навчання його окремих нейромережових компонентів. Для рішення цього завдання блок формування навчальної й тестової вибірки формує дані для навчання нейронної мережі, упорядковує й організує з метою забезпечення можливості їхньої подальшої обробки за допомогою нейромережових технологій.

Цей етап роботи алгоритму є одним з найбільш важливих, тому що дозволяє реалізувати в сукупності нейронних мереж здатність до узагальнення. Вхідні дані, необхідні для виконання своїх функцій даним блоком, і спосіб їхнього одержання для формування навчальної й тестової множини асоціативної машини формуються відповідно до принципів, наведених вище.

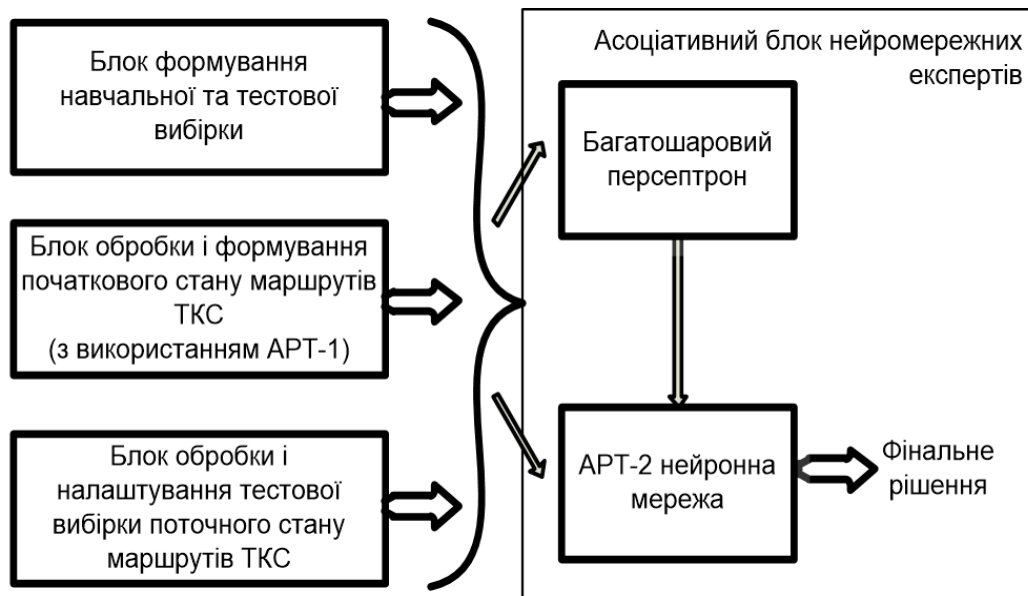


Рисунок 1 – Структурна схема системи

Блок обробки й формування початкового стану маршрутів ТКС формує значення параметрів всієї системи перед початком її навчання. Якщо змінні навчальної системи, що налаштовується, ініціалізувати таким чином, щоб вони були наближені до оптимальних значень, то процедура навчання буде зведена до «підстроювання» моделі. Синтез оптимального алгоритму ініціалізації значно скоротить час навчання нейромережних експертів.

У якості алгоритму початкової установки параметрів запропонований кооперативний імунний алгоритм із генерацією рішень на основі процедури генетичного пошуку з використанням нейронної мережі АРТ-1.

У загальну структуру блоку нейромережних експертів доцільно включити блок обробки й налаштування тестової вибірки поточного стану маршрутів ТКС, що виконує адаптацію компонентів нейронної мережі для рішення поставленого завдання. У дипломній роботі процедура навчання здійснювалася для всіх нейронних мереж по алгоритмах, адаптованим до їх архітектурам.

Антивірус на основі агента

Антивірусний агент розгортається на кожній віртуальній машині в рамках проекту та взаємодіє з модулем на гіпервізорі. Це створює споживання обчислювальних ресурсів, що робить цей підхід неефективним у великих масштабах.

Безагентний антивірус

Безагентний підхід базується на використанні Virtual Security Appliance (VSA) для сканування файлів, до яких мають доступ віртуальні машини, та Network Security Appliance (NSA) для сканування мережевого трафіку між віртуальними машинами, розташованими на хості. На жаль, лише VMware, Citrix та Microsoft підтримують VSA та NSA.

Ці рішення використовують потужність гіпервізора для зменшення навантаження на віртуальні машини, спричиненого звичайними антивірусними програмами. Однак вони мають кілька обмежень, пов'язаних із виявленням атак нульового дня:

- Антивірус, навіть оснащений евристичним механізмом, у більшості випадків не виявляє невідоме шкідливе програмне забезпечення нульового дня. Щоб уникнути виявлення, сучасні платформи кібершпигунства, такі як EquationDrug, що використовуються Regin та Epic Turla APT, використовують драйвер руткіту в режимі ядра, щоб приховати свої файли, ключі реєстру та процеси, перехоплюючи деякі функції Native API.

- Розширене шкідливе програмне забезпечення може знешкодити антивірус після виявлення на цільовій машині.

– Хмара в багатьох випадках є гетерогенним (гібридним) середовищем, побудованим на різних операційних системах та гіпервізорах, що збільшує витрати на розгортання та експлуатацію, а також робить ваш захист негнучким та залежним від постачальника.

Не рекомендуємо значних інвестицій у захист від шкідливого програмного забезпечення на вузлах. Достатньо правильно налаштувати вбудований брандмауер Linux, використовувати розумну політику контролю доступу (логіні/паролі, ключі SSH тощо) та розгорнути NGFW або IDPS для моніторингу мережевого трафіку. Для розширеного захисту від атак нульового дня та цілеспрямованих атак використовуйте рішення на основі «пісочниці», куди можна завантажувати підозрілі файли та URL-адреси для аналізу.

Переваги хмарного антивіруса:

1. Мінімальний вплив на продуктивність пристрою: Хмарний антивірус використовує мінімальну кількість ресурсів пристрою, що забезпечує плавнішу роботу з комп'ютером без зниження продуктивності, спричиненого традиційним антивірусним програмним забезпеченням.

2. Оновлення в режимі реального часу та виявлення загроз: База даних виявлення загроз знаходиться в хмарі, що дозволяє їй отримувати миттєві оновлення для боротьби з новими загрозами в міру їх появи. Це гарантує захист вашої системи від найновіших вірусів та шкідливих програм без необхідності ваших дій.

3. Швидше сканування: Сканування хмари на наявність загроз дозволяє швидше проводити аналіз, скорочуючи час взаємодії з системою. Це дозволяє швидше проводити перевірки з використанням найсучасніших заходів безпеки.

4. Використовує колективний інтелект: Хмарний антивірус використовує комплексну мережу інформації про загрози, навчаючись на основі даних, зібраних від усіх користувачів. Це колективне розуміння робить антивірус розумнішим та ефективнішим у виявленні та нейтралізації нових загроз.

Хоча хмарний антивірус пропонує чудовий захист, пам'ятайте про такі фактори:

1. Залежність від Інтернету:

- Для оптимальної роботи потрібне стабільне з'єднання
- Розгляньте можливості захисту в автономному режимі

2. Вплив на продуктивність:

- Можливі незначні затримки сканування.
- Мінімальне використання локальних ресурсів порівняно з традиційним антивірусом.

З появою генеративного штучного інтелекту та його впливом на автоматизацію безпеки, хмарні загрози розвиваються. Поява Інтернету речей (IoT) принесла підприємствам численні інноваційні можливості, але також принесла безпрецедентні ризики. Ми також повинні враховувати геополітичні зрушення, зміну динаміки ринку та економічного ландшафту. Усі ці сфери впливають на кібербезпеку та її зростання.

Кіберстійкість більше не є обов'язковою; вона стає обов'язковою, оскільки організаціям потрібно йти в ногу зі зміною темпів загроз. Зловмисники стають креативними у способах здійснення атак і можуть саботувати бізнес-операції, руйнуючи ланцюжки створення вартості за лічені секунди.

Генеративний штучний інтелект може створювати дипфейки, маніпулювати даними та розробляти спеціалізовані схеми соціальної інженерії. Підприємства не можуть уникнути цих загроз або впоратися з ними, використовуючи звичайні заходи безпеки. Для ефективної боротьби з ними їм потрібні складні засоби захисту, включаючи прогностичну розвідку загроз. Кібербезпека та хмарна безпека – це два різні типи цифрової безпеки. Обидва є критично важливими. У цьому блозі ми обговоримо відмінності між хмарною безпекою та кібербезпекою, щоб ви могли вирішити, як ефективно поєднати обидва.

Що таке хмарна безпека?

Хмарна безпека – це розділ кібербезпеки, який захищає клієнтів, постачальників хмарних послуг та організації. Вона забезпечує конфіденційність та безпеку даних клієнтів. Хмарна безпека ідеально підходить для організацій, які розміщують конфіденційні цифрові активи в хмарі. З початку пандемії COVID-19 більшість організацій перейшли на моделі віддаленої роботи.

Хмарна безпека захищає користувачів хмари, їхні облікові записи, взаємодію та програми. Це модель спільної відповідальності, в якій клієнти несуть відповідальність за завантаження та обмін своїми даними. Постачальник послуг зв'язку (CSP) відповідає за захист інфраструктури та встановлення виправлень, керування конфігурацією, фізичні хости та хмарні мережі.

Основні компоненти хмарної безпеки

Основні компоненти хмарної безпеки включають керування ідентифікацією та доступом (IAM), мережеву безпеку, безпеку даних, безпеку кінцевих точок та безпеку програм. Їх можна описати наступним чином:

– Безпека IAM: Компонент IAM безпеки хмари включає керування тим, хто має доступ до хмарних ресурсів, та діями, які вони можуть виконувати. Системи IAM керують ідентифікаторами користувачів, ведуть журнали аудиту та застосовують політики безпеки. Вони реалізують найменш привілейований доступ, розділяють обов'язки користувачів, виявляють незвичайну поведінку користувачів та виявляють ранні ознаки потенційних порушень безпеки.

– Мережева безпека: Мережева безпека поєднує системи виявлення вторгнень, системи запобігання вторгненням, віртуальні приватні мережі та брандмауери. Вона є критично важливою в хмарі, оскільки дані передаються від пристроїв до Інтернету.

– Безпека даних: Безпека даних – це компонент хмарних обчислень, який захищає дані під час передачі та в стані спокою. Він використовує різні заходи, такі як токенизація, шифрування, технології запобігання втраті даних та безпечне керування ключами. Контроль доступу та безпечні конфігурації також повинні застосовуватися до хмарних сховищ та баз даних.

– Безпека кінцевих точок : Багато організацій перейшли на моделі віддаленої роботи та запровадили політики «принеси свій власний пристрій» (BYOD) . Безпека кінцевих точок зосереджена на захисті пристроїв користувачів та кінцевих точок, які мають доступ до хмари або підключаються до неї. До них належать смартфони, планшети, ноутбуки, пристрої Інтернету речей, флеш-накопичувачі та інші портативні пристрої зберігання даних.

– Безпека додатків: Безпека додатків передбачає оптимізацію безпеки хмарних додатків. Вона захищає додатки від міжсайтового скриптингу, атак ін'єкцій та міжсайтових підробок. Вона включає сканування на вразливість, тести на проникнення, сканування інфраструктури як коду, сканування образів контейнерів та інші практики. Для додавання додаткових рівнів захисту вона також включає самозахист додатків під час виконання та брандмауери веб-додатків.

Кібербезпека – це акт і мистецтво захисту мереж, даних і пристроїв від несанкціонованого доступу та злочинного використання. Вона забезпечує дотримання практик, що забезпечують цілісність, конфіденційність та доступність інформації.

Кібербезпека захищає будь-які активи, підключені до Інтернету. Вона виходить за межі критичної інфраструктури, такої як електромережі, системи водопостачання чи будь-які апаратні рішення, що підключаються до Всесвітньої мережі. Кібербезпека гарантує безпеку ваших мереж від зовнішніх вторгнень.

Кожен бізнес повинен захищати свої дані. Цей захист не обмежується онлайн-системами; він може включати офлайн-системи та цифрові системи. Кібербезпека виходить за рамки традиційного розуміння, зосереджуючись на безпеці локальної інфраструктури та

даних. Вона має спеціальні ресурси для розміщення ваших активів, мереж, пристроїв та систем.

Ключовим моментом є те, що кібербезпека може бути передбачуваною. Ви знаєте масштаб вашої інфраструктури, і зазвичай вона фіксована. Ви не можете раптово масштабувати своє підприємство, а мобільність обмежена, оскільки дані обмежені фізичними межами організації.

Основні компоненти кібербезпеки

Ось огляд основних компонентів кібербезпеки:

- Критична інфраструктура: вона слугує основою бізнес-операцій компанії. Ваша критична інфраструктура міститиме фізичні та мережеві компоненти, такі як електричні мережі, телекомунікаційне обладнання, апаратне забезпечення тощо.

- Інтернет речей (IoT): IoT – це мережа підключених пристроїв, що з'єднуються з хмарними екосистемами. Він є частиною кібербезпеки та включає принтери, сканери, датчики, камери та інше обладнання.

- Мережева безпека: Мережева безпека в контексті кібербезпеки включає брандмауери, поведінкову аналітику, засоби контролю доступу, антивірусне програмне забезпечення та засоби захисту від шкідливих програм.

- Навчання та обізнаність співробітників – це незначний, але водночас важливий компонент. Постійне навчання співробітників може допомогти вашим працівникам впроваджувати найкращі практики кібергігієни та знати, що робити, коли вони стикаються з онлайн-загрозами. Працівники повинні регулярно проходити навчання з розуміння тактик соціальної інженерії, створення надійних паролів та ознайомлення з політиками використання особистих пристроїв. Вони також повинні пам'ятати про політику «Принеси свій пристрій із собою» (BYOD) та боротися з тіньовими IT-загрозами.

Ось три критичні відмінності між хмарною безпекою та кібербезпекою.

1. Обсяг захисту

Кібербезпека захищає ваші мережі, обладнання, кінцеві точки та інші елементи вашої локальної інфраструктури. Хмарна безпека більше зосереджена на безпеці моделей хмарних сервісів, таких як IaaS, SaaS та PaaS. Вона використовує шифрування, керування ідентифікацією та доступом, а також безпечно налаштовує ваші хмарні ресурси.

2. Управління та розгортання

Рішення з кібербезпеки передбачають розгортання локально, що вимагає значних інвестицій у фізичну IT-інфраструктуру, апаратне забезпечення, пристрої та інші компоненти. Хмарні рішення безпеки більше базуються на програмному забезпеченні. Хмарні центри обробки даних поширені по всьому світу, і постачальник відповідає за розміщення інфраструктури для надання хмарних послуг.

Підприємства повинні оформити підписку, щоб використовувати або орендувати ці інфраструктурні ресурси. Хмарне сховище та продуктивність чудові, і вони можуть знизити витрати на обладнання. Хмарна безпека пропонує максимальну гнучкість та масштабованість для підприємств, які бажають мобільного підходу до безпеки.

3. Типи атак

Традиційні загрози кібербезпеці включають програми-вимагачі, шкідливе програмне забезпечення, інсайдерські атаки, соціальну інженерію та фішинг. Загрози безпеці хмарних сервісів класифікуються як атаки SaaS-додатків, неправильні конфігурації робочого навантаження, незахищені API та витоки даних.

Організаціям доводиться вибирати між хмарною безпекою та кібербезпекою, залежно від налаштування своїх операцій, інфраструктури даних та пріоритетів безпеки. Хмарна безпека є критично важливою, якщо ваша організація значною мірою залежить від хмарних програм або послуг.

З іншого боку, кібербезпека є важливою для захисту локальних систем та активів, таких як локальні сервери, кінцеві точки та критична інфраструктура. Існує велика різниця між підходами до хмарної безпеки та кібербезпеки.

Галузі зі статичними середовищами даних або ті, що досі керують застарілими системами, такі як виробництво чи урядові організації, отримують велику користь від заходів кібербезпеки, які спрямовані на вирішення традиційних загроз, таких як шкідливе програмне забезпечення, програми-вимагачі та фішингові атаки.

Гібридні налаштування можуть вимагати балансу між обома, особливо зі зростанням впровадження хмарних технологій, але локальні системи залишаються невід'ємною частиною. Бізнеси, які переходять у хмару, повинні забезпечити поступове зміщення акценту на безпеку для захисту як застарілих систем, так і нових хмарних платформ.

Зрештою, все зводиться до оцінки вразливостей та інвестування в безпеку. Незалежно від того, чи йдеться про захист динамічного середовища в хмарі, чи про фіксовану інфраструктуру локальних систем, зосередження на правильній області гарантує повний захист від загроз, що постійно змінюються.

Ось деякі варіанти використання хмарної безпеки та кібербезпеки. Давайте розглянемо, в яких галузях використовуються ці технології та якими способами:

- Індустрія фінансових послуг найбільше потребує найкращих рішень у сфері кібербезпеки. Фірми повинні шифрувати транзакції, захищати автентифікацію та захищати себе від шкідливого програмного забезпечення та фішингових інцидентів.

- Галузь охорони здоров'я може бути використана для крадіжки особистих даних, вимагання або шантажу. Зловмисники можуть погрожувати лікарням та захоплювати бази даних. Цей сегмент потребує кібербезпеки для швидкого реагування на загрози. Він підтримує всі системи в актуальному стані з використанням найновіших протоколів, механізмів передачі даних, алгоритмів шифрування тощо. Хмарні рішення безпеки оптимізують процес реєстрації пацієнтів та спрощують процес. Вони також можуть зберігати медичні записи та обмінюватися ними з лікарями, а також записуватися на прийом.

- Роздрібна торгівля та електронна комерція є популярним випадком використання кібербезпеки. Бренди повинні захищати номери кредитних карток клієнтів, паролі, облікові дані для входу та іншу конфіденційну інформацію. Компанії використовують рішення з кібербезпеки для запобігання несанкціонованому доступу та впроваджують надійну багаторівневу автентифікацію та шифрування.

- Хмарні рішення безпеки використовуються компаніями, що активно працюють на платформах соціальних мереж, для аналізу настроїв та запобігання зловмисній поведінці. Це може допомогти виявити потенційних зловмисників та запобігти внутрішнім загрозам.

Вибір рішень для хмарної безпеки та кібербезпеки вимагає ретельного врахування потреб, бюджетів та ресурсів організації. По-перше, проаналізуйте свої бюджетні обмеження. Хмарні рішення для безпеки, часто на основі підписки, усувають необхідність інвестицій в обладнання та загалом знижують початкові витрати, пов'язані з такими покупками. З іншого боку, рішення для кібербезпеки можуть вимагати значних капітальних витрат на їх розгортання та подальше обслуговування, тому вони краще підходять для організацій з уже великим ІТ-бюджетом.

Географічне розташування також є фактором. Через масштабованість та мобільність глобальні організації з розподіленими командами частіше зосереджуються на хмарній безпеці. Водночас місцеві компанії зі стаціонарними операціями можуть більше використовувати традиційні заходи кібербезпеки для захисту локальних активів.

Інші вирішальні фактори включають розмір вашої команди та рівень досвіду. Невеликі або погано оснащені команди можуть побачити переваги хмарної безпеки, такі як керовані сервіси та просте налаштування. Однак більші компанії з великими ІТ-відділами можуть захотіти зберегти повний контроль над налаштуваннями та налаштуваннями, доступними за допомогою локальних рішень кібербезпеки.

Врахуйте свою поточну інфраструктуру та потреби щодо майбутньої масштабованості. Якщо ваша організація планує розширюватися, хмарні рішення є більш масштабованими та легшими для інтеграції з новими технологіями. З іншого боку, якщо ваша інфраструктура статична, а траєкторія зростання стабільна, традиційних інвестицій у кібербезпеку може бути достатньо.

Якщо раніше ви не могли вирішити між кібербезпекою та хмарною безпекою, тепер у вас є відповідь: вам потрібні обидві.

Хмарна безпека та кібербезпека стали важливими для захисту сучасних цифрових екосистем. У той час як хмарна безпека зосереджена на захисті хмарних середовищ та збереженні конфіденційності даних, кібербезпека захищає локальні системи та мережі. Будь-який з варіантів залежить від інфраструктури вашої організації, операційних потреб та траєкторії зростання. Зі зростанням кіберзагроз стає важливим знайти баланс, впроваджуючи хмарні та традиційні заходи безпеки.

Оцініть свої вразливості та співпрацюйте з перевіреними постачальниками, щоб розробити індивідуальну та стійку систему безпеки. Ви можете захистити свої активи та досягти довгострокового успіху за допомогою правильних інструментів.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів нейромережових експертів безпечної маршрутизації у антивіруси. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем нейромережових експертів безпечної маршрутизації у антивіруси.

- Досліджена система нейромережових експертів безпечної маршрутизації у антивіруси.

- На основі отриманих результатів досліджень створена програмна реалізація системи нейромережових експертів безпечної маршрутизації у антивіруси.

Розроблені алгоритми дозволяють успішно вирішувати завдання нейромережових експертів безпечної маршрутизації у антивіруси. 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., Ільєнко, А., Улічев, О., Мелешко, Є., Смірнов, О. «Правові засади поширення інформаційних впливів в соціальних мережах». Електронне фахове наукове видання «Кибербезпека: 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». Кибербезпека: 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». Кибербезпека: 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., 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., 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». Кибербезпека: 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.

УДК 004

Д.Ковальов, магістр гр. КІ-24М,

Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ МЕРЕЖЕВОГО ВІДЕОСПОСТЕРЕЖЕННЯ ДЛЯ РЕАЛІЗАЦІЇ СТРАТЕГІЇ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПІДПРИЄМСТВА

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

мережеве відеоспостереження

Постановка проблеми. Нещодавнє дослідження показало, що інтеграція передової відеоаналітики в системи спостереження може підвищити точність виявлення інцидентів до 30%. Цей значний крок уперед підкреслює вирішальну проблему, з якою стикаються технологічні лідери в різних галузях: інтеграція складних технологій спостереження для посилення безпеки та операційної ефективності без шкоди для конфіденційності чи відповідності вимогам.

Еволюція відеоспостереження від простого заходу безпеки до багатогранного операційного інструменту пропонує численні переваги, але також створює складні виклики. Керівники повинні діяти обережно, балансуючи між впровадженням передових технологій спостереження та етичними міркуваннями та правовими обмеженнями. У цьому блозі буде досліджено нюанси ролі відеоспостереження у підвищенні безпеки, моніторингу продуктивності, забезпеченні відповідності вимогам, покращенні обслуговування клієнтів, управлінні кризами та запобіганні фінансовим втратам. Крім того, ми заглибимося в міркування, необхідні під час вибору обладнання, важливість комплексної стратегії спостереження, необхідність забезпечення конфіденційності даних та життєво важливу роль навчання персоналу служби безпеки.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи мережевого відеоспостереження для реалізації стратегії забезпечення безпеки підприємства.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи мережевого відеоспостереження для реалізації стратегії забезпечення безпеки підприємства.

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

- Огляд існуючих систем мережевого відеоспостереження для реалізації стратегії забезпечення безпеки підприємства.

– Дослідження системи мережевого відеоспостереження для реалізації стратегії забезпечення безпеки підприємства.

– Програмна реалізація системи мережевого відеоспостереження для реалізації стратегії забезпечення безпеки підприємства.

Об'єктом дослідження є процес мережевого відеоспостереження для реалізації стратегії забезпечення безпеки підприємства.

Предметом дослідження є методи мережевого відеоспостереження для реалізації стратегії забезпечення безпеки підприємства.

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

Виклад основного матеріалу. Важливість відеоспостереження в бізнес-середовищі неможливо переоцінити, оскільки воно відіграє вирішальну роль у забезпеченні безпеки, захисту та операційної ефективності організації. Ця технологія еволюціонувала від базових заходів безпеки до складного інструменту, який пропонує безліч переваг у різних аспектах бізнес-операцій. Ось ключові області, які підкреслюють важливість відеоспостереження в бізнес-контексті:

– Підвищення безпеки та захисту – відеоспостереження діє як превентивний захід проти потенційних зловмисників, злодіїв та інших зловмисних осіб, значно знижуючи ризик несанкціонованого доступу та крадіжки. Воно дозволяє здійснювати моніторинг приміщень у режимі реального часу, гарантуючи, що будь-яку підозрілу діяльність можна буде виявити та оперативно усунути. Більше того, у разі невідомого скоєння злочинної діяльності відеозаписи можуть слугувати важливим доказом для допомоги у розслідуваннях та судових процесах.

– Моніторинг та підвищення продуктивності праці – наявність камер спостереження також може позитивно впливати на поведінку працівників, заохочуючи дотримання політик та процедур на робочому місці. Менеджери можуть використовувати відеозаписи для моніторингу робочого процесу, оцінки ефективності персоналу та визначення областей, де можна підвищити ефективність. Такий моніторинг допомагає оптимізувати ресурси та забезпечити ефективний внесок працівників у досягнення цілей організації.

– Забезпечення відповідності вимогам та запобігання відповідальності – Деякі галузі промисловості підпадають під суворі вимоги щодо дотримання нормативних актів, які передбачають моніторинг та запис операцій. Відеоспостереження допомагає забезпечити дотримання підприємствами цих правил, тим самим уникаючи потенційних штрафів та юридичних проблем. Крім того, воно може захистити організацію від неправдивих претензій щодо відповідальності, надаючи незаперечні докази інцидентів, що відбуваються на її території.

– Покращення клієнтського досвіду -Відеоспостереження – це не лише питання безпеки, це також інструмент для покращення обслуговування клієнтів. Аналізуючи відеозаписи, компанії можуть отримати уявлення про поведінку, вподобання та моделі поведінки клієнтів. Цю інформацію можна використовувати для оптимізації планування магазинів, покращення розміщення товарів та покращення загального досвіду клієнтів, що призводить до підвищення задоволеності та лояльності.

– Управління кризовими ситуаціями та реагування на надзвичайні ситуації – у надзвичайних ситуаціях, таких як стихійні лиха, пожежі чи інші кризи, системи відеоспостереження відіграють ключову роль в управлінні кризовими ситуаціями. Вони надають дані в режимі реального часу, які можуть допомогти в оцінці ситуації, координації зусиль з реагування на надзвичайні ситуації та мінімізації збитків. Аналіз відеозаписів після події також може сприяти кращій підготовці до майбутніх інцидентів.

– Економія коштів та запобігання втратам – впровадження комплексної системи відеоспостереження може призвести до значної економії коштів, запобігаючи крадіжкам, зменшуючи страхові внески та мінімізуючи потребу у фізичних заходах безпеки. Вона також

відіграє вирішальну роль у запобіганні втратам, як з точки зору активів, так і інтелектуальної власності, тим самим захищаючи фінансове здоров'я бізнесу.

Впровадження системи відеоспостереження на підприємстві дозволяє здійснювати моніторинг у режимі реального часу, що дає змогу співробітникам служби безпеки оперативно реагувати на будь-які підозрілі дії. Це забезпечує відчуття безпеки та спокою співробітникам, відвідувачам та клієнтам, сприяючи створенню позитивної робочої атмосфери.

Вибір правильного обладнання та технологій для ваших потреб безпеки

Вибір відповідного обладнання та технологій є важливим для успіху системи відеоспостереження на підприємстві. Важливо враховувати такі фактори, як розмір приміщення, необхідний рівень безпеки та конкретні потреби організації.

Оцінка організаційних потреб та цілей безпеки

Першим кроком у виборі правильного обладнання та технологій є визначення конкретних потреб організації. Це включає розуміння основних цілей безпеки, таких як стримування, спостереження в режимі реального часу, розслідування інцидентів або контроль доступу. Кожна ціль може вимагати різних типів технологій та обладнання. Наприклад, стримування може бути досягнуто за допомогою помітно розміщених камер високої роздільної здатності, тоді як розслідування інцидентів може бути корисним для камер, оснащених криміналістичною деталізацією та можливостями масштабування.

Розуміння фізичного середовища

Планування та розмір приміщення відіграють вирішальну роль у визначенні типу та кількості необхідних камер, а також необхідності використання певних функцій, таких як ширококутні об'єктиви або можливості панорамування, нахилу та масштабування (PTZ). Умови низької освітленості можуть вимагати камер з покращеними можливостями нічного бачення, тоді як великі відкриті простори можуть виграти від камер з більшою дальністю дії.

Вибір функцій камери, таких як ширококутні об'єктиви або можливості панорамування, нахилу та масштабування (PTZ), може суттєво вплинути на ефективність системи спостереження. Ширококутні об'єктиви забезпечують ширше поле зору, що полегшує моніторинг великих площ або кількох точок входу. PTZ-камери, з іншого боку, пропонують гнучкість у налаштуванні положення камери та наближенні певних деталей, що покращує здатність системи відстежувати та фіксувати інциденти в режимі реального часу.

Оцінка варіантів технологій та обладнання

Камери – камери високої роздільної здатності необхідні для отримання чітких та детальних зображень, що забезпечують цінні докази у разі інцидентів безпеки. Вибираючи між IP- та аналоговими камерами, організації повинні враховувати такі фактори, як сумісність з мережею, масштабованість та якість зображення. IP-камери пропонують перевагу цифрового підключення, що дозволяє здійснювати віддалений доступ та легко інтегруватися з іншими системами безпеки. З іншого боку, аналогові камери можуть бути більш економічно ефективними для невеликих установок або районів з обмеженою мережевою інфраструктурою.

Окрім роздільної здатності та типу камери, використання розширених функцій, таких як тепловізор, може підвищити ефективність системи спостереження. Тепловізори можуть виявляти теплові сигнатури, забезпечуючи видимість у складних умовах освітлення або в середовищі з димом чи туманом. Завдяки впровадженню технології тепловізійного зображення організації можуть покращити можливості виявлення та забезпечити комплексне охоплення спостереженням, особливо на відкритому повітрі або в зонах високого ризику.

Зрештою, вибір між камерами високої роздільної здатності, IP або аналоговими, та додатковими функціями, такими як тепловізор, має бути адаптований до конкретних вимог безпеки та умов навколишнього середовища організації. Вибравши правильне поєднання обладнання та технологій, підприємства можуть оптимізувати продуктивність своєї системи відеоспостереження та покращити загальні заходи безпеки.

Нічне бачення та виявлення руху: Камери, оснащені технологією нічного бачення, є важливими для зйомки високоякісного відео в умовах слабого освітлення, гарантуючи, що критичні деталі не будуть пропущені навіть у найтемніших умовах. Ця функція особливо цінна для систем спостереження, яким потрібно підтримувати видимість у нічний час або в місцях з обмеженим освітленням. Крім того, можливості виявлення руху ще більше підвищують ефективність системи, заощаджуючи місце для зберігання. Записуючи лише тоді, коли виявлена активність, мінімізується непотрібний відеоматеріал, що полегшує співробітникам служби безпеки перегляд та аналіз відповідних подій.

Відеоаналітика: Інтеграція програмного забезпечення для відеоаналітики в систему спостереження виходить за рамки пасивного моніторингу, перетворюючи її на активний та інтелектуальний інструмент безпеки. Ця передова технологія може автоматично ідентифікувати та попереджати персонал служби безпеки про підозрілу поведінку, таку як байдкування, несанкціонований доступ або незвичайні рухи, значно підвищуючи загальну ефективність безпеки. Використовуючи можливості штучного інтелекту та машинного навчання, відеоаналітика може надавати аналітику та сповіщення в режимі реального часу, що дозволяє проактивно реагувати на потенційні загрози та інциденти. Ця трансформаційна функція не лише підвищує ефективність зусиль спостереження, але й допомагає оптимізувати розподіл ресурсів та час реагування для більш комплексної стратегії безпеки.

Рішення для зберігання даних

Вибираючи ідеальне рішення для зберігання даних для системи відеоспостереження підприємства, організації повинні ретельно враховувати свої конкретні вимоги до доступності, контролю та безпеки. Вибір між хмарним сховищем та локальними серверами може суттєво вплинути на загальну ефективність та результативність системи спостереження.

Хмарне сховище пропонує неперевершену гнучкість та зручність, дозволяючи співробітникам служби безпеки отримувати доступ до відеоматеріалів з будь-якого місця з підключенням до Інтернету. Така доступність особливо корисна для організацій з кількома об'єктами або для віддалених служб безпеки, яким потрібен доступ до даних спостереження в режимі реального часу. Крім того, хмарні рішення для зберігання даних часто мають вбудовані функції резервування та резервного копіювання, що гарантує безпеку критично важливих відеоматеріалів. З іншого боку, **локальні сервери** надають організаціям підвищений контроль над своїми даними та можуть запропонувати розширені заходи безпеки. Зберігаючи відеозаписи на місці, організації можуть гарантувати, що конфіденційна інформація залишається в їхніх фізичних приміщеннях, зменшуючи ризик несанкціонованого доступу або витоку даних. Хоча локальні сервери можуть вимагати більших початкових інвестицій та постійного обслуговування, вони забезпечують рівень контролю та безпеки, який є важливим для певних галузей та організацій із суворими вимогами до дотримання нормативних вимог. Вибір між хмарним сховищем та локальними серверами має ґрунтуватися на комплексній оцінці потреб організації, бюджетних обмежень та пріоритетів безпеки. Вибравши найбільш підходяще рішення для зберігання даних, організації можуть оптимізувати продуктивність своєї системи відеоспостереження та ефективно захистити свої активи, співробітників та клієнтів.

Підтримка та масштабованість

Забезпечення ефективності системи спостереження з часом вимагає регулярного технічного обслуговування та оновлень. Це включає не лише фізичне очищення та перевірку камер і обладнання, але й оновлення програмного забезпечення для підтримки функцій безпеки в актуальному стані.

Масштабованість має бути ключовим фактором з самого початку. У міру зростання організації система спостереження повинна мати можливість безперешкодно розширюватися. Це може включати додавання більшої кількості камер, модернізацію існуючих або інтеграцію передового аналітичного програмного забезпечення без капітального ремонту всієї системи.

Також важливо вибрати надійні та масштабовані рішення для зберігання відеоматеріалів. Хмарні сховища забезпечують гнучкість та доступність, а локальні сервери пропонують підвищений контроль та безпеку. Регулярне обслуговування та оновлення обладнання й технологій необхідні для забезпечення оптимальної продуктивності та надійності.

Створення успішної системи відеоспостереження для підприємства починається з розробки комплексної стратегії спостереження. Це більше, ніж просто розміщення камер у певних місцях; це вимагає стратегічного підходу до визначення зон та активів, які потребують моніторингу для посилення заходів безпеки. Ретельно оцінюючи приміщення, включаючи виявлення сліпих зон та вразливостей, організації можуть забезпечити надійність та ефективність своєї системи спостереження.

Окрім фізичного розміщення камер, встановлення чітких політик та процедур має вирішальне значення для безперебійної роботи системи спостереження. Це включає визначення ролей та обов'язків, встановлення інструкцій щодо доступу та управління відеоматеріалами, а також розробку протоколів реагування на інциденти безпеки. Наявність цих політик гарантує, що стратегія спостереження буде не тільки ефективною, але й відповідатиме правовим та нормативним вимогам.

По суті, добре розроблена стратегія спостереження служить проактивним заходом для захисту активів, співробітників та клієнтів організації. Вона формує міцну основу для моніторингу та реагування на загрози безпеці, підвищуючи загальну безпеку та душевний спокій. Інтегруючи технології спостереження з комплексною стратегією, організації можуть максимізувати переваги своєї системи відеоспостереження та створити безпечне середовище для всіх зацікавлених сторін.

Забезпечення конфіденційності даних та відповідності вимогам

Конфіденційність даних та дотримання вимог є вирішальними міркуваннями під час впровадження системи відеоспостереження на підприємстві. Оскільки організації використовують можливості технологій спостереження для посилення заходів безпеки, вони також повинні пріоритезувати захист прав осіб на конфіденційність та забезпечувати дотримання правових та нормативних актів.

Асоціація індустрії безпеки наголошує на важливості проведення оцінки впливу на конфіденційність (ОВК) на етапі проектування та планування систем спостереження. ОVK може виявити потенційні проблеми конфіденційності на ранній стадії, такі як зони спостереження з камер та використання аналітичного програмного забезпечення. Також важливо встановити налаштування конфіденційності за замовчуванням, безпечні конфігурації мережі та визначити ролі та обов'язки щодо конфіденційності та кібербезпеки.

Під час розгортання системи відеоспостереження організації повинні ретельно орієнтуватися в динамічному середовищі законів і норм щодо конфіденційності даних. Це включає дотримання правил, що регулюють збір, зберігання та використання відеоматеріалів, а також повагу до прав осіб на конфіденційність та захист даних. Дотримуючись цих стандартів, організації можуть побудувати довіру зі співробітниками, клієнтами та іншими зацікавленими сторонами, одночасно зменшуючи ризики потенційних юридичних наслідків.

Крім того, для організацій важливо запровадити надійні та комплексні практики управління даними для захисту цілісності та конфіденційності відеозаписів. Це включає впровадження безпечних рішень для зберігання даних, протоколів шифрування, засобів контролю доступу та політик зберігання даних для запобігання несанкціонованому доступу або зловживанню конфіденційною інформацією. Завдяки проактивному вирішенню проблем конфіденційності даних, таких як Загальний регламент про захист даних (GDPR) або галузеві рекомендації, організації можуть дотримуватися етичних стандартів та захищати права осіб, записаних камерами спостереження.

Навчання та моніторинг персоналу служби безпеки з використання систем відеоспостереження

Навчання та моніторинг персоналу служби безпеки є важливими практиками для забезпечення ефективної роботи системи відеоспостереження підприємства. Важливість комплексного навчання персоналу служби безпеки неможливо переоцінити, оскільки це не лише підвищує їхню кваліфікацію та авторитет, але й відіграє значну роль у мінімізації відповідальності та підвищенні загальної безпеки організації. Належним чином навчений персонал служби безпеки краще оснащений для вирішення різних ситуацій, що позитивно відображається на його професіоналізмі та відданості організації питанням безпеки. Такі програми, як ті, що пропонуються Міжнародним фондом співробітників служби безпеки (IFPO), охоплюють широкий спектр тем, важливих для співробітників служби безпеки, включаючи фізичну безпеку, процедури дій у надзвичайних ситуаціях, правові аспекти тощо, гарантуючи, що співробітники добре підготовлені до виконання своїх обов'язків.

Більше того, Бюро статистики праці США підкреслює різноманітні ролі та обов'язки охоронців та співробітників служби спостереження за азартними іграми, наголошуючи на необхідності ретельного навчання та набуття спеціальних навичок для ефективного виконання своїх обов'язків. Навчальні заняття повинні бути зосереджені на ознайомленні персоналу служби безпеки з різними функціями та можливостями системи спостереження, включаючи те, як керувати камерами, отримувати доступ до записів та реагувати на інциденти безпеки. Крім того, персонал слід навчити найкращим практикам обслуговування системи, таким як регулярні перевірки несправностей камер та забезпечення безпеки даних.

Надаючи пріоритет навчанню та моніторингу персоналу служби безпеки, організації можуть забезпечити ефективне та відповідальне використання своїх систем спостереження, сприяючи безпеці своїх приміщень, а також дотримуючись правил конфіденційності та відповідності.

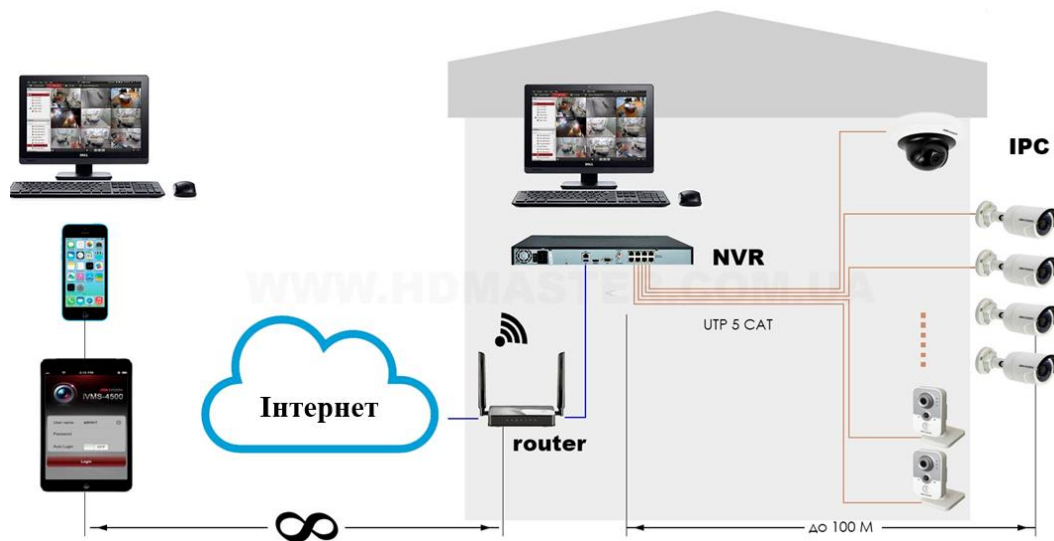


Рисунок 1 – Структурна схема системи

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів мережевого відеоспостереження для реалізації стратегії забезпечення безпеки підприємства. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем мережевого відеоспостереження для реалізації стратегії забезпечення безпеки підприємства.
- Досліджена система мережевого відеоспостереження для реалізації стратегії забезпечення безпеки підприємства.
- На основі отриманих результатів досліджень створена програмна реалізація системи мережевого відеоспостереження для реалізації стратегії забезпечення безпеки підприємства. Розроблені алгоритми дозволяють успішно вирішувати завдання мережевого відеоспостереження для реалізації стратегії забезпечення безпеки підприємства. 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., 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.
2. 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.
3. 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.
4. Smirnov, O., Neskoriadiyeva, T., Fedorov, E., Rudakov, K., Neskoriadiyeva, A. «Method Detection Audit Data Anomalies on Basis Restricted Cauchy Machine» CEUR Workshop Proceedings, Volume 3187, 2022,
5. 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.
6. 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>
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., 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.
10. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
11. 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.
12. 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.
13. 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.
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., 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., Gorbacheva, L., Babenko, V., «Hiding data in images using a pseudo-random sequence», CEUR Workshop Proceedings Volume 2608, 2020, Pages 646-660.
19. 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.
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., 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., 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. 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.
29. Т.В. Смірнова, О.М. Дреєв, О.А. Смірнов «Хмарна інформаційна система оцінювання шорсткості з використанням дискретного частотного аналізу макrofототграфій». IV міжнародна науково-практична конференція «Інформаційна безпека та комп'ютерні технології», м. Кропивницький. 15-16 квітня 2021р. – Кропивницький: ЦНТУ. – 2021. – С. 30.
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. 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.
32. Смірнов О.А., Дреєва Г.М., Дреєв О.М., Смірнова Т.В. «Фрактальний аналіз генератора самоподібного трафіку на основі ланцюга Маркова». Центральньоукраїнський науковий вісник. Технічні науки. № 2(33). с. 161-172, 2019.
33. 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.

УДК 004

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

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ПОВЕДІНКОВОГО АНАЛІЗУ КОРИСТУВАЧІВ ЗА ДОПОМОГОЮ КОНЦЕПЦІЇ UEBA

У статті розроблено програмне забезпечення, яке призначено для системи поведінкового аналізу користувачів за допомогою концепції UEBA. Метою розробки є дослідження та принципи побудови системи поведінкового аналізу користувачів за допомогою концепції UEBA. Об'єктом дослідження є процес поведінкового аналізу користувачів за допомогою концепції UEBA. Предметом дослідження є методи поведінкового аналізу користувачів за допомогою концепції UEBA. Методи дослідження базуються на методах машинного навчання, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи поведінкового аналізу користувачів за допомогою концепції UEBA. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

поведінковий аналіз користувачів, UEBA

Постановка проблеми. UEBA, що розшифровується як User and Entity Behavior Analytics (аналіз поведінки користувачів та сутностей), – це технологія кібербезпеки, яка аналізує поведінку користувачів та сутностей для виявлення аномальної та потенційно шкідливої діяльності. Вона виходить за рамки традиційних заходів безпеки, зосереджуючись на моделях поведінки, а не лише на відомих загрозах, використовуючи машинне навчання та розширену аналітику для виявлення відхилень від звичайної активності. Це допомагає організаціям виявляти внутрішні загрози, скомпрометовані облікові дані та інші складні атаки.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи поведінкового аналізу користувачів за допомогою концепції UEBA.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи поведінкового аналізу користувачів за допомогою концепції UEBA.

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

- Огляд існуючих систем поведінкового аналізу користувачів за допомогою концепції UEBA.
- Дослідження системи поведінкового аналізу користувачів за допомогою концепції UEBA.
- Програмна реалізація системи поведінкового аналізу користувачів за допомогою концепції UEBA.

Об'єктом дослідження є процес поведінкового аналізу користувачів за допомогою концепції UEBA.

Предметом дослідження є методи поведінкового аналізу користувачів за допомогою концепції UEBA.

Методи дослідження базуються на методах машинного навчання, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Ключові характеристики інструментів UEBA

Хоча UEBA як категорія безпеки зараз часто вписується в рамки більших платформ, кілька ключових можливостей є однаковими для всієї галузі. Основні функції UEBA включають моніторинг інфраструктури, аналітику, сповіщення та керування користувачами.

Моніторинг

В інфраструктурі безпеки мережі, пристрої та програми повинні контролюватися. Інструменти UEBA постійно спостерігають за ІТ-системами та повідомляють адміністраторів, коли мережевий трафік та поведінка пристроїв або програм не відповідають попередньо налаштованим стандартам.

Аналітика

У рішеннях UEBA поведінкова аналітика базується на технології машинного навчання. ML ідентифікує поведінку користувачів, щоб визначити, чи відповідає вона заздалегідь визначеним критеріям типових дій. Якщо інструмент UEBA вирішує, що нестабільна поведінка користувача є небезпечною, він виділяє цю закономірність на панелі інструментів, щоб адміністратори безпеки могли її переглянути.

Сповіщення та пріоритетність

Інструменти UEBA запускають сповіщення, коли виникає достатньо значна аномалія. Оскільки ці інструменти вивчають типові моделі поведінки користувачів і програм протягом певного часу, вони помічають, коли відбувається щось неочікуване. Інструменти UEBA часто надають пріоритет сповіщенням – ранжуючи рівень ризику, щоб ІТ-персонал та співробітники служби безпеки могли вирішити, з чим боротися в першу чергу.

Керування користувачами та об'єктами

Рішення UEBA контролюють дозволи користувачів і визначають, чи суперечить поведінка певного користувача призначеним йому правам. Це допомагає зменшити використання привілейованого доступу, а також може виявити зловмисну інсайдерську діяльність. Рішення UEBA також часто контролюють об'єкти або активи, такі як ноутбуки чи сервери, щоб визначити, чи є їхня поведінка аномальною та чи потребує карантину або вимкнення.

Розширена ідентифікація загроз

Коли інструменти UEBA моніторять системи та виявляють аномалії, вони часто визначають, який саме тип проблеми виникає. До них належать такі загрози, як горизонтальне переміщення та витік даних, а рішення UEBA також можуть повідомити вам, чи є загроза внутрішньою чи зовнішньою по відношенню до вашої організації. Ця інформація корисна для боротьби зі зловмисниками, особливо якщо це ваші власні співробітники.

Основна функція UEBA включає:

- Поведінковий аналіз: Системи UEBA аналізують поведінку користувачів та сутностей, включаючи такі дії, як спроби входу, доступ до файлів, мережевий трафік та використання програм.
- Виявлення аномалій: встановлює базовий рівень нормальної поведінки для кожного користувача та сутності, а потім позначає відхилення від цього базового рівня як потенційні загрози.
- Машинне навчання: UEBA використовує алгоритми машинного навчання для виявлення тонких закономірностей та аномалій, які можуть бути пропущені традиційними методами безпеки.

Ключові переваги включають:

- Покращене виявлення загроз: UEBA може виявляти ширший спектр загроз, включаючи внутрішні загрози, скомпрометовані облікові записи та розширені постійні загрози (APT).
- Покращений рівень безпеки: Завдяки проактивному виявленню підозрілої активності, UEBA допомагає організаціям покращити загальний рівень безпеки та зменшити ризик витоків даних.

– Зменшення кількості хибних спрацьовувань: здатність UEBA аналізувати контекст і поведінку допомагає мінімізувати кількість хибних спрацьовувань, дозволяючи командам безпеки зосередитися на справжніх загрозах.

– Швидше реагування на інциденти: Завдяки швидкому виявленню та сповіщенню про аномальну поведінку, UEBA забезпечує швидше реагування на інциденти та їх локалізацію.

– Повна видимість: UEBA надає повне уявлення про активність користувачів та організацій, допомагаючи організаціям зрозуміти, як використовуються їхні системи, та виявити потенційні слабкі місця в безпеці.

Інструменти UEBA використовують інноваційні алгоритми, засновані на традиційному машинному навчанні та глибокому навчанні, для виявлення аномальної та ризикованої поведінки користувачів, машин та інших об'єктів у корпоративній мережі, часто у поєднанні з рішенням для управління інцидентами та подіями безпеки (SIEM).

Зростаюча потреба в UEBA: внутрішні ризики перевищують зовнішні загрози

Згідно з нашим нещодавнім звітом «Від людини до гібрида: як штучний інтелект та розрив в аналітиці підживлюють внутрішні ризики», внутрішні ризики вже перевершили зовнішні загрози як головну проблему для команд безпеки. У нашому опитуванні 64% фахівців з кібербезпеки визначили зловмисних або скомпрометованих інсайдерів як більшу небезпеку, ніж зовнішніх нападників, порівняно з 36%, які вказали на зовнішніх суб'єктів.

З цих 64% 42% вважали зловмисних інсайдерів основною проблемою, а 22% – скомпрометованих інсайдерів. Понад половина (53%) повідомила, що кількість інсайдерських інцидентів зросла за останній рік, а 54% очікують, що їхня кількість зростатиме ще більше протягом наступних 12 місяців.

Можливості виявлення залишаються недостатньо розвиненими. Лише 44% організацій використовують аналітику поведінки користувачів та об'єктів (UEBA), яка є критично важливою для виявлення аномальної активності. Хоча 88% кажуть, що мають програму боротьби з внутрішніми загрозами, багато з них є неформальними, недостатньо фінансованими або мають недостатню прозорість у системах. Узгодженість керівництва також є прогалиною: 74% фахівців з безпеки вважають, що керівники недооцінюють внутрішні ризики.

Генеративний штучний інтелект (ШІ) посилює проблему. 76% організацій стикалися з несанкціонованим використанням інструментів GenAI співробітниками. Фішинг та соціальна інженерія за допомогою ШІ (27%), а також несанкціоноване використання GenAI (22%) входять до числа основних векторів внутрішніх загроз, поряд із зловживанням привілеями (18%).

Керівники служб безпеки визнають необхідність кращого аналізу поведінки, але стикаються з технічними та організаційними перешкодами. Опір конфіденційності (20%), відсутність прозорості (16%) та фрагментовані інструменти (10%) створюють сліпі зони у зусиллях з виявлення.

Як працює UEBA

Аналіз поведінки користувачів та сутностей (UEBA) – це категорія рішень або можливостей кібербезпеки, які аналізують поведінку користувачів та сутностей і застосовують розширену аналітику та моделювання поведінки для визначення аномальної поведінки. UEBA використовується для виявлення розширених загроз безпеці, таких як зловмисні інсайдери та компрометація привілейованих облікових записів, які традиційні інструменти безпеки на основі правил не можуть побачити. Рішення UEBA отримують операційні дані з багатьох джерел та визначають, яка нормальна поведінка будь-якого користувача або нелюдської сутності. Суб'єкти можуть включати ІТ-активи, такі як хости, програми, мережевий трафік, облікові записи служб та сховища даних. З часом рішення створює стандартні профілі поведінки для користувачів та сутностей у різних групах рівних, щоб створити базовий рівень для того, що є нормальним в організації. Коли виявляється

аномальна активність, їй присвоюється оцінка ризику. Оцінка зростає зі збільшенням кількості аномальної поведінки, доки вона не перетне визначений поріг, що спрацьовує для аналітиків безпеки. Деякі рішення можуть автоматизувати дії реагування.

Ось більш детальний огляд основної функції UEBA:

– Машинне навчання: UEBA застосовує методи машинного навчання з вчителем та без вчителя для виявлення ледь помітних аномалій, які статичні правила не можуть вловлювати. Алгоритми можуть адаптуватися до зміни поведінки користувача, зменшуючи потребу в постійних ручних оновленнях. Це дозволяє системі виявляти приховані моделі атак, такі як повільне витікання даних або зловживання привілеями, які розгортаються поступово та в іншому випадку могли б уникнути виявлення.

– Поведінковий аналіз: UEBA збирає та зіставляє дані з кількох джерел, таких як журнали автентифікації, файлові системи, електронна пошта та хмарні додатки, для створення комплексного уявлення про активність. Він відстежує не лише окремі події, а й послідовності дій з плином часу, що дозволяє виявляти незвичайні робочі процеси, спроби доступу або моделі використання, які можуть свідчити про неправильне використання або компрометацію.

– Виявлення аномалій: Після встановлення профілів нормальної поведінки UEBA постійно порівнює нову активність з цими базовими показниками. Відхилення, такі як спроби входу з незвичайних місць, надмірне завантаження файлів або неочікуваний доступ до конфіденційних ресурсів, позначаються. Система призначає контекст цим аномаліям, допомагаючи аналітикам розрізняти нешкідливі відхилення та справжні загрози.

Цілісний аналіз з використанням кількох джерел даних

Справжня сила рішення UEBA полягає в його здатності долати організаційні кордони, ІТ-системи та джерела даних й аналізувати всі дані, доступні для конкретного користувача чи організації.

Рішення UEBA повинно аналізувати якомога більше джерел даних, деякі приклади джерел даних включають:

- Системи автентифікації, такі як Active Directory.
- Системи доступу, такі як VPN та проксі-сервери.
- Бази даних керування конфігурацією.
- Дані про людські ресурси – нові співробітники, співробітники, що звільнилися, та будь-які дані, що надають додатковий контекст про користувачів.
- Брандмауер, системи виявлення та запобігання вторгненням (IDPS).
- Антивірусні та антивірусні системи.
- Системи виявлення та реагування на кінцеві точки.
- Аналіз мережевого трафіку.
- Стрічки інформації про загрози.

Наприклад, рішення UEBA повинно мати можливість ідентифікувати незвичний вхід через Active Directory, зіставляти його з критичністю пристрою, на який здійснюється вхід, конфіденційністю файлів, до яких здійснювався доступ, та нещодавною незвичайною мережевою або шкідливою активністю, яка могла призвести до компрометації.

Поведінкове базове дослідження та оцінки ризику

Рішення UEBA вивчає нормальну поведінку, щоб виявити аномальну. Воно аналізує широкий набір даних, щоб визначити базовий або поведінковий профіль користувача.

Наприклад, система відстежує користувача та бачить, як він використовує VPN, о котрій годині приходить на роботу та в які системи входить, який принтер використовує, як часто та якого розміру файли надсилає електронною поштою або завантажує на USB-накопичувач, а також багато інших даних, що визначають «нормальну поведінку» користувача. Те саме стосується серверів, баз даних або будь-якої значної ІТ-системи.

Коли відбувається відхилення від базового рівня, система додає до оцінки ризику цього користувача або машини. Чим незвичайніша поведінка, тим вищий бал ризику. Зі збільшенням кількості підозрілих випадків накопичення бал ризику збільшується, доки не досягне певного порогу, що призводить до передачі інформації аналітику для розслідування.

Такий аналітичний підхід має кілька переваг:

- Агрегація – оцінка ризику складається з численних подій, тому аналітикам не потрібно вручну переглядати велику кількість окремих сповіщень та подумки об'єднувати їх для виявлення загрози.

- Зменшення кількості хибнопозитивних результатів – одна незначна аномальна подія сама по собі не призведе до спрацювання сповіщення системи безпеки. Для створення сповіщення системі потрібні кілька ознак аномальної поведінки, що зменшує кількість хибнопозитивних результатів та заощаджує час аналітиків.

Більше контексту – традиційні правила кореляції, визначені адміністраторами безпеки, могли бути правильними для однієї групи користувачів або систем, але не для інших. Наприклад, якщо відділ починає наймати працівників, що працюють позмінно, або працівників, що працюють за кордоном, вони почнуть входити в систему в незвичний час, що постійно призводитиме до спрацювання сповіщень на основі правил. UEBA розумніша, оскільки встановлює контекстно-залежний базовий рівень для кожної групи користувачів. Вхід працівника, що працює за кордоном, о 3:00 ранку за місцевим часом не вважатиметься аномальною подією.

Аналіз часової шкали та зшивання сесій

Під час аналізу інцидентів безпеки часова шкала є критично важливим поняттям, яке може пов'язати, здавалося б, не пов'язані між собою дії. Сучасні атаки – це процеси, а не ізольовані події.

Передові рішення UEBA можуть «зшивати» дані з різних систем та потоків подій, щоб побудувати повну часову шкалу інциденту безпеки.

Наприклад, розглянемо користувача, який увійшов у систему, виконав підозрілу активність, а потім зник із журналів. Чи була та сама IP-адреса використана для підключення до інших організаційних систем невдовзі після цього? Якщо так, це може бути частиною того самого інциденту, коли той самий користувач продовжував спроби проникнення в систему. Додатковим прикладом може бути вхід злоумисника в систему на одному комп'ютері кілька разів, використовуючи різні облікові дані. Це також вимагає «зшивання» даних про різні спроби входу та позначення їх як одного інциденту.

Після того, як рішення UEBA об'єднає всі відповідні дані, воно може призначити оцінки ризику будь-якій діяльності вздовж часової шкали події. Засвоюється нормальна поведінка для всіх користувачів і машин. Оцінка ризику додається для високоризикової та аномальної поведінки.

Внутрішні загрози

Існує три типи внутрішніх загроз:

1. Недбалий інсайдер – недбалий інсайдер – це працівник або підрядник із привілейованим доступом до ІТ-систем, який ненавмисно наражає свою організацію на небезпеку, не дотримуючись належних ІТ-процедур. Наприклад, той, хто залишає свій комп'ютер, не вийшовши з системи, або адміністратор, який не змінив пароль за замовчуванням або не встановив патч безпеки. Визначення нормальної та аномальної активності користувача є ключовим для виявлення користувача, який був скомпрометований через недбалість.

2. Зловмисний інсайдер – Зловмисний інсайдер – це співробітник або підрядник із привілейованим доступом до ІТ-систем, який має намір здійснити кібератаку на організацію. Важко виміряти зловмисний намір або виявити його за допомогою лог-файлів або регулярних подій безпеки. Рішення UEBA допомагають, встановлюючи базову лінію типової поведінки користувача та виявляючи аномальну активність.

3. Скомпрометований інсайдер – Зловмисники часто проникають в організацію та компрометують обліковий запис привілейованого користувача або довірений хост у мережі, а потім продовжують атаку звідти. Рішення UEBA можуть допомогти швидко виявити та проаналізувати шкідливу діяльність, яку зловмисник здійснює через скомпрометований обліковий запис.

Традиційним засобам безпеки важко виявити скомпрометованого інсайдера, якщо схема атаки або ланцюжок знищення наразі невідомі (наприклад, під час атаки нульового дня), або якщо атака поширюється латерально через організацію, змінюючи облікові дані, IP-адреси або машини. Однак технологія UEBA може виявляти ці типи атак, оскільки вони майже завжди змушують активи поводитися інакше, ніж встановлені базові показники.

Пріоритетність інцидентів

SIEM збирає події та журнали з кількох інструментів безпеки та критично важливих систем, а також генерує велику кількість сповіщень, які мають розслідувати співробітники служби безпеки. Це призводить до втоми від сповіщень, що є поширеною проблемою Центрів операцій безпеки (SOC).

Рішення UEBA можуть допомогти зрозуміти, які інциденти є особливо ненормальними, підозрілими або потенційно небезпечними в контексті вашої організації. UEBA може вийти за рамки базових показників та моделей загроз, додаючи дані про організаційну структуру, наприклад, критичність активів, ролі та рівні доступу до певних функцій організації. Невелике відхилення від норми для критично захищеної системи або адміністратора вищого рівня може бути вартим уваги для слідчого; для звичайного співробітника лише значне відхилення отримає високий пріоритет.

Запобігання втраті даних (DLP) та запобігання витоку даних

Інструменти запобігання втраті даних (DLP) використовуються для запобігання витоку даних або незаконній передачі даних за межі організації. Традиційні інструменти DLP повідомляють про будь-яку незвичайну активність, що здійснюється з конфіденційними даними, – вони створюють велику кількість сповіщень, з якими може бути важко впоратися командам безпеки.

Рішення UEBA можуть приймати сповіщення DLP, визначати їх пріоритети та консолідувати, розуміючи, які події являють собою аномальну поведінку порівняно з відомими базовими показниками. Це заощаджує час слідчим та допомагає їм швидше виявляти реальні інциденти безпеки.

Аналітика сутностей (IoT)

UEBA може бути особливо важливим у боротьбі з ризиками безпеки Інтернету речей (IoT). Організації розгортають великі парки підключених пристроїв, часто з мінімальними заходами безпеки або без них. Зловмисники можуть скомпрометувати пристрої IoT, використовувати їх для крадіжки даних або отримання доступу до інших IT-систем, або, що ще гірше, використовувати їх для DDoS-атаки чи інших атак на третіх осіб.

Дві чутливі категорії Інтернету речей – це медичні прилади та виробниче обладнання. Підключені медичні прилади можуть містити критично важливі дані та можуть становити загрозу для життя, якщо їх використовувати безпосередньо для догляду за пацієнтами. Виробниче обладнання може спричинити великі фінансові втрати у разі його збою, а в деяких випадках може загрожувати безпеці працівників.

UEBA може відстежувати підключені пристрої, встановлювати базову поведінку для кожного пристрою або групи подібних пристроїв і негайно виявляти, чи пристрій поводить себе поза межами своїх звичайних меж. Наприклад:

- Підключення до або з незвичайних адрес чи пристроїв.
- Активність у незвичний час.
- Активовані функції пристрою, які зазвичай не використовуються.

Конвергенція UEBA та SIEM

Існує тісний зв'язок між технологіями UEBA та SIEM, оскільки UEBA спирається на міжорганізаційні дані безпеки для виконання свого аналізу, і ці дані зазвичай збираються та зберігаються SIEM.

Gartner розглядає UEBA як функцію, інтегровану в SIEM. Аналіз поведінки – це одна з можливостей, за допомогою якої Gartner оцінює постачальників у Магічному квадранті для управління інформацією та подіями безпеки. Gartner окреслює такі можливості для SIEM:

- Сукупні дані про події, що генеруються пристроями безпеки, мережевою інфраструктурою, системами та програмами.
- Поєднуйте дані про події з контекстною інформацією про користувачів, активи, загрози та вразливості з метою оцінювання, визначення пріоритетів та пришвидшення розслідувань.
- Нормалізуйте дані для ефективнішого аналізу.
- Пропонуйте аналіз подій у режимі реального часу для моніторингу безпеки, розширений аналіз поведінки користувачів та об'єктів, аналітику запитів, підтримку розслідування та управління інцидентами, а також звітність.

UEBA проти аналогічних технологій

UEBA проти NTA

Аналіз мережевого трафіку (NTA) зосереджений на моніторингу та аналізі мережевого зв'язку для виявлення аномалій або ознак компрометації. Хоча UEBA та NTA виявляють аномальну поведінку, їхні області застосування відрізняються.

UEBA досліджує поведінку користувачів та об'єктів у різних системах, включаючи кінцеві точки, програми та каталоги, а не лише мережеву активність. NTA обмежується мережевими даними та чудово справляється з виявленням таких загроз, як горизонтальне переміщення та витік даних. Натомість UEBA може виявляти загрози, пов'язані з зловживанням привілейованим доступом, незвичайною поведінкою під час входу або змінами в шаблонах доступу до файлів. NTA зазвичай підтримує аналіз трафіку в режимі реального часу, тоді як UEBA працює як з даними в реальному часі, так і з історичними даними для довгострокового моделювання поведінки.

Разом UEBA та NTA можуть доповнювати один одного: NTA виділяє підозрілі мережеві шляхи, тоді як UEBA надає поведінковий контекст щодо того, хто або що задіяно.

UBA проти UEBA

Аналітика поведінки користувачів (UBA) – це попереднє покоління технологій, орієнтованих виключно на користувачів-людей. Вона аналізує поведінку користувачів для виявлення таких ризиків, як неправомірне використання облікових даних, внутрішні загрози або підозрілі моделі доступу.

UEBA (аналітика поведінки користувачів та об'єктів) розширює цю концепцію, включаючи нелюдські об'єкти, такі як сервери, програми та пристрої Інтернету речей. Цей ширший охоплення є критично важливим, оскільки багато атак спрямовані на об'єкти, що не є користувачами-людьми, або походять від них. UEBA також зазвичай включає більш просунуту аналітику, таку як моделі машинного навчання, здатні виявляти складні поведінкові аномалії в гібридних середовищах.

Коротше кажучи, UEBA базується на UBA, надаючи більш повне уявлення про всі сутності в IT-середовищі та взаємозв'язки між ними.

Методи аналітики UEBA

Деякі рішення UEBA покладаються на традиційні методи виявлення підозрілої активності. До них можуть належати правила, визначені вручну, кореляції між подіями безпеки та відомими шаблонами атак. Обмеження традиційних методів полягає в тому, що вони ефективні лише настільки, наскільки ефективні правила, визначені адміністраторами безпеки, і не можуть адаптуватися до нових типів загроз або поведінки системи.

Розширена аналітика включає кілька сучасних технологій, які можуть допомогти виявити аномальну поведінку навіть за відсутності відомих закономірностей:

- Машинне навчання з вчителем – набори відомої хорошої та відомої поганої поведінки подаються в систему. Інструмент навчається аналізувати нову поведінку та визначати, чи є вона «схожою» на набір відомої хорошої чи відомої поганої поведінки.

- Баєсівські мережі – можуть поєднувати машинне навчання з вчителем та правила для створення поведінкових профілів.

- Самонавчання – система вивчає нормальну поведінку та здатна виявляти аномальну поведінку й попереджати про неї. Вона не зможе визначити, чи є аномальна поведінка хорошою чи поганою, лише те, що вона відхиляється від норми.

- Підсилене/напівавторизоване машинне навчання – гібридна модель, де основою є навчання без вчителя, а фактичні рішення щодо сповіщень передаються назад у систему, щоб забезпечити точне налаштування моделі та зменшити співвідношення сигнал/шум.

- Глибоке навчання – дозволяє проводити віртуальне сортування та розслідування тривог. Система навчається на наборах даних, що представляють тривоги безпеки та їх результати сортування, виконує самоідентифікацію ознак та здатна прогнозувати результати сортування для нових наборів тривог безпеки.

Традиційні методи аналітики є детермінованими в тому сенсі, що якщо певні умови були виконані, генерувалося сповіщення, а якщо ні, система вважала, що «все гаразд». Розширені методи аналітики, перелічені вище, відрізняються тим, що вони є евристичними. Вони обчислюють оцінку ризику, яка є ймовірністю того, що подія являє собою аномалію або інцидент безпеки. Коли оцінка ризику перевищує певний поріг, система створює сповіщення безпеки.

Проблеми розгортання UEBA

Інтеграція та масштабування даних

Однією з головних проблем розгортання UEBA є інтеграція різноманітних джерел даних. Системи UEBA покладаються на комплексні, високоякісні дані із систем керування ідентифікацією, журналів програм, мережевого трафіку, телеметрії кінцевих точок тощо. Інтеграція цих джерел – часто в різних форматах і обсягах – може бути складною та трудомісткою.

Масштабованість – ще одна проблема. Зі зростанням організацій та додаванням нових пристроїв, програм і користувачів обсяг даних зростає експоненціально. Рішення UEBA повинні обробляти ці дані майже в режимі реального часу, зберігаючи при цьому продуктивність. Без належного планування вузькі місця в продуктивності та збільшена затримка можуть погіршити можливості виявлення та робочі процеси аналітиків.

Хибнопозитивні результати

Незважаючи на розширену аналітику, хибнопозитивні результати залишаються значною проблемою в розгортанні UEBA. Якщо система генерує забагато сповіщень про нешкідливі аномалії, такі як робота легітимного користувача з нового місця розташування, аналітики безпеки можуть бути перевантажені або втратити чутливість.

Ця проблема часто пов'язана з незрілим базовим підходом або недостатнім контекстом у моделях поведінки. З часом, коли система навчається та налаштовує оцінку ризиків, кількість хибнопозитивних результатів може зменшитися. Однак на ранніх етапах розгортання або в динамічних середовищах підтримувати прийнятну якість сповіщень може бути складно.

Вимоги до навичок та ресурсів

Платформи UEBA потребують кваліфікованого персоналу для конфігурації, налаштування та обслуговування. Організаціям потрібні аналітики зі знаннями поведінкової аналітики, виявлення загроз та реагування на інциденти. Крім того, можуть знадобитися інженери обробки даних, щоб забезпечити належне отримання та нормалізацію даних. Меншим організаціям може бракувати досвіду або кількості персоналу для підтримки

повномасштабного впровадження UEBA. Навіть для великих підприємств інтеграція UEBA в існуючі операції безпеки може вимагати значних часових витрат та постійних зусиль для підтримки точності та ефективності моделей.

Ключові найкращі практики впровадження UEBA

1. Забезпечення комплексної та високоякісної інтеграції даних

Системи UEBA покладаються на багаті, різноманітні дані для точного моделювання поведінки. Почніть з визначення ключових джерел даних від постачальників ідентифікації (наприклад, Active Directory, LDAP), журналів кінцевих точок, хмарних додатків, VPN, проксі-серверів та мережевого трафіку. Отримуйте як структуровані, так і неструктуровані дані для створення повних профілів поведінки.

Використовуйте конектори, API або відправники журналів для автоматизації збору даних та забезпечення узгодженої синхронізації часу між джерелами – розбіжності в часі можуть перешкоджати точному аналізу часової шкали. Інвестуйте в процеси нормалізації та збагачення даних, щоб стандартизувати формати, вирішувати неоднозначності та позначати відповідні метадані, такі як ролі користувачів або класифікації активів.

Високоякісні дані – це не просто технічна вимога, вони є основоположними для здатності UEBA генерувати змістовні та практичні висновки. Низька якість даних призводить до спотворення базових показників, неефективного виявлення аномалій та збільшення кількості хибнопозитивних результатів.

2. Встановлення надійних базових показників поведінки

Ефективність UEBA залежить від сили її поведінкових моделей. Почніть з надання системі періоду спостереження – зазвичай кілька тижнів – протягом якого вона відстежує активність без попереджень. Протягом цього періоду система встановлює базові показники для користувачів та об'єктів, вивчаючи моделі використання, час доступу, мережеву взаємодію та поведінку системи.

Для більшої точності базові показники повинні враховувати взаємодію з колегами, включаючи порівняння поведінки користувачів, які виконують схожі ролі або мають схожі системи в одній операційній категорії. Врахування організаційного контексту, такого як відділ або місцезнаходження, допомагає адаптувати базові показники та запобігти неправильній класифікації. Регулярно переглядайте та вдосконалюйте ці базові показники. Якщо бізнес-операції змінюються, наприклад, додавання віддалених команд або сезонний сплеск активності, переконайтеся, що система адаптується. Статичні базові показники в динамічному середовищі призводять до появи сліпих зон або втоми від оповіщень.

3. Ретельно налаштуйте порогові значення та оцінку ризику

Не всі аномалії заслуговують на однакову стурбованість. Системи UEBA використовують оцінки ризику для оцінки серйозності відхилень, але їх необхідно ретельно калібрувати. Почніть з консервативних порогових значень, щоб уникнути перевантаження аналітиків, і коригуйте їх на основі оперативного зворотного зв'язку та аналізу інцидентів.

Оцінка ризику повинна враховувати частоту аномалій, їх серйозність та критичність для ураженої системи чи користувача. Наприклад, незвичайний вхід адміністратора на цінний сервер повинен мати більшу вагу, ніж така сама дія на звичайній робочій станції.

Використовуйте динамічні порогові значення, де це можливо – адаптивні системи, які з часом вивчають прийнятну дисперсію, можуть забезпечити більш нюансовані сповіщення. Також визначте шляхи ескалації та автоматизуйте дії реагування на події з високою достовірністю та високим ризиком, щоб пришвидшити пом'якшення наслідків.

4. Збагачуйте сповіщення контекстом та інформацією про загрози

Контекст є важливим для скорочення часу сортування та покращення прийняття рішень. Збагачуйте сповіщення метаданими з HR-систем (наприклад, статус зайнятості, відділ), інвентаризації активів (наприклад, критичність системи) та історичних моделей поведінки. Включайте такі деталі, як час входу, ідентифікатори пристроїв, геолокацію та журнали доступу до даних.



Рисунок 1 – Структурна схема системи

Інтегруйте канали аналітики загроз для зіставлення аномалій з відомими індикаторами компрометації (ІОС) або тактиками, методами та процедурами зловмисників (TTP). Це допомагає розрізняти випадкові аномалії та цілеспрямовані загрози.

Представляйте збагачені сповіщення у зручному для аналітиків форматі, пов'язуючи їх із відповідними подіями в ланцюжку атаки. Це мінімізує час ручного розслідування та покращує якість дій реагування.

5. Інтеграція відповідно до стеку безпеки та робочих процесів

Щоб максимізувати цінність, UEBA має працювати в рамках ширшої екосистеми безпеки. Інтегруватися з платформами SIEM для використання існуючих можливостей збору та кореляції журналів. Передавати оцінки ризиків та сповіщення в системи SOAR, щоб забезпечити автоматизоване виконання сценаріїв, таких як ізоляція пристроїв або скидання облікових даних.

Забезпечте відповідність результатів UEBA вашим існуючим робочим процесам реагування на інциденти, системам видачі заявок та панелям звітності. Це забезпечує безперешкодну передачу між групами виявлення та розслідування та уникає дублювання зусиль.

Ретельно протестуйте інтеграції – системи UEBA повинні не лише надавати точні сповіщення, а й відповідати операційним реаліям. Обсяг сповіщень, час реагування та зручність використання так само важливі, як і точність виявлення. Прагніть до тісно

пов'язаної архітектури, де поведінкова аналітика стає природною частиною життєвого циклу ваших операцій безпеки.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів поведінкового аналізу користувачів за допомогою концепції UEBA. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем поведінкового аналізу користувачів за допомогою концепції UEBA.
- Досліджена система поведінкового аналізу користувачів за допомогою концепції UEBA.
- На основі отриманих результатів досліджень створена програмна реалізація системи поведінкового аналізу користувачів за допомогою концепції UEBA.

Розроблені алгоритми дозволяють успішно вирішувати завдання поведінкового аналізу користувачів за допомогою концепції UEBA. 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. 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.
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. Akhalaia, G., Iavich, M., Iashvili, G., Prysiazhnyy, D., Smirnova, T. «Secure Encrypted Connection on Georgian Website». CEUR Workshop Proceedings, 2023, 3550, pp. 313-320.
6. 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
7. 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.
8. 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.
9. 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.
10. 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.
11. 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.
12. 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.
13. 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.

14. 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.
15. 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,
16. 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.
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 ґешування 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 ґешування 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 ґешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 1(67). С. 84-89.
21. 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
22. 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.
23. 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.
24. 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.
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., 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., Arischenko A., Chepurko I., Onikiychuk A., Kuznetsova T. «Pseudorandom sequences for spread spectrum image steganography». CEUR Workshop Proceedings Volume 2654, 2020, Pages 122-131.
29. 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.
30. 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.
31. 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.
32. 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.

УДК 004

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

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ІНТЕЛЕКТУАЛЬНОЇ ІНТЕГРАЦІЇ ІСНУЮЧИХ КОМПОНЕНТ ІТ-СИСТЕМИ З ХМАРНИМИ СЛУЖБАМИ НАСТУПНОГО ПОКОЛІННЯ

У статті розроблено програмне забезпечення, яке призначено для системи інтелектуальної інтеграції існуючих компонент ІТ-системи з хмарними службами наступного покоління. Метою розробки є дослідження та принципи побудови системи інтелектуальної інтеграції існуючих компонент ІТ-системи з хмарними службами наступного покоління. Об'єктом дослідження є процес інтелектуальної інтеграції існуючих компонент ІТ-системи з хмарними службами наступного покоління. Предметом дослідження є методи інтелектуальної інтеграції існуючих компонент ІТ-системи з хмарними службами наступного покоління. Методи дослідження базуються на методах хмарних технологій, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи інтелектуальної інтеграції існуючих компонент ІТ-системи з хмарними службами наступного покоління. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

інтелектуальна інтеграція, ІТ-система, хмарні служби наступного покоління

Постановка проблеми. Останнім часом значно активізувалися зусилля по реалізації хмарних сервісів, прагнучи відвоювати лідируючі позиції в конкурентів, які раніше прийшли на цей ринок. Cloud Platform надає хмарні інструменти для мобільної розробки, замовленого програмування й модернізації наявних додатків. Хоча Cloud підтримує всі типи хмарних сервісів: IaaS, PaaS і SaaS, – важливе значення надається взаємодії з розроблювачами.

Розходження між інфраструктурою як сервісом і платформою як сервісом можна визначати по-різному. Говорячи із замовниками, я звичайно не акцентую на цьому їхня увага. Однак певна – невелика – різниця зберігається. Ключове слово – автоматизація. У випадку IaaS замовник має можливість більшого контролю, але й залишає за собою більшу відповідальність. Наприклад, він повинен сам установити й зконфігурувати ПЗ, що збирається перенести в хмарну інфраструктуру.

При використанні ж PaaS (у всякому разі, це справедливо у відношенні Cloud Platform) забезпечується високий ступінь автоматизації надання ресурсів, середовища розробки й процесів. Автоматизація розгортання додатків, установки відновлень, резервного копіювання, відновлення й масштабування – все це атрибути платформи як сервісу, які далеко не завжди застосовні до IaaS.

Cloud Platform розрахована на різні категорії клієнтів. Очевидно, що розроблювачі – одна з них, але цільовим сегментом є також ІТ-менеджери, інтегратори додатків і інші користувачі.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи інтелектуальної інтеграції існуючих компонент іт-системи з хмарними службами наступного покоління.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи інтелектуальної інтеграції існуючих компонент ІТ-системи з хмарними службами наступного покоління.

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

- Огляд існуючих систем інтелектуальної інтеграції існуючих компонент ІТ-системи з хмарними службами наступного покоління.
- Дослідження системи інтелектуальної інтеграції існуючих компонент ІТ-системи з хмарними службами наступного покоління.
- Програмна реалізація системи інтелектуальної інтеграції існуючих компонент ІТ-системи з хмарними службами наступного покоління.

Об'єктом дослідження є процес інтелектуальної інтеграції існуючих компонент ІТ-системи з хмарними службами наступного покоління.

Предметом дослідження є методи інтелектуальної інтеграції існуючих компонент ІТ-системи з хмарними службами наступного покоління.

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

Виклад основного матеріалу. Замовники можуть споживати інфраструктуру як сервіс і платформу як сервіс або з публічної хмари, або зі свого ЦОДу. В останньому випадку надається в оренду все необхідне встаткування й управляємо сервісами точно так само, як у публічній хмарі, тобто замовник одержує ті ж самі ресурси й функції в себе в ЦОДі.

Портфоліо Cloud at Customer включає кілька реалізацій. Наприклад, Cloud Machine надає інфраструктуру й платформу як сервіс. Якщо замовник хоче одержати Exadata як сервіс, ми пропонуємо йому Exadata Cloud Machine і надаємо повний контроль над цими сервісами. За допомогою захищеного шлюзу інженери можуть установлювати необхідні відновлення, але даних клієнтів їм не видні. Вся інформація в нашій хмарі шифрується (при зберіганні, при передачі або в пам'яті), а ключі шифрування відомі тільки замовникові.

Незважаючи на те що в інженерів немає доступу до даних, деякі підприємства не хочуть, щоб до їхнього середовища можна було підключитися ззовні. Із цієї причини ми пропонуємо підтримку так званого відключеного режиму (disconnected mode). Це означає, що регіональний інженер регулярно відвідує замовника для установки відновлень, тобто замість проведення операцій віддалено наші інженери виконують їх на місці. Очевидно, що така послуга обходиться дорожче.

Все залежить від того, що розуміти під галузевою хмарою. Якщо мова йде про специфічний різновид додатків, то ми дуже багато робимо в цьому напрямку. пропонує саме різне програмне забезпечення у вигляді сервісу, призначене для конкретних галузей: телекомунікаційних компаній, роздрібного й фінансового секторів, а також для ряду інших напрямків.

Інший підхід – швидше за все, ви мали на увазі саме його – передбачає наявність окремого ЦОДу для конкретної галузі. У нас є, наприклад, урядова хмара, що відповідає вимогам державних організацій. Є фінансова хмара, побудована з урахуванням відповідних стандартів, зокрема PCI DSS.

Вибір технологій залежить від особливостей законодавства тої або іншої країни. Наприклад, у США державний сектор дуже жорстко регулюється такими нормами, як FedRAMP, тому ми повинні були створити окремий ЦОД для відповідності цим вимогам. Так само ми надходимо й в інших регіонах, де урядове регулювання дуже тверде і є критична маса користувачів, достатня для створення окремої хмари.

Від інших технологій Інтернет речей відрізняється насамперед обсягом даних. Їхня обробка в реальному часі вимагає величезних обчислювальних потужностей.

Для Інтернету речей пропонує різні рішення. Так, розроблений хмарний сервіс IoT Cloud Service, за допомогою якого можна реєструвати різні пристрої, здійснювати безпечні комунікації з ними й управляти двосторонньою взаємодією, а крім того, у реальному часі

обробляти всю вступник від них інформацію. Можна аналізувати ці дані, витягати з них важливі відомості й управляти з їхньою допомогою бізнесами-процесами.

З обліком генеруємого обсягу даних і подій разом з IoT часто використовуються технології Великих Даних, а виходить, крім обробки в реальному часі, потрібна можливість поміщати інформацію в конкретні озера даних. Відповідне середовище дуже важко правильно масштабувати, тоді як еластичність хмари дозволяє починати з малого й нарощувати ресурси в міру необхідності. Ми пропонуємо цілий спектр хмарних сервісів для Великих Даних. Так, Big Data Preparation Cloud Service дозволяє підготувати дані для переносу в середовище Великих Даних, а Big Data Discovery Cloud Service – витягти всю корисну інформацію.

Інтернет речей висуває високі вимоги до інтеграції із внутрішніми системами. Подій відбувається багато, а реагувати на них треба вчасно. Однак для цього необхідно запустити бізнес-процес, що з великим ступенем імовірності буде задіяти різні внутрішні системи, тобто IoT-середовище повинна бути тісно взаємозалежна з ними. Ми надаємо сервіси інтеграції в хмару, щоб можна було запускати необхідні бізнес-процеси при настанні події.

Таким чином, IoT не можна розглядати окремо. Інтернет речей породжує безліч супутніх завдань у таких областях, як керування даними, інтеграція із внутрішніми системами, інформаційна безпека й керування IT.

Про прикордонні обчислення говорять усе більше й більше. Однак можливі різні сценарії. Деякі пристрої, маючи достатні інтелектуальні можливості й необхідну обчислювальну потужність, здійснюють обробку подій в автоматичному режимі, але при цьому потрібно контролювати, які дані вони використовують. Цілісне подання про те, що відбувається на таких пристроях, припускає агрегування й централізацію даних, а для цього необхідно хмара.

Маятник розвитку гойдається туди й назад. Спочатку все поєднується, потім розподіляється, потім знову поєднується й т.д. Хмара – це насамперед централізація. Прикордонні ж обчислення припускають значну децентралізацію. Потреба буде зберігатися й у тому і в іншому. Даних і подій стільки, а потреба в їхній обробці росте так стрімко, що перенос частини обчислень на границю досить бажаний, але хмари при цьому не розсіюються, тому що в одних сценаріях краща децентралізація, в інші – централізація.

Контейнери, безумовно, роблять все більший вплив на те, як замовники розробляють і впроваджують нові додатки. Застосування контейнерів підвищує гнучкість рішення, до того ж додатки ізолюються від платформи, на якій вони будуть функціонувати. Контейнери можна розгорнути у власному ЦОДі, хмарі або будь-якому іншому. Гнучкість – одна із причин того, чому контейнери використовуються всі частіше.

І знову мова йде про волю вибору. У наші дні можливість вибору надзвичайно важлива, оскільки універсального рішення не існує. Я можу виділити три різних підходи до застосування контейнерів. Один з них припускає повний контроль: замовник сам створює контейнери, розгортає їх у хмарі й управляє ними. Ми підтримуємо цю опцію: Docker, Swarm і інші технології, що базуються на Docker, Kubernetes і т.д., можна розгорнути в хмарі й використовувати самостійно. Але такий контроль жадає від замовника більших зусиль.

Інший підхід представлений Container Cloud Service. Замовник сам створює образи контейнерів і розміщає їх у хмарі за допомогою цього сервісу. Хмара відповідає за оркестрацію, розміщення образів, моніторинг і контроль образів Docker. Таким чином, замовникові немає необхідності освоювати всі необхідні технології оркестрації.

Третій розрахований на тих, хто хотів би скористатися всіма перевагами контейнерів, але не знаком з технологією. Для них ми пропонуємо Application Container Cloud Service. Замовник може написати застосунок і розгорнути його в контейнерному середовищі, при цьому йому не прийдеться мати справу з образами Docker. Додатки можуть створюватися за допомогою різних мов програмування й середовищ розробки: node, Java SE, Ruby, Python. Всі середовища працюють на Docker, але розроблювач навіть не знає, що він використовує контейнери.

Таким чином, залежно від того, що замовникові необхідно, він може вибрати кожної із трьох сценаріїв використання. Ми вважаємо, що Docker відмінно підходить для створення нових додатків. Але, крім того, не можна не відзначити потреба в контейнеризації наявних додатків. Всі продукти, які підтримує Oracle, можуть бути розгорнуті в контейнерному середовищі.

Кожний із замовників, з ким мені доводило зустрічатися, займається розробками програмного забезпечення тією чи іншою мірою, оскільки воно лежить у самому серці інновацій і дозволяє компанії виділитися серед конкурентів. Розроблювачів може бути небагато, але тим, що є, необхідно сфокусуватися на інноваціях.

У деяких галузях (роздрібна торгівля, фінанси, телекомунікації) потреба в диференціації вище, ніж в інших. Перераховані галузі перетерплюють серйозну трансформацію, і програмна розробка лежить у її основі. Але перетворення відбуваються всюди. Наприклад, державні інститути розробляють безліч додатків для надання кращих сервісів громадянам з використанням нових технологій і мобільних пристроїв.

Насправді тестування включене в процес розробки – у цьому суть сучасних підходів DevOps, що передбачають автоматизацію тестування й складання програм. Нові стандарти покликані спростити завдання забезпечення безпеки. Наприклад, технологія OAuth одержала широке поширення як спосіб забезпечити керування ідентифікацією в різних застосунках.

З переходом у хмару зростає потреба в консолідації ідентифікаційної інформації. Фрагментація ідентифікаторів породжує серйозну проблему для компаній: користувач може бути представлений в SaaS-застосунках у внутрикorporативних застосунках і в хмарних сервісах третіх сторін. Тому ми створили хмарний сервіс Identity Cloud Service, за допомогою якого ідентифікаційні дані можна консолідувати в хмарі. Крім того, Identity Cloud Service здійснює об'єднання (федерацію) ідентифікаторів з різних додатків і їхнє надання зовнішнім сервісам. Таким чином, досить один раз зареєструватися, щоб одержати доступ до всіх додатків при наявності відповідних прав.

Інший важливий момент, що стосується безпеки в хмарах, – ідея брокера безпеки хмарного доступу (Cloud Access Security Broker, CASB). Компанії найчастіше не знають, що саме роблять у хмарах їхні співробітники. CASB реєструється у всіх хмарах від вашого ім'я й надає детальні дані про використання хмарних сервісів. При виявленні якого-небудь аномального поведіння (наприклад, завантаження понад 20 Мбайт із корпоративної системи CRM) генеруються тривожні повідомлення. Популярність подібних сервісів росте, оскільки використання CASB стає обов'язковою вимогою в багатьох організаціях.

Можна ще довго говорити про те, що робить для реалізації мер захисту на всіх рівнях хмарної платформи. Підкреслю лише, що безпеки приділяється першорядна увага на всіх рівнях – від елементного до рівня керування.

Що таке хмари й коли має сенс будувати хмарні рішення? І якщо будувати, то які платформи використовувати? Чи потрібно надавати клієнтам хмарні сервіси? А може краще використовувати віртуалізацію? І чим відрізняється віртуалізація від хмар? Ці питання задають всі ІТ і «не ІТ» компанії: від великих операторів зв'язку до невеликих стартапів. Давайте спробуємо розібратися! Виникає питання – якщо й те й інше пов'язане з віртуалізацією і мережами, то це вийшли хмари? Адже всі ми прекрасно знаємо, що хмари – це віртуалізація ресурсів десь у мережі. Я спробував знайти формальне визначення хмар, але не знайшов. Визначення були розпливчасті й нечіткі, як справжні хмари. Для початку знайшов стандарт Cloud Computing, що розробляє NIST (National Institute of Standards and Technology). Він виділяє 3 виміру хмарних сервісів:

Хмари

Тобто чіткого визначення хмари немає навіть у стандарті. Розглянемо докладніше всі виміри:

Модель обслуговування або сервісна модель

Наступні поняття напевно всі чули:

– **IaaS (Infrastructure as a Service)** – постачальник надає тільки обчислювальні ресурси (servers, storage, processing, memory, network bandwidth). При цьому може надаватися набір підготовлених образів OS, які розвертаються за кілька хвилин. Також надається мережна зв'язність між віртуальними машинами й додаткові дискові ресурси. Окремою частиною IaaS є MaaS (Metal as a Service) – надання доступу до голого заліза без OS (bare-metal servers). Приклад постачальника IaaS: AWS. Платформи для побудови IaaS: VMware, OpenStack, Azure.

– **PaaS (Platform as a Service)** – постачальник надає операційну систему й певний софт для самостійної реалізації замовником своїх послуг, наприклад, DB, CMS. Приклади: OpenShift, Heroku, Google Cloud Platform, Cloud Foundry.

– **SaaS (Software as a Service)** – постачальник надає софт для використання замовником, наприклад: Microsoft Office 360, Microsoft Exchange і т.п.

Є думка, що справжні хмари це тільки PaaS і SaaS, але стандарт ця думка не підтверджує.

Модель розгортання

Тепер про моделі розгортання, які теж на слуху:

– **Private cloud (Частка хмара)** – інфраструктура розвертається усередині організації, тим самим забезпечується безпека й продуктивність.

– **Public cloud (Публічна хмара)** – інфраструктура призначена для надання послуг стороннім замовникам. Наприклад, AWS, Google Cloud. Переваги отут очевидні: не потрібний обслуговуючий персонал, швидкорозширюємі ресурси, платиш тільки за те, що спожив (години, гігабайти), можливість зосередитися на ідеї або бізнесі, а не на обслуговуванні інфраструктури. Добре підходять для швидкого розгортання невеликих систем, для організації стартапів.

– **Community cloud (Суспільна хмара)** – інфраструктура розділяється між декількома організаціями зі схожими концепціями споживання ресурсів, політиками в безпеці й т.п. Споживачів менше ніж у публічній хмарі, але більше чим у частці. Приклад: Google Apps for Government.

– **Hybrid cloud (Гібридна хмара)** – це комбінація із двох або більше різних хмарних інфраструктур (приватних, публічних або суспільних). Серед гібридних хмар є цікаві кейси використання, наприклад: усередині частки хмари організація зберігає всю необхідну актуальну інформацію, а резервні копії прозоро відправляються в публічну хмару.

Функціональні характеристики

А от на функціональні характеристики хмар найчастіше не звертають увагу, тоді як для хмар це невід'ємні вимоги:

– **Broad Access Network** – можливість доступу до ресурсів з Інтернету за допомогою різноманітних пристроїв.

– **Rapid Elasticity** – еластичність ресурсів. При необхідності швидке виділення додаткових ресурсів, аж до нескінченності.

– **Measured Services** – автоматичний вимір послуг і виставлення рахунків для оплати.

– **On-Demand Self Services, Resource Pooling** – виділення обчислювальних ресурсів (resource pooling) за запитом від замовників (on demand).

Виходить, щоб Сервіс мав право називатися хмарним, потрібно вміти відповісти на запитання «Де він перебуває по всім трьох вимірах?».

Зворотна сторона хмар

Але при всіх перевагах хмар існує ряд моментів, які можуть мати негативні наслідки, особливо в публічних хмарах:

– Хмарою порівняно легко управляти, але відновлення софта впливає на тисячі користувачів, що потенційно може привести до серйозних аварій.

– У публічних хмарах більші конфігурації не завжди дешевше, треба вважати TCO.

Виникає кілька питань до безпеки в публічних хмарах:

– Як обробляються конфіденційні дані?

- Чи дотримані вимоги регулятора до персональних даних?
- Наскільки надійна схоронність даних (дублювання, бекапування)?
- Який захист від хакерських атак?

Це всі, звичайно, не привід відмовитися від використання хмар, а причина більш ретельно розібратися в плюсах і мінусах.

Віртуалізація

Тепер кілька слів про віртуалізацію, без якої не може бути хмар. У віртуалізації також є кілька вимірів, які умовно можна назвати «Тип» і «Спосіб віртуалізації». Я коротко розскажу про усі.

Типи віртуалізації

Віртуалізація серверів

Звичайно під віртуалізацією мається на увазі розміщення декількох віртуальних серверів у рамках одного фізичного. Але може ще бути об'єднання декількох фізичних серверів в один логічний для рішення певного завдання:

Розподіленість + віртуалізація = GRID системи

Віртуалізація ресурсів

Ресурси – це оперативна пам'ять, жорсткі диски, процесори. Вони також можуть бути нарізані й роздані вроздріб різним користувачам.

Віртуалізація додатків

Віртуалізація додатків – це те, що ми вже знаємо як PaaS і SaaS.

Способи віртуалізації

Повна віртуалізація й паравіртуалізація

Основні методи віртуалізації – це повна віртуалізація й паравіртуалізація. Схема обох методів дуже схожа. Є гіпервізор і віртуальні машини з гостьовими OS. При повній віртуалізації в гостьову OS не вносяться ніякі зміни. При паравіртуалізації встановлюються оптимізовані образи для певного гіпервізора. Це дозволяє максимально використовувати апаратні ресурси й не вимагає ніяких змін від додатків. Прикладом системи, що реалізує повну віртуалізацію, є VMware, приклад паравіртуалізації – Xen і KVM. В KVM особливістю є те, що гостьова OS може бути тільки Linux.

Ще виділяють кілька способів віртуалізації.

Віртуалізація рівня операційної системи

Особливістю є, що гостьова OS може бути тільки одна. Прикладом віртуалізації на рівні OS є Linux-VServer.

Контейнеризація

Останнім часом усе більше використовуються системи контейнеризації, такі як Docker або Kubernetes. Вони дозволяють автоматично розвертати підготовлені образи OS в основному для цілей автоматичного тестування й для систем CI. Контейнери дуже схожі на віртуальні машини, але для них не потрібно гіпервізор, а тільки відповідний движок.

Емуляція встаткування

При цьому способі віртуалізації VM повністю емулює роботу певного встаткування. З одного боку, це дає можливість, наприклад, на одному процесорі емулювати інший тип процесора. З іншого боку, зрозуміло, що при цьому буде з роботи в десятки разів. Приклад емулятора – це Bochs.

Емуляція бібліотек OS

І для повноти картини додам емуляцію бібліотек. Це спосіб, при якому емулюється не вся OS, а тільки частина. Наприклад, Wine в Linux – емуляція бібліотек для Windows-додатків.

Виходить, що ми можемо віртуалізувати різні системи різними методами. Тобто бачимо, що існуючими способами й типами віртуалізації можна вирішити безліч завдань. Виникає логічне запитання, коли ж має сенс розвертати хмарну платформу?

Хмарні платформи розташовуються над набором віртуальних машин, повністю ізолюють застосунок як від заліза, так і від структури віртуального середовища. Хмарні

платформи використовуються для автоматичного й ручного scale in / scale out, запуску / зупинки / конфігурування VM і додатків. Коли має сенс залишатися у віртуалізації, а коли залишатися в хмарі? Концепція наступна: коли всього багато – хмара, мало – віртуалізація:

- Для завдань із більшим числом віртуальних серверів – краще хмара, для завдань із 10-20 віртуалками можна не розвертати хмарну платформу.
- Якщо потрібно постійно міняти конфігурацію ресурсів – хмара.
- Багато користувачів, даних, клієнтів – хмара.

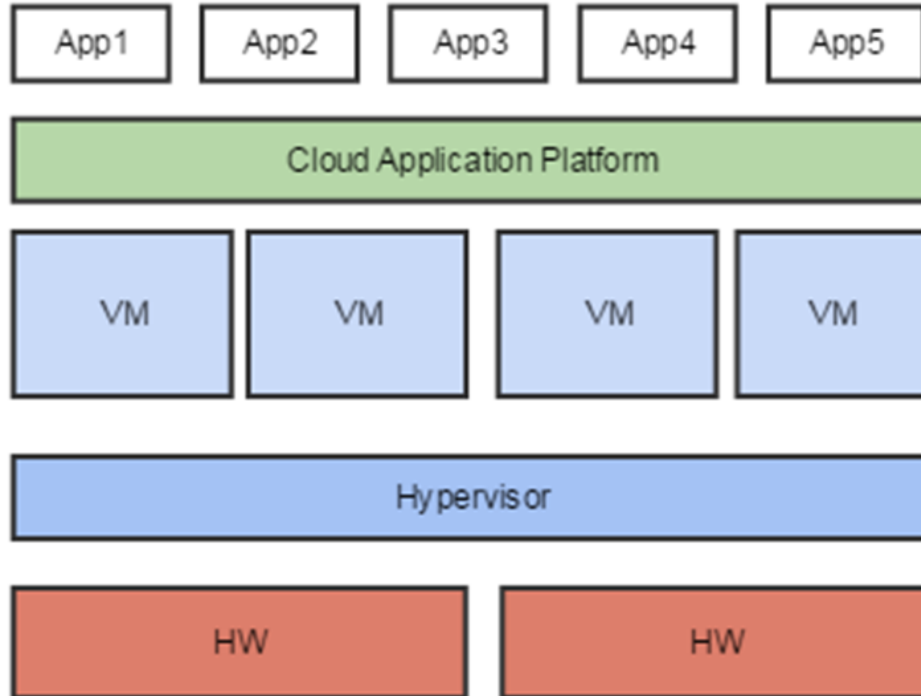


Рисунок 1 – Структурна схема системи

Кілька слів про платформи для побудови хмар. Інформації з них маса, тому приведу тільки суху вижимку.

Платформи для побудови хмар

Для побудови хмар зараз є дві основні платформи, інші (Eucalyptus, Cloudstack, Microsoft Azure) займають несуттєву частку.

– VMware – платформа vSphere. VMware зібрала величезну кількість технологій, веде розробку власної версії OpenStack.

– OpenStack – утворився в 2010 році, є комплексом проектів вільного програмного забезпечення, що може бути використаний для створення інфраструктурних хмарних сервісів і хмарних сховищ. Організація OpenStack Foundation (2012) нараховує більш ніж 1000 організацій і більше 30 000 учасників. Основні постачальники стека: Mirantis, RedHat, HP.

Хмарні платформи звичайно використовуються замовниками для реалізації наступних завдань:

- Робота із часто мінливою конфігурацією заліза, про що ми говорили вище.
- Надання інтернет-послуг і інші мережні додатки. Додатки повинні бути «Cloud Ready».
- Telco Cloud (вони ж SDN & NFV).
- Збір, зберігання, обробка BigData.

З отриманих даних можна зробити висновок, що для мобільних операторів зв'язку надання хмарних сервісів не є пріоритетним завданням, вони більше зосереджені на розвитку своїх мереж і сервісів. До операторів зв'язку потрібно звертатися за мережними послугами, такими як: віртуальна АТМ, віртуальна мережа, M2M и взагалі за всім тим, що може

надаватися на SDN & NFV технологіях: віртуальні Firewall, DPI і т.п. А за обчислювальними хмарами краще йти до спеціалізованих провайдерів.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів інтелектуальної інтеграції існуючих компонент ІТ-системи з хмарними службами наступного покоління. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем інтелектуальної інтеграції існуючих компонент ІТ-системи з хмарними службами наступного покоління.
- Досліджена система інтелектуальної інтеграції існуючих компонент ІТ-системи з хмарними службами наступного покоління.
- На основі отриманих результатів досліджень створена програмна реалізація системи інтелектуальної інтеграції існуючих компонент ІТ-системи з хмарними службами наступного покоління.

Розроблені алгоритми дозволяють успішно вирішувати завдання інтелектуальної інтеграції існуючих компонент ІТ-системи з хмарними службами наступного покоління. 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., 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. 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

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

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ПРОТИДІЇ ДЕТЕКТУВАННЮ АНТИВІРУСНОЮ СИСТЕМОЮ ЗА ДОПОМОГОЮ ШТУЧНОГО ІНТЕЛЕКТУ

У статті розроблено програмне забезпечення, яке призначено для системи протидії детектуванню антивірусною системою за допомогою штучного інтелекту. Метою розробки є дослідження та принципи побудови системи протидії детектуванню антивірусною системою за допомогою штучного інтелекту. Об'єктом дослідження є процес протидії детектуванню антивірусною системою за допомогою штучного інтелекту. Предметом дослідження є методи протидії детектуванню антивірусною системою за допомогою штучного інтелекту. Методи дослідження базуються на методах штучного інтелекту, методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи протидії детектуванню антивірусною системою 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.

протидія, детектування, антивірусна система, штучний інтелект

Постановка проблеми. У даній роботі будуть запропоновані ефективні методи обходу статичного, динамічного й евристичного аналізу, використовуваного в новітніх антивірусних продуктах. Деякі техніки вже відомі навзагал, але є й додаткові трюки, які є ключовими при генерації недетектуемого вірусу. Обсяг файлу не менш важливий при використанні даних методів, і я постарався оптимізувати розмір настільки, наскільки можливо. У цьому документі також буде порушена тема внутрішнього пристрою антивірусів і операційної системи Windows.

Методи реалізації технік антидетекта залежать від типу вірусу. Всі методи, описувані в даній роботі, будуть працювати з усіма типами вірусів, однак основна увага приділена складеним корисним навантаженням для meterpreter, оскільки цей командний інтерпретатор уміє практично все, що й інші вірусні програми. Одержання сесії за допомогою meterpreter на віддаленій машині відкриває масу можливостей: розширення привілеїв, крадіжку облікових записів, міграцію між процесами, маніпуляцію реєстром і інші трюки пост-експлуатації.

Крім того, навколо meterpreter зібралось потужне й активне співтовариство, і цей інструмент популярний серед фахівців з безпеки.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи протидії детектуванню антивірусною системою за допомогою штучного інтелекту.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи протидії детектуванню антивірусною системою за допомогою штучного інтелекту.

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

- Огляд існуючих систем протидії детектуванню антивірусною системою за допомогою штучного інтелекту.
- Дослідження системи протидії детектуванню антивірусною системою за допомогою штучного інтелекту.

– Програмна реалізація системи протидії детектуванню антивірусною системою за допомогою штучного інтелекту.

Об'єктом дослідження є процес протидії детектуванню антивірусною системою за допомогою штучного інтелекту.

Предметом дослідження є методи протидії детектуванню антивірусною системою за допомогою штучного інтелекту.

Методи дослідження базуються на методах штучного інтелекту, методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Перед початком вивчення ефективним методом, варто згадати пару слів про те, які є проблеми із широко відомими техніками й утилітами. На сьогоднішній день антивірусні компанії повністю оцінили всі ризики й найчастіше крім пошуку сигнатур і вірусного впливу шукають ознаки крипторів і пакувальників. У порівнянні з вірусами детектування крипторів і пакувальників простіше, оскільки останні мають однакові підозрілі алгоритми, на зразок розшифровки PE-файлу й запуску в пам'яті.

PE ін'єкція

Для того щоб зрозуміти схему запуску PE-образа в пам'яті, необхідно згадати про тім, як ОС Windows завантажує PE-файли. Звичайно при компіляції PE-файлу на адресу головного модуля встановлюється значення 0x00400000. Потім обробляються покажчики повних адрес і розраховуються інструкції довгих переходів на базі адреси головного модуля. По закінченні компіляції в PE-файлі створюється секція таблиці релокації, що містить адреси інструкцій, що залежать від базової адреси образа, наприклад, покажчики повних адрес і інструкцій довгого переходу.

Під час виконання PE-образа операційна система перевіряє доступність кращого адресного простору. Якщо даний простір не доступно, перед стартом системний завантажник процесів повинен підбудувати абсолютні адреси в пам'яті. За допомогою секції релокації завантажник виправляє всі інструкції, що залежать від адреси, і запускає припинений процес. Весь цей механізм називається «Рандомізація розміщення адресного простору» (Address Space Layout Randomization; ASLR).

Для того щоб виконати PE-образ у пам'яті, криптору потрібно распарсити PE-заголовки й перемістити абсолютні адреси. Найчастіше там є підроблений системний завантажник, що відразу викликає підозру. Коли ми аналізуємо криптори, написані на C або мовах високого рівня, практично в кожному випадку спостерігаються API функції «NtUnmapViewOfSection» і «ZwUnmapViewOfSection», які попросту відключають подання секції від віртуального адресного простору процесу. Ці функції грають дуже важливу роль при використанні методу RunPE, що зустрічається практично в 90% крипторів.

Природно, антивірусні продукти не можуть позначати кожен програму як вірусну, котра використовує ці API-функції. Однак сам факт наявності даних функцій значить багато чого. Існує невеликий відсоток крипторів (в основному написаних на асемблері), які не використовують ці функції й виконують релокацію вручну. Якийсь час ці криптори працюють ефективно, але рано або пізно наслідку через спробу підробити системний завантажник. Інший серйозний мінус – при шифруванні PE-файлу серйозно збільшується ентропія. Якщо антивірусний сканер детектує нетиповий рівень ентропії, цілком можливо PE-файл буде позначений як підозрілий.

Ідеальний метод

Концепція шифрування вірусного коду має право на життя, але функцію дешифрування варто обробити гарною обфускацією. Коли справа доходить до виконання дешифрованого коду в пам'яті, можна обійтися без переміщення абсолютних адрес. Крім того, усередині вірусу потрібно передбачити алгоритм перевірки знаходження усередині пісочниці. Якщо перевірка виявила, що вірусний код аналізується антивірусом, функцію дешифрування запускати не слід. Замість шифрування всього PE-файлу, більш грамотно шифрувати шелл-код або тільки секція .text. У цьому випадку ентропія й розмір файлу залишаються на прийнятному рівні, і не міняються заголовки образа й секції.

Функція буде детектувати, чи аналізується вірус динамічно усередині чи пісочниці ні. Якщо функція виявляє ознаки антивірусного сканера, то або знову викликається функція main, або вірус аварійно завершується. Якщо ж ознаки сканування відсутні, буде викликана функція для розшифровки шелл-коду.

Для збереження ентропії й розміру на прийнятному рівні я будуть обробляти шелл-код шифрувальником на базі алгоритму XOR з використанням мультибайтового ключа. Алгоритм XOR не є стандартом в індустрії, як наприклад RC4 або blowfish, але в нашій випадку сильне шифрування не потрібно. Антивірусні продукти не будуть займатися дешифруванням. Нам досить захисту від статичного аналізу рядків. Крім того, XOR-Шифрування набагато швидше й не використовує бібліотек, що впливає на підсумковий розмір вірусу.

Оскільки ми пишемо новий шматок вірусу, геш-сигнатура не буде відома антивірусним продуктам, і нам не потрібно турбуватися про виявлення за допомогою детектування, побудованого на базі сигнатур. Ми шифруємо шелл-код і обфускуємо функції анти-детектування/налагодження й алгоритм дешифрування, що цілком достатньо для обходу статичного/евристичного аналізу. Нам залишилося знайти спосіб обходу динамічного аналізу, що є найбільш важливою частиною функції «AV detect». Перед написанням даної частини необхідно розібратися, як працюють евристичні алгоритми антивірусних продуктів.

Евристичні движки

Евристичні движки засновані на статичному аналізі й механізмі правил. Головна мета таких движків – детектування вірусів нового покоління, які ще не відомі, за допомогою угруповання й оцінки погроз/ризиків в окремих фрагментах коду відповідно до визначених критеріїв. Навіть при скануванні найпростішої програми, що виводить на екран «Привіт, світ», евристичний движок визначає рівень погрози й ризику. Якщо оцінка перевищує граничний рівень, файл позначається як вірусний. Евристичні движки – найбільш просунутий компонент антивірусних продуктів і використовують значну кількість правил і критеріїв. Оскільки антивірусні компанії не випускають документації, що описує евристичні движки, відомі лише деякі критерії оцінки погроз/ризиків. Природно, тут може бути багато помилок допущень і помилок.

От деякі відомі правила, використовувані при оцінці погроз:

Присутність циклу дешифрування.

- Читання поточного ім'я комп'ютера.
- Читання криптографічного машинного GUID.
- З'єднання з випадковими доменами.
- Читання дати установки Windows.
- Видалення файлів, що виконуються.
- Присутність потенційного IP-адреси в пам'яті бінарного файлу.
- Модифікація налаштувань проксі-сервера.
- Установка хуків/патчів до запущеного процесу.
- Інжектування в explorer.
- Інжектування у віддалений процес.
- Запит інформації про процес.
- Установка процесу в режим помилки для приховання повідомлення об помилки.
- Нетипова ентропія.
- Можлива перевірка на присутність антивірусного движка.
- Присутність функціонала для розширення привілеїв.
- Модифікація налаштувань політик додатків.
- Читання версії BIOS системи/відеокарти.
- Кінець PE-заголовка перебуває усередині нестандартної секції.
- Створення захищених областей пам'яті.
- Створення безлічі процесів.
- Спроба призупинити роботу на довгий час.

- Нестандартні секції.
- Читання Windows Product Id.
- Присутність функціонала для запуску/взаємодії із драйверами пристроїв.
- Присутність функціонала для блокування користувальницького уведення.

При написанні функції по детектуванню антивірусних продуктів і дешифрування шелл-коду, варто брати до уваги ці правила.

Дешифрування шелл-коду

Обфускація механізму дешифрування надзвичайно важлива, оскільки більшість евристичних движків у стані виявити цикли дешифрування усередині PE-файлів. Після значного збільшення випадків, коли програма вимагала викуп, деякі евристичні движки були майже повністю заточені під детектування процедур дешифрування. Після виявлення процедури дешифрування деякі сканери чекали, поки в реєстрі ESI не виявиться значення 0, що в більшості випадків означає закінчення циклу. По досягненню закінчення циклу дешифрування виробляється повторний аналіз вмісту файлу, що буде являти собою функцію дешифрування шелл-коду.

Показано цикл for, усередині якого виконуються логічні операції XOR між байтом шелл-коду й байтом ключа. Асемблерні блоки нагорі й унизу, по суті, не виконують ніяких операцій. Ці блоки «накривають» XOR-операцію випадковим набором байтів і переходів. Оскільки ми не користуємося просунуті механізми дешифрування, подібної обфускації буде досить для функції «Decrypt Shellcode».

Детектування динамічного аналізу

У процесі написання механізму детектування пісочниці нам необхідно зробити обфускацію методів. Якщо евристичний движок виявить ознаки методів анти реверс-інжинірингу, різко зросте оцінка погрози з боку нашого вірусу.

Детектування відладника

Наш перший механізм детектування антивірусного продукту буде перевіряти присутність відладника усередині процесу. Для рішення даного завдання існує API-функція, що визначає, чи налагоджує процес відладником рівня користувача (user-mode debugger). Але ми не будемо використовувати дану функцію, оскільки більшість антивірусних продуктів моніторять вираження API-Викликів. Швидше за все, після детектування виклик буде розцінений як протидіючому реверсу-інжинірингу. Замість використання API-функції ми будемо шукати байт «BeingDebugged» в PEB-блоці.

Ділянка коду на рисунку вище витягає байт BeingDebugged з PEB-блоку. Якщо відладник є присутнім, перевірка повторюється знову, і так доти, поки в стеці не буде переповнення. Після переповнення спрацює виключення, і процес буде закритий. Цей шлях – найпростіший для виходу із програми. Ручна перевірка байта BeingDebugged дозволить обійти пристойну кількість антивірусних продуктів, але в деяких додатках передбачений подібний випадок, і ми повинні зробити обфускацію коду, щоб захиститися від статичного аналізу рядків.

Додавання переходів (інструкцій JZ) після кожної операції не вплине на логіку роботи функції, але додавання смітєвих байтів між переходами дозволить обійти фільтри статичного аналізу рядків.

Завантаження підробленої бібліотеки

У цьому методі ми спробуємо завантажити неіснуючу бібліотеку під час виконання додатка. Звичайно коли ми намагаємося завантажити неіснуючу бібліотеку, NISTENCE повертає NULL, але деякі механізми динамічного аналізу, використовувані в антивірусних продуктах, допускають такі випадки й продовжують подальше дослідження потоку виконання додатка.

Використання функції GetTickCount

У цьому методі ми будемо опиратися на той факт, що час, що приділяється на сканування, обмежено. У більшості випадків антивірусні сканери створені для кінцевого користувача. Відповідно, додаток повинне бути як можна більш дружельно й придатне для

щоденного використання. Цей факт означає, що сканер не може витрачати занадто багато часу на сканування файлів, а повинен завершувати весь процес якнайшвидше. Спочатку розроблювачі вірусів використовували функцію «sleep» з метою дочекатися закінчення сканування, але зараз цей трюк практично не працює, оскільки кожний антивірусний продукт пропускає дану функцію. Ми будемо використовувати інший метод, показаний існує, що використовує API-функцію «GetThickCount». Дана функція витягає кількість мілісекунд, що пройшли з моменту запуску системи (до 49.7 днів). Ми будемо використовувати цю функцію для одержання часу, що пройшло з моменту запуску операційної системи, потім зупинимося на 1 секунду. Після функції sleep ми перевіримо, чи була ця ділянка пропущена, за допомогою порівняння двох значень, отриманих за допомогою GetThickCout.

Перевірка кількості ядер

Цей метод перевіряє кількість ядер процесора, що присутні у системі. Оскільки антивірусні продукти не можуть займати занадто багато ресурсів, ми можемо перевірити кількість ядер для того, щоб визначити, чи перебуваємо ми в пісочниці. Багато антивірусів не підтримують мульти-ядерну обробку й не можуть зарезервувати більше одного ядра для пісочниці.

Виділення великого обсягу пам'яті

Цей метод також експлуатує обмежений час, використовуваний при скануванні. Ми виділяємо близько 100 Мб пам'яті й заповнюємо даний простір порожніми байтами. Потім пам'ять звільняється.

Коли пам'ять, використовувана програмою, під час виконання починає рости, через якийсь час антивірусні сканери зупиняються, щоб не витрачати багато часу на аналіз файлу. Цей метод можна використовувати кілька разів. Дана техніка дуже стара й примітивна, але усе ще допомагає обійти пристойна кількість сканерів.

Маніпуляція прапором трасування

Як треба з назви, цей прапор використовується під час трасування програм. Якщо прапор трасування встановлений, кожна інструкція буде ініціювати виключення «SINGLE_STEP». Прапором трасування можна маніпулювати з метою протидії трасувальникам за допомогою коду, показаного існує:

Перевірка мьютексів

Цей метод через свою простоту виглядає дуже перспективним. Суть техніки полягає в перевірці присутності певного мьютекса в системі.

Якщо функція «CreateMutex» не поверне помилку ERROR_ALREADY_EXISTS, вірус запускається ще раз, оскільки більшість антивірусних продуктів не дозволяють програмам, які піддаються динамічному аналізу, запускати нові процеси або працювати з файлами поза пісочницею. Якщо за результатами перевірки мьютекса вертається помилка ERROR_ALREADY_EXISTS, можна запускати функцію дешифрування. Існують набагато більше креативні способи використання мьютексов з метою анти-детектування.

Правильні методи виконання шелл-коду

Починаючи з Windows Vista, компанія Microsoft впровадила технологію DEP (Data Execution Prevention; Запобігання виконання даних). Ця міра, спрямована на зміцнення безпеки, допомагає запобігти псуванню комп'ютера шляхом періодичного моніторингу. Моніторинг дозволяє підтримувати коректно використання пам'яті. Якщо механізм DEP виявляє випадок некоректного використання пам'яті вашого комп'ютера, програма закривається, і користувач сповіщається. Відповідно, ви не можете просто помістити трохи байт у символічний масив і виконати свою творчість. Вам потрібно виділити область пам'яті із прапорами на читання, запис і виконання за допомогою API-функцій.

Компанія Microsoft передбачила трохи API-функцій для резервування сторінок пам'яті. Більшість вірусів для резервування використовують функцію «VirtualAlloc», що, як ви вже догадалися, полегшує завдання по детектуванню. Використання інших функцій для маніпуляції пам'яттю допоможе виконати той же самий трюк більш непомітно.

Далі я покажжу методи виконання шелл-коду за допомогою різних API-функцій.

HeapCreate/HeapAlloc:

ОС Windows також дозволяє створити купи з атрибутами на читання, запис і виконання.

LoadLibrary/GetProcAddress

Комбінація WINAPI-функцій LoadLibrary і GetProcAddress дозволяє використовувати інші API-функції. У цьому випадку не буде прямого виклику функцій, пов'язаних з маніпуляцією пам'яті, а сам вірус, імовірно, буде більше непомітний.

GetModuleHandle/GetProcAddress

Цей метод зовсім не використовує функцію LoadLibrary, а одержує оброблювач уже завантаженого модуля kernel32.dll за допомогою функції GetModuleHandle. Дана техніка для запуску шелл-коду, можливо, одна із самих непомітних.

Мультипоточність

PE-файли, що використовують кілька потоків, завжди складніше аналізувати, у тому числі й для антивірусних продуктів. За допомогою мультипоточного підходу ми можемо запускати шелл-код і одночасно продовжувати виконання функції «AV Detect».

У коді, показаному вище, виконання шелл-коду відбувається в окремому потоці. Паралельно виконанню шелл-коду в нескінченному циклі виконується функція для обходу антивірусу. Такий підхід дозволяє перевіряти присутність пісочниці й динамічного аналізу, що життєво важливо для обходу просунутих евристичних движків, які чекають запуску шелл-коду.

При компіляції вихідних текстів вірусів необхідно включити захист стека й видалити символи з метою утруднення реверс-інжинірингу й зменшення розміру кінцевого файлу, що виконується. Рекомендується компілювати в Embarcadero RAD Studio через присутність асемблерних вставок.

Якщо скористатися одночасно всіма методами, продемонстрованими в даній роботі, згенерований вірус зможе обійти 35 найбільш просунутих антивірусних продукту.

Впровадження бекдору в PE-файл

Далі, у даній роботі розповімо про декілька методів, використовуваних для розміщення вірусу в PE-файлі. Щоб зрозуміти суть матеріалу, що викладається, читачеві необхідно бути знайомим з асемблером для архітектури x86 і відладниками хоча б на середньому рівні й розуміти формат PE файлів. Цей документ був опублікований 8 грудня 2016 року на сайті pentest.blog, а також підготовлений в PDF форматі для офлайнного читання.

У цей час практично всі фахівці з безпеки, пентестери й аналітики вірусів мають справу з бекдорами на щоденній основі. Приміщення трояна в систему або в конкретну програму – найбільш популярний спосіб для підтримки постійного доступу до цільової машини. У більшості статей розповідається про методи для імплантування вірусів в 32 бітні PE файли, але оскільки PE-формат являє собою модифіковану версію формату Unix COFF (Common Object File Format; Загальний формат об'єктних файлів), логіка, закладена в основу цих технік, застосовна й до всіх інших типів файлів, що виконуються. Крім того, непомітність убудованого вірусу дуже важлива й прямо впливає на тривалість знаходження в системі. Методи, які будуть описані в даній роботі, спрямовані на зниження відсотка детектування настільки наскільки можливо. Перед подальшим читанням рекомендую ознайомитися з першою частиною, де розповідалося про обхід технік детектування, внутрішньому пристрої антивірусів і фундаментальних постулатів антидетектування.

Уведемо додаткову термінологію.

Навчальне проникнення

Існують групи, що складаються зі світлих хакерів (або білих капелюхів), які атакують цифрову інфраструктуру організації, як якщо це робив реальний зловмисник, для того, щоб протестувати стійкість системи до зовнішніх погроз (по-іншому це називається пентест). Наприклад, компанія Microsoft регулярно проводить подібні кібер-навчання. Плюси від

подібних заходів лежать на поверхні – у процесі можуть знайтися проломи й проблеми, які можна заздалегідь усунути. Крім того, тут можуть виявитися шляхи влучення конфіденційної інформації назовні, схеми експлуатації й інші «недокументування» можливості системи.

Рандомізація розміщення адресного простору

ASLR являє собою техніку безпеки, спрямовану на захист від атак, пов'язаних з переповнення буфера. Щоб не дати зловмисникові коректно перейти на певну функцію усередині пам'яті, ASLR у випадковому порядку вишиковує позиції ключові областей інформації в адресному просторі процесу. Сюди ж включається базова адреса файлу, що виконується, і позиції стека, купи й бібліотек.

Code Cave (Печера в коді)

Code Cave являє собою шматок коду, що записується іншою програмою на згадку стороннього процесу. Цей код може бути виконаний за допомогою створення віддаленого потоку усередині цільового процесу. Code cave найчастіше є посиланням на секцію скриптових функцій коду, куди можна інjectувати будь-які інструкції. Наприклад, якщо в пам'яті скрипту 5 байт, і 3 байти використовуються, в 2 байти, що залишилися скрипту можна додати зовнішній код.

Контрольна сума

Контрольна сума являє собою невелику порцію інформації із блоку цифрових даних для виявлення помилок, які можуть з'явитися під час передачі або зберігання файлу. Звичайно за допомогою контрольної суми перевіряється настановний файл після одержання із сервера. Між нами говорячи, контрольні суми звичайно використовуються для верифікації цілісності даних, але не враховують дійсність інформації.

Основні методи

Всі приклади з даної роботи будуть продемонстровані на базі файлу, що виконується, SSH-клієнта з ім'ям putty. Є кілька причин для вибору саме цього додатка як піддослідний зразок. Putty використовує безліч бібліотек і API-функцій. По-друге, впровадження вірусу в ssh-клієнт залучає менше уваги, оскільки програма вже виконує tcp-з'єднання, і, таким чином, буде простіше уникнути моніторингу з боку системи безпеки.

Код бекдору буде взятий із шелл-коду, використовуваного при зворотному TCP-з'єднанні й написаного під meterpreter. Головна мета – інjectувати шелл-код у цільовий PE-файл без псування функціональності додатка. Інjectований шелл-код буде запускатися в окремому потоці й буде постійно намагатися приєднатися до оброблювача. Друге завдання – під час виконання всіх цих маніпуляцій необхідно залишатися непомітним настільки, наскільки можливо.

Загальний підхід впровадження вірусу в PE-файл складається з 4 кроків:

- Знаходження доступного простору для коду бекдору.
- Перехоплення потоку виконання.
- Впровадження бекдору.
- Відновлення потоку виконання.

У кожному кроці є свої нюанси, які прямо впливають на стійкість, тривалість і непомітність убудованого вірусу.

Проблема з доступним простором

Знаходження доступного простору – перший крок до реалізації нашого завдання. Надзвичайно важливо вибрати правильне місце усередині PE-файлу для впровадження бекдору. Оцінка погрози з боку зараженого файлу сильно залежить від того, як ви вирішите це завдання. Тут існує два підходи.

Додавання нової секції

У порівнянні із другим підходом тут більше ймовірність виявлення. Хоча, з іншого боку, при додаванні нової секції в нас немає обмежень по просторі, і ми можемо впровадити бекдор будь-якого розміру.

За допомогою дизасемблера або редактори LordPE PE-файл можна розширити за допомогою додавання заголовка нової секції. Існує таблиця секцій файлу, що виконується, putty. За допомогою PE-редактора додана нова секція «NewSec» розміром 1000 байт.

Під час створення нової секції важливо встановити прапори на читання/запис/виконання, щоб запустити шелл-код, коли PE-образ проектується (map) на згадку.

Після додавання заголовка секції необхідно адаптувати розмір файлу, що робиться в шістнадцятковому редактору за допомогою додавання порожніх байтів розміром з нову секцію в кінець файлу.

Після додавання нової порожньої секції необхідно запустити виконується файл, що, і перевірити, є чи помилки. Якщо все пройшло гладко, нова секція готова до модифікації в відладнику.

Рішення проблеми доступного простору за допомогою додавання нової секції має деякі недоліки. Практично всі антивіруси пізнають нестандартні секції, і якщо, до того ж, там є повний набір прапорів на читання/запис/виконання, те ця ситуація виглядає ще більш підозріло.

Навіть якщо ми просто додамо нову секцію з повними правами без бекдору, деякі антивіруси вже позначають виконується файл, що, як вірусний.

Використання Code Cave

У другому методі, спрямованому на рішення проблеми доступного простору, використовуються code cave'и із цільового файлу, що виконується. Практично всі скомпільовані бінарні файли мають code cave'и, які можуть бути використані для впровадження вірусу. Code cave у порівнянні з новою секцією залучає набагато менше уваги, оскільки в цьому випадку застосовуються вже існуючі звичайні секції. Додатковий і не менш важливий плюс полягає в тому, що після впровадження вірусу розмір PE-файлу не міняється. Однак ця техніка має свої недоліки.

Кількість і розмір code cave'ов варіюється від файлу до файлу, але в цілому загальний розмір менше, ніж при додаванні нової секції. При використанні code cave'ов код бекдору варто зменшувати настільки, наскільки можливо. Другий недолік – набір прапорів. Оскільки виконання буде перенаправлятися в code cave, у секції повинні бути права на виконання. У випадку з деякими шелл-кодами (які самі себе кодують або піддають обфускації) потрібно права на запис для того, щоб виконувати зміни усередині секції.

Використання декількох code cave'ов дозволяє перебороти обмеження із простором. Тут же додатковий плюс у тому, що вірус збирається з окремих шматків. Однак зміна привілеїв секції буде виглядати підозрілим. Існують просунуті методи для модифікації привілеїв в області пам'яті під час виконання додатка з метою запобігання прямої зміни прапорів секції, але оскільки ці техніки вимагають спеціалізованого шелл-коду, кодування й парсингу таблиці ІАТ, ця тема буде порушена в наступних статтях.

За допомогою утиліти Cminer дуже легко підрахувати всі code cave'и бінарного файлу. Використовуємо команду ./Cminer putty.exe 300 для пошуку code cave'ов більше 300 байт.

У нашій випадку знайдено 5 гарних екземплярів для наступного використання. Стартова адреса задає адресу віртуальний пам'яті (virtual memory address, VMA) в code cave при завантаженні PE-файлу на згадку. Зсув файлу, вимірюваного в байтах, – адреса місцезнаходження потрібної області усередині PE-файлу.

За результатами пошуку з'ясувалося, що більшість областей перебувають усередині секції даних. Оскільки в цих секціях не встановлений прапор на виконання, будуть потрібні зміни. Розмір бекдору біля 400-500 байт, і області Cave 5 вистачить позаочі. Стартова адреса даної області потрібно зберегти, а після зміни привілеїв секції перший етап впровадження вірусу можна вважати завершеним. Тепер потрібно перенаправляти виконання на нашу область.

Перехоплення потоку виконання

На цьому етапі потрібно перенаправляти потік виконання на код бекдору за допомогою модифікації потрібної інструкції у файлі, що виконується. Тут варто згадати важливу деталь щодо вибору інструкції для зміни. Всі бінарні інструкції мають розмір у байтах. Щоб перейти до адреси розташування бекдору буде потрібно довгий перехід (long jump) розміром, що використовує 5 або 6 байт. При зміні бінарного файлу інструкція, що буде патчиться, повинна бути того ж розміру, що й довгий перехід, інакше попередня й наступна інструкція будуть зіпсовані.

Дуже важливий вибір правильного місця для перенапряму виконання, оскільки якщо перенапрямок буде здійснюватися прямо, неминуче детектування на етапі динамічного аналізу антивірусними продуктами.

Приховання усередині користувацьких функцій

Перше, що спадає на думку, для обходу пісочниці й динамічного аналізу – відкладене виконання шелл-коду або використання детектора пісочниці, за результатами роботи якого виконується та або інша вітка алгоритму. З іншого боку, у більшості випадків через обмеження по розмірах ми не можемо додати зайві ділянки коду в PE-файл. Крім того, реалізація технік антидетектування на низькому рівні вимагає багато часу й сил.

Цей метод використовує функції, що вимагають дій користувача. Перенапрямок виконання усередині подібних функцій буде спрацьовувати тільки в тому випадку, якщо користувач працює в програмі. Якщо дана техніка буде реалізована коректно, успіх практично гарантований, і, до того ж, не буде збільшений розмір бекдору.

По натисканню кнопки «Open» із графічної оболонки запускається функція перевірки встановленого IP-адреси.

Якщо поле IP-адреси не порожнє, і значення коректне, запускається функція для з'єднання із зазначеним IP-адресою.

Якщо клієнт успішно створив ssh-сесію, з'явиться нове вікно для введення ім'я користувача й пароля.

Саме в цьому місці відбудеться перенапрямок. Оскільки антивірусні продукти не настільки просунуті для аналізу такого роду механізмів, впроваджений бекдор, швидше за все, не буде виявлений за допомогою динамічного аналізу.

За допомогою нескладних методів реверс-інжинірингу, призначених для роботи з рядками й посиланнями на рядки, буде не складно знайти адресу функції з'єднання після того, як клієнт установив з'єднання із призначеним IP-адресою. Рядок «login as:», що з'являється в спливаючому вікні, допоможе нам знайти адресу функції з'єднання. У пошуках посилань на рядки нам допоможе IDA Pro.

Для знаходження рядка «login as:» в IDA Pro відкриваємо Views->Open Subviews->Strings on IDA

Після знаходження потрібного рядка двічі клікаємо і переходимо до місцезнаходження. Усередині секцій даних IDA знаходить всі перехресні посилання на рядки. Для виводу всіх перехресних посилань натискаємо комбінацію клавіш «Ctrl+X».

Існує посилання усередині функції, що виводить рядок «login as:»

Існує інструкція, що ми будемо змінювати. Після виконання коду бекдору, ця інструкція буде використовуватися знову.

Після зміни інструкції PUSH 467C7C на JMP 0x47A478 процес перенапряму потоку виконання можна вважати завершеним. Важливо не забувати, що адреса наступної інструкції буде використовуватися як адреса повернення після виконання коду вірусу. Наступний крок – інжектування коду бекдору.

Інжектування коду бекдору

Перша думка, що спадає на думку при впровадженні бекдору, – збереження регістрів перед виконанням вірусного коду. Кожне значення усередині регістрів – надзвичайно важливо для виконання програми. Помістивши інструкції PUSHAD і PUSHFD на початку code cave, ми зможемо зберегти всі регістри й прапори регістрів усередині стека. Ці значення

будуть повернуті після виконання коду вірусу, і програма продовжить виконання без яких-небудь проблем.

Як було згадано раніше, наш бекдор являє собою зворотний tcp-шелл-код під meterpreter, узятий із проекту metasploit. Однак буде потрібно деякі зміни усередині шелл-коду. Звичайно зворотний tcp-шелл-код намагається приєднатися до оброблювача деяка кількість разів, і якщо з'єднатися не вдалося, процес закривається за допомогою виклику API-функції ExitProcess.

Проблема полягає в тім, що якщо з'єднатися з оброблювачем не вийде, виконання клієнта putty буде зупинено. Після внесення невеликих змін після невдачі шелл-код буде знову намагатися з'єднатися з оброблювачем. До того ж, небагато зменшиться розмір шелл-коду.

Після внесення змін усередині асемблерного коду виконуємо компіляцію за допомогою команди `nasm -f bin stager_reverse_tcp_nx.asm`. Тепер зворотний tcp-шелл-код готовий до вживання, але поки ще не поміщений у правильне місце. Наша мета – здійснити виконання в окремому потоці, для створення якого буде потрібно окремий шелл-код, що виконує виклик API-функції CreateThread. Функція буде вказувати на первісний зворотний tcp-шелл-код.

Після приміщення байтів шелл-коду усередину файлу `createthread.asm` у шістнадцятковому форматі, як показано на рисунку вище, виконуємо компіляцію за допомогою команди `nasm -f bin createthread.asm`. Тепер шелл-код готовий для впровадження в code cave, але перед вставкою варто виконати кодування для того, щоб обійти статичний/сигнатурний аналіз антивірусу. Оскільки всі кодувальники із проекту metasploit відомі більшості антивірусів, рекомендується використовувати нестандартне кодування. У даній роботі не буде розказано про створення нестандартних кодувальників, але можна обійтися сполученням декількох кодувальників із проекту metasploit. Після кожного акту кодування завантажуюмо шелл-код у проект Virus Total в «сиром» форматі й перевіряємо результати перевірки. Комбінуємо кодувальники доти, поки шелл-код стане повністю непомітним.

Після правильного кодування шелл-код готовий до впровадження усередину code cave. Вибираємо інструкцію, яка треба за інструкцією PUSHFD, і натискаємо Ctrl+E в відладнику Immunity Debugger. Шелл-код буде вставлений у шістнадцятковому форматі.

Одержати закодований шелл-код у шістнадцятковому форматі можна двома способами: вивести на печатку за допомогою команди `xxd -ps createthread` або відкрити й скопіювати в шістнадцятковому редакторі. При копіюванні шістнадцяткових значень в відладник Immunity Debugger не забувайте про обмеження на копіюємі байти, які присутні при вставці коду. Необхідно запам'ятати останні два вставлених байти, і після натискання на кнопку ОК потрібно зробити повторне копіювання наступних ділянок. Коли шелл-код повністю вставлений в code cave, операцію по впровадженню можна вважати завершеною.

Відновлення потоку виконання

Після створення потоку виконання бекдору необхідно відновити виконання програми. Тобто регістр EIP повинен вказувати на функцію, що перенаправляла виконання на code cave. Однак перед переходом на цю функцію варто відновити раніше збережені регістри.

Помістивши інструкції POPFD і POPAD у кінець шелл-коду, ми відновимо усе раніше збережені регістри зі стека в тім же порядку. Після відновлення регістрів необхідно згадати ще про один нюанс. При перехопленні потоку виконання інструкція PUSH 467C7C була замінена на інструкцію JMP 0x47A478 для того, щоб перенаправляти виконання на code cave. При приміщенні інструкції PUSH 467C7C у кінець коду, перехоплена інструкція також відновиться. Тепер прийшов час повернутися до функції, що перенаправляла виконання до code cave за допомогою вставки інструкції JMP 0x41CB73. Кінець результуючого коду повинен виглядати, як показано існує.

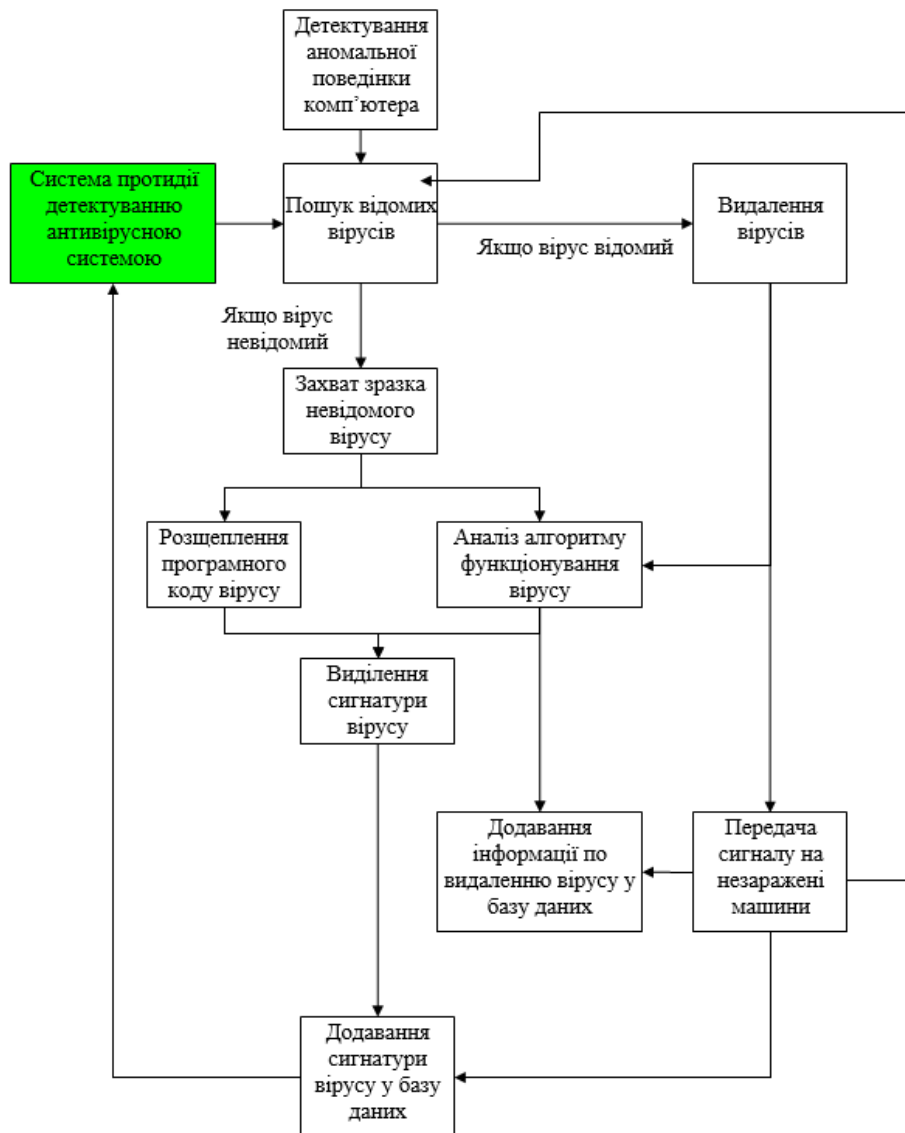


Рисунок 1 – Структурна схема системи

Потім виділяємо всі змінені й вставлені інструкції, натискаємо праву кнопку миші й копіюємо у виконується файл, що. Ця операція повинна бути пророблена з кожною модифікованою інструкцією. Коду всі інструкції скопійовані й збережені у файл, закриваємо відладник і тестуємо нашу творчість. Якщо виконання проходить без помилок, бекдор готовий до вживання.

У завершенні рекомендується змінити контрольну суму файлу, що вийшов, щоб зберегти автентичність і не викликати зайві підозри.

Якщо всі описані методи використані правильно, готовий бекдор буде повністю непомітним. На закінчення будуть наведені контрзаходи для захисту від описаних раніше технік. Це методи будуть корисні адміністраторам, аналітикам вірусів і розроблювачам антивірусів.

Контроль над привілеями секцій

Коли мова заходить про заражені файли, у першу чергу варто думати про детектуванні аномалій, пов'язаних із привілеями секцій. За замовчуванням компілятори ніколи не встановлюють повні права на секції, якщо тільки програміст не виставив спеціальні налаштування. Особливо не повинні мати привілеїв на виконання секції даних: .data і .rdata. Крім того, секції коду (наприклад, .text) не повинні мати прав на запис. Подібні аномалії, пов'язані зі зміною привілеїв, варто розглядати як підозріле поведження.

Присутність нестандартних секцій

Якщо програміст не вносить зміни в конфігурацію, компілятори звичайно створюють 5-6 стандартних типів секцій. В усі продукти, пов'язані з безпекою, повинен бути впроваджений механізм виявлення нестандартних і підозрілих секцій. Даний механізм повинен стежити за ентропією й вирівнює дані усередині секції. Якщо секція містить високу ентропію й нестандартно впорядковану інформацію, це ще одна підозріла ознака.

Перевірка сигнатур

Незважаючи на те, що ця техніка стара як світ, метод є дуже ефективним при перевірці файлів, що завантажуються з інтернету. Перевірка сигнатури sha1 – один з найбільш надійних способів уникнути зараження системи.

Перевірка контрольної суми файлу

Якщо є розходження між контрольною сумою усередині заголовка образу й поточною контрольною сумою файлу, це означає, що файл був змінений. У системи безпеки варто впровадити механізм перевірки автентичності файлу за допомогою порівняння поточної контрольної суми й контрольної суми заголовка образу.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів протидії детектуванню антивірусною системою за допомогою штучного інтелекту. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем протидії детектуванню антивірусною системою за допомогою штучного інтелекту.
- Досліджена система протидії детектуванню антивірусною системою за допомогою штучного інтелекту.
- На основі отриманих результатів досліджень створена програмна реалізація системи протидії детектуванню антивірусною системою за допомогою штучного інтелекту.

Розроблені алгоритми дозволяють успішно вирішувати завдання протидії детектуванню антивірусною системою 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. Вінтенко Б.Ю., Миронець І.В., Смірнов О.А. «Модель комп'ютерно-орієнтованої процедури системи підтримки оперативного персоналу АЕС». IV Міжнародна науково-практична Інтернет-конференція «Інновації та перспективні шляхи розвитку інформаційних технологій (ІПШРІТ-2025)» м.Черкаси 25 листопада 2025 року – Черкаси: ЧДТУ.– 2025. – С.101-103.
2. 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.
3. 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.
4. 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.
5. 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
6. 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.
7. 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.
8. 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.
9. Al-Azzeh, J., Ayyoub, B., Mesleh, A., Smirnova, T., Gnatyuk, S., Drieiev, O., Smirnov, O., Dorenskiy, 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.
10. 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». *Центральноукраїнський науковий вісник. Технічні науки*. 2025. Вип. 11(42), ч. II. С.52-62.
 11. 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.
 12. Смірнов, О.А., Константинова, Л.В., Коноплицька-Слободенюк, О.К., Козірова, Н.В., Якименко, Н.М., Доренський, О.П., Буравченко, К.О. «Дослідження інструментів підтримки штучного інтелекту для роботи з базами даних та аналізу даних». *Кібербезпека: освіта, наука, техніка*. 2025. №3(27), С. 429–448.
 13. 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.
 14. 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.
 15. 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.
 16. 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.
 17. 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.
 18. 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.
 19. 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.
 20. 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.
 21. 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.
 22. 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.
 23. 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.
 24. 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.
 25. 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>.
 26. 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.
 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., 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.
 31. 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.

УДК 004

С.Коробка, магістр гр. КІ-24М,*Центральноукраїнський національний технічний університет*

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КРИТИЧНИХ РЕСУРСІВ АСУ ТП

У статті розроблено програмне забезпечення, яке призначено для системи забезпечення безпеки критичних ресурсів АСУ ТП. Метою розробки є дослідження та принципи побудови системи забезпечення безпеки критичних ресурсів АСУ ТП. Об'єктом дослідження є процес забезпечення безпеки критичних ресурсів АСУ ТП. Предметом дослідження є методи забезпечення безпеки критичних ресурсів АСУ ТП. Методи дослідження базуються на методах захисту інформації у комп'ютерних мережах, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи забезпечення безпеки критичних ресурсів АСУ ТП. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

забезпечення безпеки, критичні ресурси, АСУ ТП

Постановка проблеми. У наші дні практично в будь-якому виробництві використовуються автоматизовані системи управління технологічними процесами (АСУ ТП). Однак автоматизація без виконання вимог інформаційної безпеки може бути критично небезпечним. Розглянемо, чому захист АСУ ТП сьогодні став особливо важливим, які погрози зараз найбільш реальні, і як захистити промислові інфраструктури від зловмисників. Автоматизована система управління технологічними процесами (АСУ ТП) – це ціла група технічних і програмних засобів, призначених для автоматизації процесів управління технологічним устаткуванням на промислових підприємствах. Сьогодні багато експертів одностайні в тому, що основна погроза – це втручання терористичних, екстремістських і вороже настроєних груп у управління автоматизованими системами критично важливих об'єктів, у тому числі й з метою виводу їх з ладу. Деякі експерти зараз прогнозують, що терористичні організації будуть купувати технічну інформацію компаній для здійснення атак. Тому державам так важливо вчасно убезпечити себе від подібних погроз. Галузі, для яких тема захисту АСУ ТП найбільш критична – ті, де можливий максимальний збиток і може постраждати найбільша кількість людей. У першу чергу, це енергетичні компанії й підприємства ПЕК – отут можливі як економічні наслідки, наприклад, порушення поставок нафти або газу, або перебої в електропостачанні населення, так і екологічні або гуманітарні катастрофи. Крім того, під погрозою перебуває транспорт. Ці галузі мають широку розгалужену мережу по всій країні, і безпека на подібних підприємствах – стратегічно важливе завдання для держави.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи забезпечення безпеки критичних ресурсів АСУ ТП.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи забезпечення безпеки критичних ресурсів АСУ ТП.

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

- Огляд існуючих систем забезпечення безпеки критичних ресурсів АСУ ТП.
- Дослідження системи забезпечення безпеки критичних ресурсів АСУ ТП.

- Програмна реалізація системи забезпечення безпеки критичних ресурсів АСУ ТП.
- Об'єктом дослідження* є процес забезпечення безпеки критичних ресурсів АСУ ТП.
- Предметом дослідження* є методи забезпечення безпеки критичних ресурсів АСУ ТП.

Методи дослідження базуються на методах захисту інформації у комп'ютерних мережах, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Системи безпеки АСУ ТП найбільш актуальні в розвинені з погляду промислової автоматизації галузях – це енергетика, нафтогазова галузь, транспорт, металургія, машинобудування. Безпека всієї промислової мережі й АСУ ТП забезпечується застосуванням комплексного послідовного підходу, що враховує специфіку й особливості промислових систем, і заснованого на вимогах і рекомендаціях як міжнародних стандартів, так і українських нормативних документів з забезпечення інформаційної безпеки промислових систем.

Комплексний підхід означає також проведення регулярного аудита стану захищеності АСУ ТП на основі інтерв'ювання фахівців підприємства, аналізу документації, структури й конфігурації систем, а також проведення інструментального аналізу захищеності з метою пошуку уразливостей. На основі отриманих за підсумками аудита даних виробляється аналіз ризиків, у результаті якого визначаються погрози, що представляють небезпеку функціонуванню об'єкта.

Класифікація рішень для інформаційної безпеки АСУ ТП

Приступаючи до побудови архітектури рішення, у першу чергу, варто підібрати вірний тип базового продукту. Умовно всі рішення ІБ АСУ ТП можна розділити на дві категорії:

- Системи моніторингу активності й виявлення погроз. Вони забезпечують тільки моніторинг, нічого не блокують, але стежать за погрозами й проблемами, виявляють їх і повідомляють служби безпеки.

Системи моніторингу активності також підрозділяються по класах, серед них:

- система виявлення комп'ютерних атак і мережних аномалій;
- система моніторингу подій інформаційної безпеки й бездротових мереж;
- система пасивного аналізу уразливостей;
- система аналізу конфігурацій устаткування, правил доступу мережного встаткування;
- а також система контролю цілісності даних і ПЗ.

Наприклад, перші з них, системи виявлення комп'ютерних атак і мережних аномалій, аналізують мережний трафік і виділяють із нього інформацію про мережні потоки (flow), аналіз якої більше ефективний для виявлення погроз у порівнянні із сигнатурними методами й дозволяє виявити в тому числі й атаки на невідомі (zero day) уразливості й вчасно реагувати на підозрілі інциденти.

- Системи запобігання погроз (або управління доступом).

Ще одна класифікація систем інформаційної безпеки АСУ ТП – це розподіл їх на традиційні й спеціалізовані. Класичні системи ІБ можуть використовуватися на промислових підприємствах для побудови архітектури, управління інформаційними потоками. Друга група рішень – спеціалізовані, підходять для компаній важкої промисловості. Це металургія, енергетика, нафтогаз, де більше агресивне середовище (температура, магнітні випромінювання, пил). Якщо системи безпеки перебувають безпосередньо на промислових об'єктах, отут повинні застосовуватися додаткові умови, ураховуватися специфічні вимоги середовища, застосовуватися спеціальний монтаж промислового встаткування, стійке до агресивних середовищ виконання й т.д. Грубо говорячи, спеціалізовані системи повинні бути «розумними», повинні розбиратися в промисловому трафіку, ураховувати саме програмне забезпечення, трафік промислових систем. Однак це не виходить, що традиційні системи безпеки не застосовуються на промислових підприємствах.

На жаль, сьогодні основна проблема безпеки АСУ ТП – це відсутність уваги до її забезпечення. Через те, що технологічні мережі найчастіше досить статичні, не прийняте щонебудь міняти, устаткування застаріває, використовуються старі версії програмних продуктів і операційних систем з безліччю уразливостей. Відсутність уваги до ІБ проявляється й у безконтрольному використанні периферійних пристроїв, флеш-накопичувачів, відсутності політик захисту АСУ ТП і відповідальних осіб.

Також усе реальніше стає ймовірність кібертероризму. У прогнозі МНС про надзвичайну обстановку на території України відзначається, що в цей час рівень інформаційної безпеки не відповідає рівню погроз у даній сфері, і в 2018 році можливе підвищення хакерських атак з метою створення умов для виникнення техногенних надзвичайних ситуацій. Тому в той час, поки ринок захисту АСУ ТП поки тільки дозріває, важливо нарощувати компетенції для надання ефективної допомоги замовникам у побудові комплексних систем управління й забезпечення інформаційної безпеки.

Сучасним трендом АСУ ТП є впровадження Інтернету речей. Рішення в області Інтернету речей будуються на базі мікропроцесорних систем з використанням різного роду ПЗ, що реалізує, у тому числі, і сучасні технології підключення до зовнішніх мереж зв'язку, які працюють по стандартизованих протоколах. Будь те Wi-fi або Bluetooth. Із цієї позиції різниця між офісною мережею або розумним будинком – невелика. І в того, і в іншого – є можливість підключення до інтернету, наприклад, для віддаленого моніторингу й управління. Але як тільки з'являється підключення до інтернету й програмний рівень, то неминуче виникають і помилки, якими можуть скористатися зловмисники. Тому підходи до забезпечення інформаційної безпеки нових застосувань ІТ повинні бути аналогічні підходам, застосовуваним у класичних випадках забезпечення інформаційної безпеки.

Ринку ще має бути розвиток убік виробництва засобів захисту, які могли б елегантно вбудовуватися в ІТ-контур «розумних» систем, аналогічно тому, як це відбувається із захистом корпоративних систем. Зараз виробники тільки починають вишиковувати в себе життєвий цикл розробки й супроводу компонентів «розумних» систем, що враховує можливість здійснення у відношенні їх несанкціонованих впливів, включаючи тестування на предмет наявності уразливостей.

Все залежить від того, наскільки й із чим інтегровано те, до чого виходить доступ, і хто власник пристрою. Наприклад, якщо говорити про розумний будинок – можна спробувати одержати доступ до конфіденційних даних домовласника, або, також відключивши сигналізацію, проникнути в будинок. У випадку з виробничим підприємством і промисловим Інтернетом речей – також є ризики. Промислові системи, невідомо підключені до інтернету, – це дуже небезпечне явище, що може привести не тільки до зупинки технологічного процесу, але й регіональній катастрофі. Тому виробництво змушене балансувати на тонкій грані між безпекою й автоматизацією. Наприклад, відповідно до інформації, на Shodan – ресурсі, що самостійно сканує Всесвітню мережу й надає інформацію про те, які користувальницькі й промислові пристрої підключені до інтернету із вказівкою їхніх протоколів, доступ через інтернет можливий до цілого ряду критичних пристроїв, починаючи від медичних, закінчуючи системами управління будинками, сонячною енергетикою, розумними будинками та ін.

Застосування технологій IoT досить актуально для ЖКГ (за рахунок інтернету речей можна знизити енерго- і теплоспоживання в житлових будинках), для управління міською інфраструктурою (включаючи транспорт, висвітлення й т.д.), у сільському господарстві (для підвищення врожайності ґрунту й відстеження її параметрів), а також для промислового сектора, де збір і аналіз різних даних дозволяє, зокрема, звістки моніторинг стан устаткування й вчасно попереджати його поломку.

При зваженому підході до реалізації захисту з виявленням основних погроз і вбудовуванням в існуючу систему технологій захисту інформації, безумовно, строки впровадження можуть бути трохи збільшені. Однак мінімізація ризиків, що обіцяє рішення питань безпеки, безумовно, цього коштує.

Насправді, напрямок промислового Інтернету речей у нашій країні тільки починає розвиватися. А раз немає публічних проєктів, те немає й інформації про відповідні інциденти в області інформаційної безпеки. Але світових випадків злому промислових систем досить багато. Наприклад, кілька інцидентів було в США. А у звіті Центра досліджень ризиків Кембриджського університету США в 2015 році відзначалося, що якщо зловмисники атакують кілька сегментів американської енергомережі, у результаті чого 15 штатів і Вашингтон без електрики, те економічні втрати можуть досягти \$1 трлн. доларів.

Інший відомий випадок відбувся в Європі. У грудні 2014 року в Німеччині була зроблена атака на металургійний завод. Хакерам удалося віддалено вивести з ладу доменну піч, що привело до поломки встаткування. Наскільки відомо, атака складалася з декількох проникнень у системи заводу, і в результаті одна з печей перестала бути керованою. Швидше за все, цей напад було цілеспрямованим, а самі зловмисники – підкованими й в області ІТ, і в області контрольних систем великих промислових підприємств.

Ще приклад – атака із зараженням вірусом Stuxnet декількох ядерних об'єктів Ірану в 2010 році. У результаті було уражено біля третини центрифуг на заводі по збагаченню урану, а також зірвані строки запуску ядерної АЕС. Це, мабуть, найгучніший випадок на сьогодні.

З більше наближених до України випадків – кібератака на українських постачальників електроенергії, «Прикарпатьеобленерго» і «Київенерго», що привела до перебоїв з електрикою. Проте, хоч на об'єктах і було виявлене шкідливе ПЗ BlackEnergy, однак явних доказів тому, що атакуючі скористалися ним для проникнення в технологічну мережу, поки, наскільки я знаю, немає.

З огляду на той факт, що тематика захисту АСУ ТП – автоматизованих систем управління технологічними процесами – зараз набирає популярність. Цей момент також знайшов відбиття в оновленій доктрині інформаційної безпеки, де особлива увага приділяється блоку погроз із боку закордонних країн у плані впливу на критичну інформаційну інфраструктуру України, підприємства оборонно-промислового комплексу та ін. До речі, показово, що й у недавно проведеному опитуванні 18 з 100 опитаних керівників великих українських компаній також бачать погрозу з боку іноземних урядів.

Тому, сподіваюся, що в самому найближчому майбутньому при впровадженні технологій Інтернету речей безпека буде стояти на чолі кута. Адже зовсім точно можна сказати, що витрати на інформаційну безпеку не порівнянні з можливими негативними наслідками. Адже якщо не боротися з виникаючими погрозами, виникають ризики тимчасової зупинки виробництва, повної втрати бізнесу й навіть катастроф.

Багато чого залежить від того, що диктує ринок. Зокрема, мобільні телефони існують досить давно, але користувальницьких засобів захисту дотепер не так вуж багато, а випадки проникнення вірусів або доступу зловмисників до банківських даних через мобільні пристрої трапляються регулярно. Так може бути й у випадку з Інтернетом речей. Однак, чим перспективніше напрямок, чим більше голосних проєктів реалізується (у які застосовуються спеціалізовані програмні платформи, використовуються архітектурні підходи IoT, бездротові протоколи й т.п.), тим швидше йде процес створення інструментів по захисту даних.

Моніторинг аномалій мережної активності в промислових системах

У сфері забезпечення ІБ промислових систем важливим завданням є вибір ефективних заходів і засобів захисту, які повинні запобігати несанкціонованому доступу до управління технологічними процесами, але не створювати перешкоди для роботи АСУ. Домагатися цього дозволяють рішення, що забезпечують безперервне пасивне спостереження за активністю в промислових системах і мережах, виявлення потенційних погроз і оперативне повідомлення відповідальних служб про виникаючі проблеми. Серед таких рішень можна виділити системи виявлення аномалій мережної активності (Network Behavior Anomaly Detection), застосування яких у промислових системах активно обговорюється експертним співтовариством.

Основною перевагою систем аналізу аномалій є їхнє пасивне застосування. Компоненти систем, відповідальні за збір мережного трафіку, підключаються до

дзеркалюючих (SPAN) портів мережних комутаторів або безпосередньо до мережі через TAP-пристрої (це дозволяє не створювати мережні навантаження й не породжує затримок у роботі сервісів) і не взаємодіють прямо із промисловим устаткуванням. Такі системи аналізують мережний трафік і виділяють із нього інформацію про мережні потоки (Flow). Аналіз Flow-статистики більше ефективний для виявлення погроз, чим сигнатурні методи, оскільки дає можливість виявляти, у тому числі, атаки на невідомі (zero day) уразливості, сигнатури для яких ще не випущені.

Є й інші переваги. З обліком того, що штатна взаємодія пристроїв у промисловій мережі повинне бути статичним протягом тривалого часу, розгортання систем виявлення аномалій, їх «навчання», запуск в «бойовому» режимі й безперервній експлуатації значно спрощуються, оскільки не потрібні часті зміни профілю нормального поведіння. Нарешті, робота систем аналізу аномалій дозволяє оцінити реальний рівень безпеки й виявити проблеми в системі забезпечення ІБ промислової мережі, причому результати аналізу можуть стати основою її вдосконалювання.

Системи класу Network Behavior Anomaly Detection (NBAD) добре зарекомендували себе при захисті офісних мереж і ЦОДів. Серед пропозицій є як комерційні (наприклад, Lancorp StealthWatch, Arbor Networks Pravail NSI, McAfee Network Threat Behavior Analysis), так і безкоштовні (FlowMatrix, FlowBAT, Bro) рішення.

Функціонал цих систем містить у собі наступні можливості:

- виявлення підключення мережних пристроїв і побудова карти мережі;
- створення профілю нормальної мережної взаємодії;
- моніторинг мережної активності в режимі 24/7 для виявлення аномального поведіння (аномальні з'єднання, пристрої, час і обсяги трафіку й інші показники);
- виявлення зовнішніх і внутрішніх (пов'язаних з навмисними або помилковими діями персоналу) погроз;
- оперативне оповіщення відповідальних служб про проблеми й передача інформації про їх у суміжні системи безпеки;
- ведення історії змін мережного поведіння й допомога при розслідуванні інцидентів;
- формування звітів з різними рівнями деталізації.

Експерти затверджують, що своєчасне застосування рішень, що забезпечують моніторинг мережної активності, дозволило б виявити активність шкідливого ПЗ Stuxnet, Havex і BlackEnergy, оскільки в таких випадках мережне поведіння виходить за рамки нормальної взаємодії пристроїв у мережі. Наприклад, не залишилися б непоміченими спроби відновлення прошивання контролера по мережі або збору даних. Незважаючи на всю користь і ефективність традиційних NBAD-систем, вони не можуть виявляти аномальний уміст прикладних промислових протоколів. Ріст числа погроз для систем промислової автоматизації привів до того, що на ринку стали з'являтися рішення, адаптовані для роботи саме в промислових мережах. Їхня робота заснована на тім же принципі пасивного збору трафіку, але вони здатні аналізувати промислові протоколи (deep packet inspection) і виявляти в них аномальні дані. У деяких джерелах цей клас рішень одержав назву Industrial Network Anomaly Detection (INAD).

Зараз відомі наступні закордонні рішення: Dragos Security CyberLens, NexDefense Sophia, C4 Security Fides, SCADAfense. Ці рішення перебувають на різних стадіях зрілості. Деякі з них існують уже кілька років (наприклад, NexDefense Sophia), а деякі – тільки анонсовані (зокрема, SCADAfense). У кожному разі помітний інтерес виробників і замовників до рішень цього класу.

Розглянуті системи підтримують як відкриті, так і пропрієтарні промислові протоколи, у тому числі DNP3, ModbusTCP, Profinet, ISO-TSAP, AB-PCCC, BACNet, Ethernet / IP і інші. У різних продуктах підтримувані протоколи й функціональні можливості розрізняються.

У загальному виді системи даного класу дозволяють виявляти наступні види активності:

- нелегітимні команди й мережний трафік, що виводять із ладу системи управління;
- присутність у промисловій мережі шкідливого ПЗ, локалізація вогнищ зараження;
- дії зловмисників у промисловій мережі без використання шкідливого ПЗ;
- керуючі команди, що приводять до порушень технологічного процесу;
- команди на зупинку / перезавантаження / перепрошивання / переконфігурацію контролерів;

– команди, що встановлюють неприпустимі / небажані значення ключових параметрів управління технологічним процесом.

З особливостей застосування таких систем відзначимо наступні. Їм потрібне значний час на первісний збір даних для побудови профілю нормального поведіння й завдання базової політики безпеки. Але це – плата за невикористання активного сканування, що може створювати проблеми в роботі промислової мережі. Крім того, для підключення до SPAN-порту мережного комутатора або підключення TAP-пристрою, що необхідно для пасивного збору трафіку, потрібне активна взаємодія з мережним устаткуванням (конфігурація, установка в розрив). Однак імовірність того, що ці дії й подальша робота системи приведуть до проблем, украй мала. Ефективність систем безпеки в цьому випадку незрівнянно вище ризику від їхнього застосування.

Крім систем, орієнтованих на пошук аномалій у мережному трафіку промислових мереж, стали з'являтися цікаві рішення, націлені на безконтактне виявлення аномалій у роботі промислового встаткування (такий функціонал забезпечує PFP Cybersecurity). Останнє завдання реалізується шляхом спостереження за енергоспоживанням процесора.

Безумовно, вибір конкретного продукту повинен здійснюватися на основі аналізу індивідуальних вимог замовника, особливостей промислових систем і мереж, типу промислового об'єкта. Конче потрібно й ретельне тестування продукту до його введення в експлуатацію. Однак вибір рішень на ринку однозначно є.

Інтеграція бізнес-додатків з виробничими процесами, впровадження рішень класу MES, ERP, розвиток мережних комунікацій між офісними й промисловими сегментами, використання ОС Windows / Linux і IP-протоколів – все це створює потенційну погрозу несанкціонованого доступу до промислових систем з непередбаченим збитком.

Аудит безпеки й аналіз захищеності

Містить у собі аналіз документації, структури й конфігурації систем, проведення інтерв'ю фахівців замовника, а також аналіз захищеності інфраструктури підприємства з визначенням існуючих уразливостей. Підсумковий звіт містить вичерпну інформацію з поточного стану інформаційної безпеки, опис існуючих погроз і рекомендації із протидії їм, методику й опис ходу роботи. У ході аудиту перевіряється практична реалізація вимог і рекомендацій IEC 62443, NIST SP 800-82r2, і інших українських і міжнародних стандартів з забезпечення інформаційної безпеки промислових систем.

Побудова системи управління інформаційною безпекою

Розробляється комплексна система управління інформаційною безпекою (СУІБ) підприємства, у тому числі політикові інформаційної безпеки, корпоративні стандарти й нормативна документація, що регулює процеси управління ІБ. Додатково персонал замовника проходить навчання правилам інформаційної безпеки промислових систем.

Побудова системи забезпечення інформаційної безпеки

Система забезпечення ІБ виявляє й блокує спроби несанкціонованого доступу до технологічної інформації й управління промисловими системами. При її створенні враховуються тенденції розвитку сучасних промислових систем при підключенні до Інтернету, організації віддаленого доступу до встаткування Dial-UP, підключенні до корпоративної мережі, використанні бездротових мереж UMTS / HSDPA / ZigBee / WiFi.

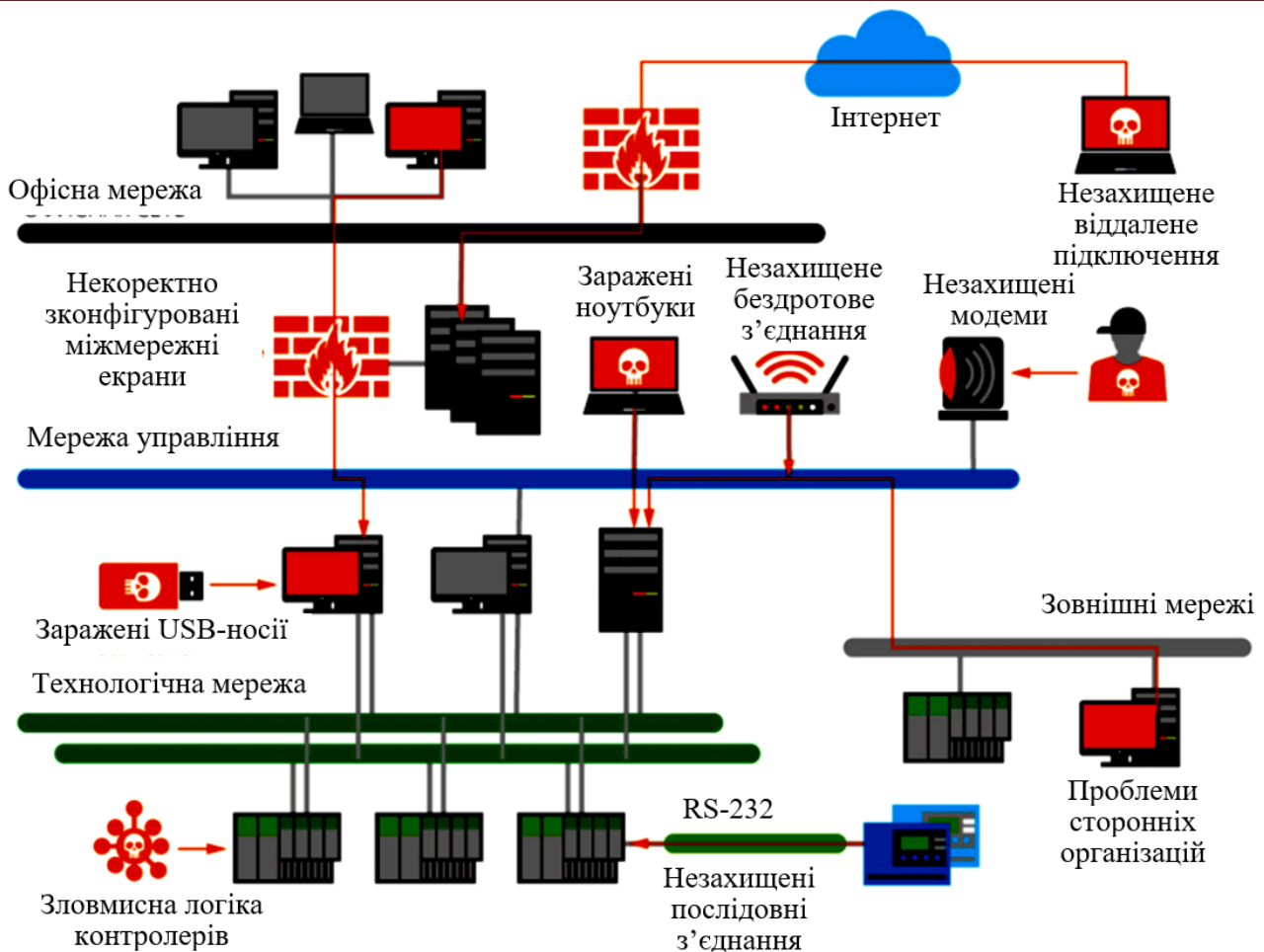


Рисунок 1 – Структурна схема системи

На структурній схемі системи наведена типова мережа промислового підприємства й основні погрози інформаційної безпеки.

Під захист попадають основні компоненти промислових систем: робітники станції операторів і інженерів, сервери SCADA і архіву, програмувальні логічні контролери, інтелектуальні виконавчі пристрої й датчики, промислове мережне встаткування, канали зв'язку, шлюзи віддаленого доступу й інші компоненти. Арсенал використовуваних засобів містить у собі односпрямовані шлюзи, промислові міжмережні екрани, рішення для розвідки кіберзагроз, виявлення мережних атак і аномалій, контролю команд, що відправляються на контролери АСУ ТП, системи контролю запуску додатків на серверах і автоматизованих робочих місцях (АРМ) операторів АСУ ТП, сервіси розвідки кіберзагроз.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів забезпечення безпеки критичних ресурсів АСУ ТП. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем забезпечення безпеки критичних ресурсів АСУ ТП.

- Досліджена система забезпечення безпеки критичних ресурсів АСУ ТП.

- На основі отриманих результатів досліджень створена програмна реалізація системи забезпечення безпеки критичних ресурсів АСУ ТП. Розроблені алгоритми дозволяють успішно вирішувати завдання забезпечення безпеки критичних ресурсів АСУ ТП. 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. 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. 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.
6. Al-Azzeh, J., Ayyoub, B., Mesleh, A., Smirnova, T., Gnatyuk, S., Drieiev, O., Smirnov, O., Dorenskyi, O. «Cloud-Based Information System for Evaluating Cavities in the Process of Blasting Metal Surfaces of Details». International Review on Modelling and Simulations 18 (1), 2025. pp. 32-42.
7. 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.
8. 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.
9. 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.
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. 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. 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.
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. 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.
18. 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.
19. 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.

20. 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.
21. 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.
22. 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.
23. 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.
24. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
25. 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.
26. 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.
27. 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.
28. 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.
29. 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.
30. 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.
31. 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.
32. 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.
33. 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.
34. 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.

УДК 004

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

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ІНТЕЛЕКТУАЛЬНОЇ ОПТИМІЗАЦІЇ ПРОДУКТИВНОСТІ ТА НАДІЙНОСТІ ХМАРНИХ МЕРЕЖЕВИХ СИСТЕМ ЗБЕРІГАННЯ ДАНИХ

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

інтелектуальна оптимізація, продуктивність, надійність, хмара, мережева система, зберігання даних

Постановка проблеми. Мережевий накопичувач (NAS) – це система жорстких дисків, підключена до вашої локальної мережі, а не до окремого комп'ютера. Це дозволяє будь-кому, хто знаходиться у вашому місці розташування, отримувати доступ до файлів, а деякі конфігурації пропонують можливості віддаленого доступу.

Системи NAS зазвичай поєднують кілька дисків, щоб вони виглядали як один великий пристрій зберігання даних. Залежно від конфігурації, вони можуть створювати системи швидше, ніж диски настільних комп'ютерів, або збільшувати резервування даних, щоб збої дисків не руйнували вашу роботу – деякі роблять і те, і інше.

Хоча традиційно вони будуються на фізичних жорстких дисках, сучасні системи NAS підтримують SSD або комбінації SSD/жорсткий диск. Такий гібридний підхід пришвидшує передачу даних, водночас знижуючи витрати, ніж у конфігураціях, що використовують виключно SSD.

Навіть для окремих користувачів NAS забезпечує величезне сховище та резервування даних, що забезпечує спокій. Багато домашніх NAS-систем включають функції потокової передачі медіа, що дозволяє транслювати телебачення та фільми по всій мережі.

Незалежно від того, чи редагуєте ви відео 8K, архівуєте бібліотеки фотографій, чи потребуєте розширюваного безпечного сховища, NAS – це ідеальний центр для творчих робочих процесів.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи інтелектуальної оптимізації продуктивності та надійності хмарних мережесистем зберігання даних.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи інтелектуальної оптимізації продуктивності та надійності хмарних мережесистем зберігання даних.

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

- Огляд існуючих систем інтелектуальної оптимізації продуктивності та надійності хмарних мережевих систем зберігання даних.

- Дослідження системи інтелектуальної оптимізації продуктивності та надійності хмарних мережевих систем зберігання даних.

- Програмна реалізація системи інтелектуальної оптимізації продуктивності та надійності хмарних мережевих систем зберігання даних.

Об'єктом дослідження є процес інтелектуальної оптимізації продуктивності та надійності хмарних мережевих систем зберігання даних.

Предметом дослідження є методи інтелектуальної оптимізації продуктивності та надійності хмарних мережевих систем зберігання даних.

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

Виклад основного матеріалу. Розуміння різних типів мережевих сховищ є важливим для ефективного керування даними. У цій статті буде розглянуто різні типи мережевих сховищ, включаючи мережеві сховища (NAS), мережі зберігання даних (SAN), безпосередньо підключені сховища (DAS), хмарні сховища, розподілені файлові системи та об'єктні сховища. У цьому розділі розглядаються ці типи мережевих сховищ, а також надається уявлення про їхні функції, переваги та застосування, щоб допомогти вам приймати обгрунтовані рішення, адаптовані до ваших потреб у управлінні даними.

Типи мережевих сховищ відіграють вирішальну роль у сучасній IT-інфраструктурі, надаючи організаціям масштабовані та ефективні стратегії управління даними. Мережі зберігання даних (SAN), мережеві сховища даних (NAS) та сховища даних з прямим підключенням (DAS) представляють собою різні підходи до зберігання та доступу до даних, кожен з яких має унікальні характеристики, адаптовані до різних операційних потреб.

SAN пропонують високошвидкісне сховище на рівні блоків, яке зазвичай використовується в корпоративних середовищах, що вимагають високої продуктивності та централізованого управління сховищем.

Системи NAS забезпечують сховище на рівні файлів, доступне через мережеві протоколи, що робить їх ідеальними для спільних файлових середовищ та спільних робочих просторів. На відміну від них, DAS підключає пристрої зберігання даних безпосередньо до певного сервера або комп'ютера, пропонуючи простіше та економічніше рішення для потреб меншого обсягу сховища.

Ці технології зберігання відрізняються своєю архітектурою, доступністю, масштабованістю та продуктивністю, що дозволяє IT-фахівцям вибирати найбільш підходяще рішення на основі конкретних вимог організації до зберігання даних, продуктивності та доступності.

Розуміння мережевого сховища (NAS)

Мережеве сховище даних (NAS) – це спеціальний тип сховища, яке підключається до мережі. Воно надає багатьом користувачам і пристроям простий спосіб зберігання, доступу та обміну файлами. Це робить його чудовим варіантом як для домашнього, так і для комерційного використання.

Переваги NAS:

- Легкий доступ: Користувачі можуть отримувати доступ до файлів з будь-якого пристрою, підключеного до мережі.

- Централізоване сховище: усі файли зберігаються в одному місці, що спрощує керування ними.

- Економічно ефективні: NAS-системи, як правило, дешевші за інші рішення для зберігання даних.

Обмеження NAS:

- Проблеми зі швидкістю: Якщо забагато користувачів одночасно отримують доступ до NAS, це може призвести до уповільнення його роботи.
- Залежність від мережі: якщо мережа виходить з ладу, доступ до файлів втрачається.
- Обмежена продуктивність: Не така швидка, як у сховищ із прямим підключенням (DAS) для важких завдань.

Випадки використання NAS:

- Домашнє використання: Люди використовують NAS для зберігання фотографій, відео та музики.
- Малий бізнес: Це допомагає в обміні документами та резервному копіюванні даних.
- Віддалена робота: команди можуть легко отримувати доступ до файлів з різних місць.

Таким чином, NAS – це гнучкий та ефективний спосіб керування даними для різних потреб, що робить його популярним вибором для багатьох користувачів.

Дослідження мереж зберігання зон (SAN)

Огляд архітектури SAN

Мережа зберігання даних (SAN) – це спеціальний тип мережі, яка з'єднує пристрої зберігання даних із серверами. Така конфігурація дозволяє кільком серверам отримувати доступ до спільного сховища, ніби це локальний диск. SAN призначені для ефективної обробки великих обсягів даних, що робить їх важливими для підприємств, яким потрібен швидкий доступ до інформації.

Переваги SAN:

- Висока продуктивність: мережі SAN забезпечують високу швидкість передачі даних, що є критично важливим для програм, яким потрібен швидкий доступ до великих файлів.
- Масштабованість: компанії можуть легко додавати більше пристроїв зберігання даних до мережі зберігання даних, не порушуючи існуючі операції.
- Централізоване управління: мережі SAN дозволяють легше керувати ресурсами зберігання даних, що спрощує розподіл простору та моніторинг їх використання.

SAN проти NAS

Підсумовуючи, хоча SAN та NAS пропонують рішення для зберігання даних, вони задовольняють різні потреби. SAN ідеально підходять для високопродуктивних середовищ, тоді як NAS більше підходить для загального зберігання та обміну файлами.

Огляд безпосередньо підключених сховищ (DAS)

Пряме підключене сховище (DAS) являє собою традиційну архітектуру сховища, де пристрої зберігання даних безпосередньо підключені до одного комп'ютера або сервера через інтерфейси, такі як SATA, SCSI або SAS. На відміну від мережевих рішень для зберігання даних, DAS фізично підключений до хост-системи, забезпечуючи просте та безпосереднє підключення до сховища.

Основні характеристики:

- Пряме підключення: пристрої зберігання даних фізично підключаються безпосередньо до материнської плати сервера або комп'ютера або до слотів розширення.
- Простота: пропонує підхід «підключи та працюй» з мінімальними вимогами до конфігурації
- Низька затримка: забезпечує швидший доступ до даних завдяки прямому підключенню та зниженим мережевим накладним витратам
- Економічно ефективність: Загалом дешевше порівняно зі складними мережевими рішеннями для зберігання даних.

Переваги:

- Простота налаштування: легко встановити та налаштувати з мінімальними технічними знаннями.
- Нижча початкова вартість: зазвичай дешевше, ніж рішення SAN або NAS
- Висока продуктивність: пряме підключення забезпечує швидшу швидкість читання/запису даних.
- Локальний контроль ресурсів: Повне управління та контроль залишаються за локальною системою.

Недоліки:

- Обмежена масштабованість: складно розширити ємність сховища на кілька систем.
- Проблеми спільного використання ресурсів: сховище не можна легко розподілити між кількома серверами або комп'ютерами.
- Потенційна єдина точка відмови: якщо хост-система виходить з ладу, підключене сховище стає недоступним.
- Обмеження простору та управління: вимагає фізичної близькості та індивідуального управління кожним пристроєм зберігання даних.

Варіанти використання:

- Малий бізнес з обмеженими вимогами до зберігання.
- Індивідуальні робочі станції та персональні обчислювальні середовища.
- Сценарії, що вимагають високошвидкісних, локалізованих рішень для зберігання даних.
- Системи резервного копіювання та архівування з мінімальними потребами в спільному доступі.

Порівняння з мережевим сховищем

Хоча DAS пропонує простоту та безпосередню продуктивність, йому бракує гнучкості та масштабованості мережевих рішень для зберігання даних, таких як SAN та NAS, що робить його більш придатним для конкретних, локалізованих сценаріїв зберігання даних.

Отже, який тип сховища найкраще підходить для моєї мережі?

Тип мережі, який ви оберете, залежатиме, перш за все, від найкращого рішення для зберігання даних для вашого бізнесу. Після того, як ви визначите фактори, які є вирішальними для вашої діяльності, ви зможете вибрати варіант зберігання, який відповідає вашим конкретним потребам.

Хмарне сховище – це хмарний сервіс обчислень, який дозволяє користувачам зберігати дані та файли поза межами свого офісу у стороннього постачальника. Це означає, що ви можете отримати доступ до своїх файлів через Інтернет, що полегшує отримання інформації з будь-якого місця. Ось деякі важливі аспекти хмарного сховища:

Види хмарних сховищ:

- Публічна хмара: такі сервіси, як Google Диск і Dropbox, пропонують сховище, до якого може отримати доступ кожен.
- Приватна хмара: вона призначена для однієї організації, що забезпечує більший контроль та безпеку.
- Гібридна хмара: інтегрує публічні та приватні хмари, забезпечуючи гнучкість в управлінні даними.

Безпека хмарного сховища:

- Шифрування: дані кодуються для захисту від несанкціонованого доступу.
- Контроль доступу: Тільки авторизовані користувачі мають доступ до певних файлів.
- Регулярне резервне копіювання: гарантує, що дані не будуть втрачені у разі збою.

Підсумовуючи, хмарні рішення для зберігання даних пропонують зручний спосіб керування даними без потреби у фізичних пристроях зберігання. Вони надають різні опції

для задоволення різних потреб, гарантуючи, що користувачі можуть безпечно та ефективно отримувати доступ до своїх даних.

Розподілені файлові системи

Розподілені файлові системи (DFS) призначені для керування файлами на кількох серверах, що полегшує користувачам доступ до даних з різних місць. Ці системи є важливими для організацій, яким потрібно ефективно обмінюватися великими обсягами даних.

Як працюють розподілені файлові системи

Розподілені файлові системи працюють, розбиваючи файли на менші частини та зберігаючи їх на різних серверах. Це дозволяє:

- Покращена продуктивність: кілька серверів можуть обробляти запити одночасно.
- Масштабованість: можна додавати більше серверів у міру зростання потреб у даних.
- Відмовостійкість: якщо один сервер вийде з ладу, інші все ще можуть забезпечити доступ до даних.

Популярні розподілені файлові системи

Ось деякі відомі розподілені файлові системи:

- Розподілена файлова система Hadoop (HDFS): використовується для програм, що включають великі дані.
- Файлова система Google (GFS): створена для ефективної обробки великих обсягів даних.
- Ceph: Рішення для зберігання даних з відкритим кодом, яке надає можливості для зберігання об'єктів, блоків та файлів.

Проблеми розподілених файлових систем

Хоча розподілені файлові системи пропонують багато переваг, вони також мають свої труднощі:

- Складність: Керування кількома серверами може бути складним.
 - Узгодженість даних: Забезпечити, щоб усі користувачі бачили однакові дані, може бути складно.
 - Залежність від мережі: проблеми з мережею можуть впливати на продуктивність.
- Підсумовуючи, розподілені файлові системи відіграють вирішальну роль у сучасному управлінні даними, дозволяючи організаціям ефективно обробляти великі обсяги даних. Розуміння їхньої роботи та проблем є життєво важливим для ефективного впровадження.

Порівняння зберігання об'єктів з традиційним зберіганням

Об'єктне сховище – це сучасний спосіб зберігання даних, призначений для обробки великих обсягів неструктурованих даних. На відміну від традиційних систем зберігання, воно може керувати всім: від відео до електронних листів та медичних записів. Це робить його чудовим вибором для компаній, яким потрібно зберігати багато різних типів інформації.

Переваги зберігання об'єктів:

- Масштабованість: сховище об'єктів може легко масштабуватися для задоволення зростаючих потреб у даних.
 - Економічна ефективність: Зберігання великих обсягів даних часто коштує менше порівняно з традиційними методами.
 - Доступність: До даних у сховищі об'єктів можна отримати доступ з будь-якого місця, що робить його ідеальним для віддаленої роботи.
- Застосування використання зберігання об'єктів:
- Медіа та розваги: Зберігання великих відеофайлів та зображень.
 - Охорона здоров'я: керування записами пацієнтів та даними візуалізації.
 - Резервне копіювання та архівування: безпечне зберігання копій важливих даних.

Підсумовуючи, хоча традиційні методи зберігання даних, такі як NAS та SAN, мають своє місце, об'єктне сховище пропонує унікальні переваги, що роблять його придатним для сучасних потреб у даних. Оскільки бізнес продовжує генерувати більше неструктурованих даних, роль об'єктного сховища, ймовірно, зростатиме ще більшою.

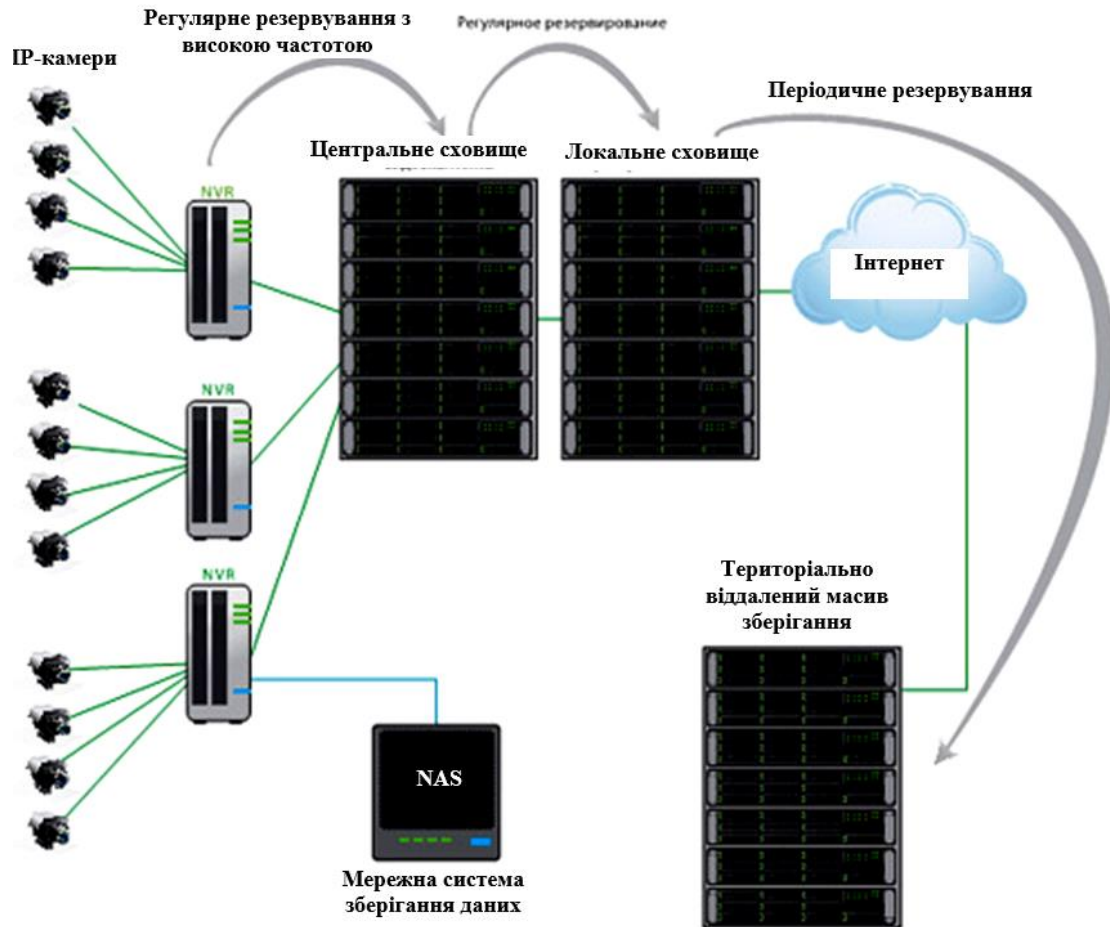


Рисунок 1 – Структурна схема системи

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів інтелектуальної оптимізації продуктивності та надійності хмарних мережесих систем зберігання даних. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем інтелектуальної оптимізації продуктивності та надійності хмарних мережесих систем зберігання даних.
- Досліджена система інтелектуальної оптимізації продуктивності та надійності хмарних мережесих систем зберігання даних.
- На основі отриманих результатів досліджень створена програмна реалізація системи інтелектуальної оптимізації продуктивності та надійності хмарних мережесих систем зберігання даних.

Розроблені алгоритми дозволяють успішно вирішувати завдання інтелектуальної оптимізації продуктивності та надійності хмарних мережесих систем зберігання 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., 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.
 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». Центральнотуристський 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

О.Кривда, магістр гр. КІ-24М,

Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ДЕДУПЛІКАЦІЇ В ІНФРАСТРУКТУРІ РЕЗЕРВНОГО КОПІЮВАННЯ

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

дедуплікація, інфраструктура, резервне копіювання

Постановка проблеми. Дедуплікація знайшла широке застосування як спосіб упоратися з ростом витрат на інфраструктуру резервного копіювання при збільшенні обсягів даних.

Доступність і схоронність даних – застава безперервності бізнес-процесів і ефективності роботи. Сьогодні дані – один із самих коштовних активів, тому їхнє резервне копіювання й архівне зберігання – найбільш типові завдання, а система резервного копіювання – важлива частина будь-якої корпоративної інформаційної системи. При правильній організації вона здатна надійно захистити критичні дані.

Впровадження систем резервного копіювання дає можливість оперативно відновлювати інформацію в самих різних ситуаціях, однак і вони не позбавлені недоліків. Традиційні проблеми – неефективне використання ємності зберігання (обсяг резервних копій за тиждень може вдвічі перевищити обсяг вихідних даних), низька швидкість копіювання, непередбачений час відновлення (як правило, набагато більше планованого), не дуже висока надійність (по даним Gartner, ризик неможливості відновлення перевищує 10%).

Рішення для резервного копіювання й відновлення повинні ефективно функціонувати в умовах експонентного росту даних, жорсткості вимог регуляторів і скорочення вікон резервного копіювання. Україй бажано також забезпечити зниження витрат, пов'язаних із захистом даних. Перебороти перераховані проблеми покликана дедуплікація даних. У том або іншому виді її пропонують у своїх продуктах всі провідні вендори систем резервного копіювання корпоративного класу.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи дедуплікації в інфраструктурі резервного копіювання.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи дедуплікації в інфраструктурі резервного копіювання.

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

- Огляд існуючих систем дедуплікації в інфраструктурі резервного копіювання.
- Дослідження системи дедуплікації в інфраструктурі резервного копіювання.

– Програмна реалізація системи дедуплікації в інфраструктурі резервного копіювання.

Об'єктом дослідження є процес дедуплікації в інфраструктурі резервного копіювання.

Предметом дослідження є методи дедуплікації в інфраструктурі резервного копіювання.

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

Виклад основного матеріалу. Дедуплікація буває різна – на рівні файлів, блоків даних і навіть на бітовому рівні. Використовується блокова дедуплікація. Файли розбиваються на невеликі блоки різного розміру (32-128 КБ), визначаються дублюючі блоки й зберігається одна копія кожного блоку. Надлишкові копії блоку замінюються посиланнями на цю єдину копію. Блоки організуються у файли-контейнери, які можуть стискуватися для подальшої оптимізації використання простору, і містяться в сховище блоків.

Для приклада припустимо, у нас є два файли – File1 і File2. У вихідному стані вони містять метадані (ім'я файлу, атрибути й т.п.) і самі дані.

Після дедуплікації дані з File1 і File2 видаляються й замінюються заглушками, що вказують на відповідні блоки даних, що зберігаються в загальному сховищі блоків. Тому що блоки А, В і С однакові для обох файлів, вони зберігаються в єдиній копії, що знижує обсяг дискового простору, необхідний для зберігання обох файлів.

Під час доступу до одного з файлів відповідні блоки збираються разом. При цьому користувач або додаток працюють із файлом як і раніше, не підозрюючи про те, що файл був підданий перетворенням. Це дозволяє застосовувати дедуплікацію, не турбуючись про її вплив на поведінку застосунків або доступ користувачів до файлу.

Таким чином, після включення дедуплікації тому й оптимізації даних том містить:

– Оптимізовані файли (файли точок повторного аналізу) які містять покажчики на відповідні блоки даних у сховище блоків, необхідні для побудови вихідного файлу.

– Сховище блоків (дані оптимізованих файлів).

– Неоптимізовані файли (тобто пропущені файли, наприклад файли стану системи, зашифровані файли, файли з додатковими атрибутами або файли розміром менш 32 КБ).

Планування

Дедуплікація може значно знизити споживаний дисковий простір (на 50-90% і більше), але тільки при правильному плануванні. Тому при виборі об'єкта для дедуплікації варто враховувати деякі моменти.

Тип даних

Ефективність дедуплікації дуже сильно залежить від типу даних. Так мультимедійні файли (фотографії, музика, відео) практично не містять повторюваних даних, тому їх дедуплікація не дасть великої економії. У той же час файли віртуальних машин (VHD) чудово дедуплікуються й на них економія може становити до 95 %. Із цієї причини перед включенням дедуплікації рекомендується виконати попередню оцінку даних на предмет дедуплікуємості.

Частота зміни файлів

Файли, які часто змінюються й до яких часто звертаються користувачі або додатки, не дуже підходять для дедуплікації. Постійний доступ до даних і їхній зміна швидше за все зведуть нанівець всі результати дедуплікації й можуть просто не дати дедуплікації можливості обробити файли. Простіше говорячи, для дедуплікації добре підійдуть дані, які часто читають, але рідко змінюють.

Завантаженість сервера

Під час дедуплікації виконується читання, обробка й запис великого обсягу даних. Цей процес споживає ресурси сервера, що необхідно враховувати при плануванні розгортання. Як правило, сервера мають періоди високої й низької активності. Більшу

частину дедуплікації можливо виконати, коли ресурси доступні. Постійно високонагруженні сервера не рекомендується використовувати для дедуплікації.

Не рекомендується виконувати дедуплікацію файлів, які відкриті, постійно змінюються протягом тривалого періоду часу або мають високі вимоги вводу/виводу, наприклад файли працюючих віртуальних машин, динамічних баз даних SQL або активних сеансів VDI. Справа в тому, що при дедуплікації не виконується обробка файлів, відкритих постійно в монопольному режимі для запису. Це значить, що дедуплікація не буде проведена доти, поки файл не буде закритий. Тільки тоді завдання оптимізації виконає спробу обробити файл, що відповідає обраним параметрам політики дедуплікації.

У принципі дедуплікацію можливо налаштувати на обробку постійно, що змінюються файлів. Але в цьому випадку можлива ситуація, коли процес оптимізації не зможе одержати доступ до цих файлів і пропустить їхню обробку. Не варто витрачати ресурси сервера на дедуплікацію файлів, у які постійно записуються нові дані.

Приведу рекомендації Microsoft. Для дедуплікації:

Не рекомендується

- Сервера Hyper-V.
- VHD-Файли запущених віртуальних машин.
- Служби WSUS.
- Сервера SQL і Exchange.
- Будь-які файли, розмір яких дорівнює або більше 1 Тб.

Рекомендується:

- Файлові ресурси загального доступу (загальні папки, профілі й домашні папки користувачів, інші файлопомойки).
- Розгортання програмних продуктів (бінарники, образи дисків і відновлення ПЗ).
- Бібліотеки віртуалізації (VHD-диски).
- Томи архівів SQL і Exchange.

Треба сказати, що рекомендації Microsoft часто суперечать один одному, тому не треба їх беззастережно приймати на віру. У кожному разі перед включенням дедуплікації необхідний ретельний аналіз.

Для визначення очікуваної економії в результаті включення дедуплікації можливо використовувати засіб оцінки дедуплікації Ddpeval.exe. Після установки компонента дедуплікації утиліта Ddpeval.exe автоматично встановлюється в папку \Windows\System32\.. До речі, її можливо просто скопіювати з будь-якої установки Windows Server 2025 і запустити в системах Windows 10/11.

Синтаксис у програми простіше нікуди, пишемо Ddpeval.exe і вказуємо шлях. Як шлях можливо вказати локальний диск, папку або мережну кулі:

Ddpeval.exe E:

Ddpeval E:\Test\

Ddpeval.exe \\Server\Share

Програма видасть очікуваний розмір економії дискового простору, після чого вже можливо приймати рішення – включати дедуплікацію чи ні.

Системні вимоги

Дедуплікація пред'являє до системи деякі вимоги.

Тому

- Тома, призначені для дедуплікації не повинні бути системними або завантажувальними. Дедуплікація не підтримується для томів операційної системи.
- Тома можуть бути розбиті під MBR або GPT і відформатовані в NTFS. Нова відказостійка файлова система ReFS не підтримується.
- Тома можуть перебувати на локальних дисках або в загальнодоступному сховищі (SAS, iSCSI або Fibre Channel).

– Windows повинна бачити томи як незнімні диски. Мережні диски й знімні носії не підтримуються.

– Не можливо включати дедуплікацію для загальних томів кластера (Cluster Shared Volume, CSV). Якщо дедуплікований том перетворити в CSV, то доступ до даних залишиться, але завдання дедуплікації не зможуть відробити.

Апаратні ресурси

– Устаткування серверів повинне відповідати мінімальним вимогам Windows Server 2025. Функція дедуплікації розроблена для підтримки мінімальних конфігурацій, таких як система з одним процесором, 4 ГБ ОЗУ й одним жорстким диском SATA.

– Сервер повинен мати одне процесорне ядро й 350 МБ вільної пам'яті для виконання завдання дедуплікації на одному томі, при цьому буде оброблятися близько 1,5 ТБ даних у день. Якщо планується підтримувати дедуплікацію в декількох томах на одному сервері, необхідно відповідним чином збільшити продуктивність системи, щоб гарантувати, що вона зможе обробляти дані.

– Функція дедуплікації підтримує одночасну обробку до 90 томів, однак при дедуплікації одночасно може оброблятися один том на фізичне процесорне ядро плюс один. Застосування технології Hyper-Threading не впливає на цей процес, оскільки для обробки тому можливо використовувати тільки фізичні ядра. Наприклад сервер з 16 процесорними ядрами й 90 томами буде обробляти по 17 томів одночасно, поки не обробить всі 90 томів.

– До віртуальних серверів застосовуються ті ж правила, що й до фізичного встаткування відносно ресурсів сервера.

Загальні вимоги

– Наявність вільного місця на диску. При відсутності дискового простору на дедуплікованому томі деякі додатки не зможуть одержати доступ до даних і будуть завершені з помилкою. Необхідно зберігати, принаймні, один гігабайт вільного місця на дедуплікованому томі.

– Тверді квоти. При використанні FSRM (File System Resource Manager) не підтримується установка твердих квот на обсяг тому. Коли для тому встановлені тверді квоти, фактичний обсяг вільного місця на томі й обмежене квотами простір відрізняється, що може привести до невдачі процесу дедуплікації. Всі інші FSRM-Квоти, у тому числі м'які квоти на обсяг тому й квоти на підпапки, будуть нормально працювати при дедуплікації.

– Файли з додатковими атрибутами, зашифровані файли, файли розміром менше 32 КБ і файли точок повторного аналізу при дедуплікації не обробляються.

Дедуплікація, по визначенню IDC, – це технологія створення з дублікатів єдиної копії даних з можливістю спільного доступу, що підвищує ефективність використання ємності систем зберігання. Згідно Microsoft, це процедура пошуку й видалення даних, що дублюються, без шкоди для їхньої якості й цілісності з метою зменшення обсягу простору, займаного даними.

Блоки, загальні для декількох файлів, зберігаються у вигляді однієї копії, тому вимоги до ємності зберігання всіх файлів знижуються. Видаляючи повторювані послідовності даних, дедуплікація дозволяє значно скоротити обсяг переданих і/або збережених даних. Щоб ще сильніше його зменшити, дедуплікацію нерідко сполучать із компресією (стиском), називаючи все це ущільненням даних.

При запиті файл збирається з відповідних блоків (для користувача або застосунку цей процес прозорий), тому, застосовуючи дедуплікацію до файлів, можливо не турбуватися про те, що робота застосунків ускладниться або доступ користувачів до файлів виявиться неможливий. Дедуплікація знижує витрати, зводячи до мінімуму накладні витрати на зберігання й передачу даних.

При використанні в системах резервного копіювання дедуплікація допомагає вирішити цілий ряд проблем і дає вагомні переваги.

Основні причини використання дедуплікації даних у системі резервного копіювання – невеликий розмір резервних копій, зниження потреби в ємності зберігання, скорочення

мережного трафіку, зменшення вікна резервного копіювання. Щодня виконуване повне резервне копіювання дозволяє гарантувати швидке відновлення за один крок.

У системах резервного копіювання з функцією дедуплікації можливі різні варіанти зберігання резервних копій: стрічкові накопичувачі й бібліотеки, віртуальні стрічкові бібліотеки, дискові масиви й системи зберігання даних, у тому числі з убудованою дедуплікацією. Дедуплікація виконується «на лету» (у процесі резервного копіювання або архівування), тому на диску, а також у хмарних сховищах (cloud backup) зберігаються вже дедупліковані дані.

Вимоги до ємності скорочуються в середньому 10-30 разів, значно підвищуються швидкість і надійність відновлення й добування даних. Але ніщо не дається даром: дедуплікація вимагає витрат. Потрібні обчислювальні ресурси, до того ж відбувається зниження продуктивності систем або збільшується їхня вартість. Тому потрібно з'ясовувати, які витрати неминучі при використанні кожного методу.

Існують різні види, або методи, дедуплікації, у кожного свої переваги й недоліки.

Дедуплікація може виконуватися на джерелі даних або безпосередньо в сховище. Залежно від цього розподіляється обчислювальне навантаження. При першому методі дані обробляються на стороні клієнта й по закінченні дедуплікації пересилаються на пристрої зберігання. У результаті навантаження на мережу знижується, але на клієнтах доводиться встановлювати спеціалізоване ПЗ й оснащувати їх значними обчислювальними ресурсами.

Другий метод передбачає застосування могутнішої й дорогих СЗД, але витрати на первісну передачу даних фактично не знижуються. У кожному разі потрібно враховувати, що вимоги дедуплікації до ресурсів системи досить високі.

По даним Dell EMC, дедуплікація на джерелі дозволяє скоротити ємність зберігання до 50 разів, трафік – до 500 разів, час резервного копіювання – до 10 разів. Однак її ефективність дуже сильно залежить від типу даних. Очевидно, що найбільший ефект досягається, коли дані мають велику надмірність, а також коли копіюються й/або зберігаються після внесення незначних змін.

У загальному випадку для неструктурованих даних (файли документів, журналів, образів і віртуальних машин, електронної пошти й архівів) характерний високий коефіцієнт дедуплікації – їхній обсяг нерідко зменшується в 20–30 разів. Наприклад, добре дедуплікуються файли віртуальних машин (VHD): економія може становити до 90%. Дедуплікація структурованої інформації, наприклад баз даних, не настільки ефективна (звичайно до 5-8 разів).

Дедуплікація мультимедійних файлів теж не забезпечує великої економії. Зображення, відео (JPEG, GIF, TIF, MPEG, і ін.), результати стиску й шифрування, картографічні й сейсмічні дані, файли САПР – всі ці формати проблемні для дедуплікації.

Добре дедуплікуються рідко змінювані дані, оскільки постійний доступ до даних і їхній зміну можуть звести до мінімуму ефект дедуплікації. Microsoft не рекомендує застосовувати дедуплікацію до серверів Hyper-V, SQL і Exchange, файлам запущених віртуальних машин, більшим файлам (більше терабайта). Вона може функціонувати на файловому, блоковому або бітовому рівні.

У деяких схемах, заснованих на гешуванні, для підвищення коефіцієнта дедуплікації застосовується попередня обробка даних. Якщо дані обробляються на стороні клієнта, дедуплікація блоків змінної довжини дозволяє значно зменшити час резервного копіювання, тому що зберігаються тільки унікальні сегменти. Цей метод більше ефективний, чим традиційна дедуплікація сегментів фіксованої довжини, коли навіть невеликі зміни в наборі даних приводять до резервного копіювання всього файлу.

У системах резервного копіювання можуть використовуватися й інші методи дедуплікації. До того ж розроблювачі систем зберігання застосовують різні алгоритми дедуплікації, у тому числі досить складні, для яких потрібно більше процесорних ресурсів. Тому величина коефіцієнта дедуплікації залежить від реалізації цієї технології.

Сучасні рішення дають можливість створювати резервні копії даних у хмарі, що дозволяє надійно зберегти й відновити їх, визволивши час і ресурси.

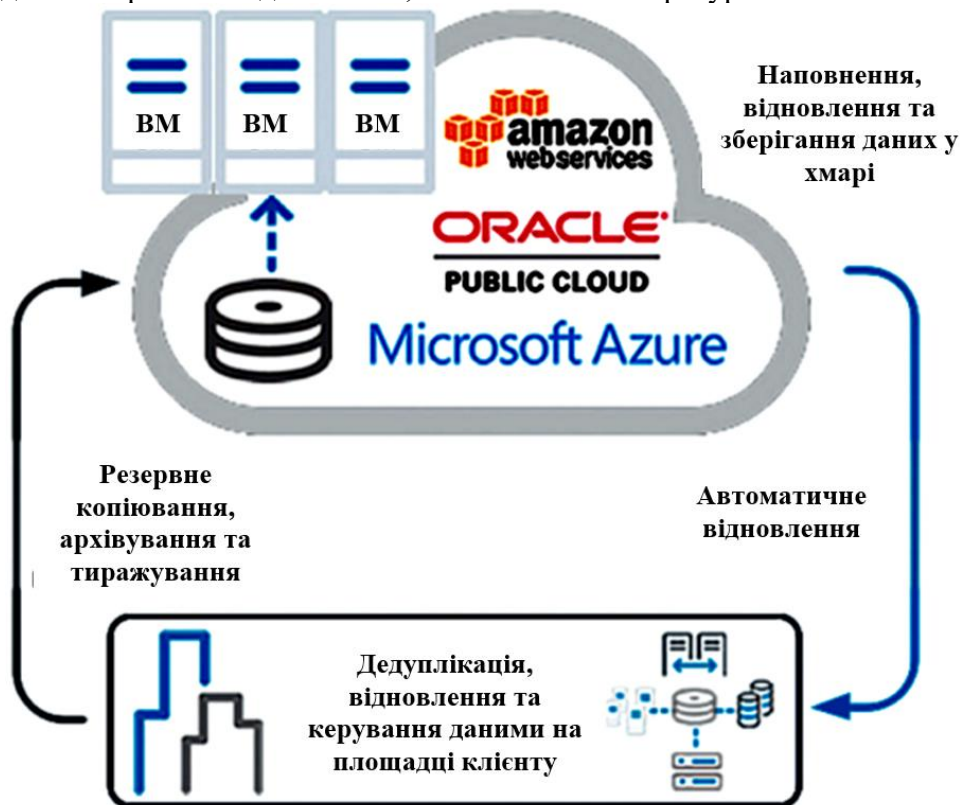


Рисунок 1 – Структурна схема системи

Вихідні дані можуть перебувати на будь-якій площадці: на стороні клієнта, в іншому комерційному ЦОДі або в хмарі. Таким чином, можливо швидко реалізувати переваги резервного копіювання даних у хмару, використовуючи його як розширення корпоративної ІТ-інфраструктури. У числі переваг такого рішення:

- швидке й надійне резервне копіювання, оперативне відновлення даних;
- відсутність необхідності в дорогих шлюзах і складних проміжних рішеннях;
- можливість замінити стрічкове сховище хмарним;
- використання хмари для аварійного відновлення.

Компанії все частіше застосовують комбінований підхід: дискові масиви в сполученні з копіюванням у хмару. Така стратегія зберігання резервних копій дозволяє прискорити резервне копіювання найбільш актуальних даних і знизити вартість володіння відповідною інфраструктурою резервного копіювання. Використання дедуплікації дає можливість не тільки оптимізувати займану резервними копіями ємність сховищ, але й зменшити мережний трафік при резервуванні в хмару, що робить цю технологію ще більш актуальною.

Постійний розвиток і інтеграція рішень дедуплікації даних розроблювачами систем резервного копіювання й виробниками систем зберігання буде сприяти більшій економічності пропонуваного рішення, зниженню вартості впровадження, більше швидкому переміщенню резервних копій між територіально віддаленими площадками.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів дедуплікації в інфраструктурі резервного копіювання. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем дедуплікації в інфраструктурі резервного копіювання.
- Досліджена система дедуплікації в інфраструктурі резервного копіювання.

– На основі отриманих результатів досліджень створена програмна реалізація системи дедуплікації в інфраструктурі резервного копіювання. Розроблені алгоритми дозволяють успішно вирішувати завдання дедуплікації в інфраструктурі резервного копіювання. 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., 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. 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.
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 гешування 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 гешування 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., 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.
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., 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.
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

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

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ SDN НА ОСНОВІ HUAWEI CLOUD FABRIC

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

SDN, Huawei Cloud Fabric

Постановка проблеми. Бізнес усе активніше використовує віртуалізацію й хмарні технології для підвищення ефективності, удосконалювання процесів і одержання конкурентних переваг. Корпоративні центри обробки даних еволюціонують у напрямку хмарних середовищ на основі віртуалізації, що стала для бізнесу банальною необхідністю, а не якимось «ноу-хау». Логічний ланцюжок досить простий:

1. Віртуалізація обчислювальних ресурсів і ресурсів зберігання в сполученні з автоматизацією керування й оркестрації уможливили віртуалізацію робочого навантаження;
2. У свою чергу, віртуалізація робочого навантаження дозволяє менеджерам ІТ-систем і розроблювачам додатків швидко створювати нові екземпляри сервісів і додатків у центрі обробки даних.

Підвищення пропускної здатності при з'єднанні незалежних робочих навантажень і будь-яких зв'язаних сервісів через мережу до останнього часу було однієї з основних «точок росту», однак зрості темпи розвитку віртуалізованих ресурсів для обчислень і зберігання даних диктують нові правила гри.

Прихід програмно-визначаємих мереж (SDN) ініціював появу більш гнучких систем визначення й конфігурації мережевих шляхів і екстерналізації площини мережевого контролю від індивідуальних пристроїв. Дана «що виноситься в поза» площина керування, що визначає логічну топологію мережі, тепер представляє вид мережі «великим планом» і забезпечує гнучку оптимізацію мережі на основі критеріїв, адаптованих до операційних аспектів середовища.

З погляду зовнішньої інтеграції цей SDN-контролер більш кращий завдячуючи програмним інтерфейсам, які дозволяють системам працювати спільно й узгоджено з іншими компонентами центра обробки даних.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи sdn на основі Huawei Cloud Fabric.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи SDN на основі Huawei Cloud Fabric.

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

- Огляд існуючих систем SDN на основі Huawei Cloud Fabric.
- Дослідження системи SDN на основі Huawei Cloud Fabric.
- Програмна реалізація системи SDN на основі Huawei Cloud Fabric.

Об'єктом дослідження є процес SDN на основі Huawei Cloud Fabric.

Предметом дослідження є методи SDN на основі Huawei Cloud Fabric.

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

Виклад основного матеріалу. Хмарне сервісне рішення Cloud Fabric для ЦОД

Інноваційне рішення Huawei для мереж програмно-визначаємих ЦОД забезпечує користувачам гнучкість адаптації до постійних змін у роботі хмарних сервісів. Рішення дозволяє прискорити цифрову трансформацію завдяки простоті, прозорості й гнучкості мереж хмарних ЦОД. Рішення Huawei CloudFabric Data Center Network Solution засноване на технології програмно-визначаємих мереж, що дозволяє розгортати мережі хмарних ЦОД наступного покоління із сервіс-орієнтованою, відкритою архітектурою.

Мережа хмарних центрів обробки даних Huawei CloudFabric включає високопродуктивні базові комутатори CloudEngine 12800, стійкові комутатори верхнього рівня CloudEngine 8800/7800/6800/5800 і віртуальний комутатор CloudEngine 1800V. Застосування гнучкого контролера й технології SDN дозволяє розгортати мережі ЦОД наступного покоління в автоматичному режимі, оперативно й гнучко застосовувати конструктивні рішення й використовувати переваги інтелектуальної системи експлуатації й обслуговування мережі.

Рішення автоматизованого розгортання мережі на базі технології CloudFabric SDN

Щоб поспівати за змінами попиту на ринку в епоху цифрових технологій необхідні засоби, які дозволять організаціям оперативно впроваджувати сучасні персоналізовані додатки. У звичайних центрах обробки даних, де мережа й послуги розділені, цей процес іде повільно. Якщо необхідно запустити нові види послуг, розгортання мережі може зайняти від декількох тижнів до декількох місяців. Такі зміни вимагає перегляду безлічі політик, адаптація яких без засобів автоматизації відбувається неефективно. Мережа передачі даних може поєднувати фізичні пристрої, віртуальні машини й контейнери. Управляти настільки різноманітними ресурсами – завдання не із простих.

Щоб залишатися конкурентоспроможними, підприємства повинні швидко реагувати на зміни ринкового попиту. Для цього завдання компанія Huawei пропонує своє рішення на базі технології CloudFabric SDN, що автоматизує процеси конфігурування мережі, впровадження додаткових послуг, а також оптимізує доступ до фізичних пристроїв, віртуальним машинам і контейнерам, а також до хмарних систем. Автоматизація даних процесів дозволить скоротити строки запуску послуг з декількох тижнів до декількох хвилин, підвищити гнучкість обслуговування й домогтися успіху в бізнесі.

Інтелектуальна система експлуатації й техобслуговування Fabric Insight

За рахунок стрімкого розвитку хмарних обчислень традиційні мережі центрів обробки даних перестали задовольняти потреби в ІТ-сервісах. Підвищення ефективності керування мережею, її експлуатації й техобслуговування стає основним завданням модернізації архітектури мережі і її технологій. Технологічна інновація, програмно-визначаєма мережа SDN, забезпечує віртуалізацію й гнучке планування мережевих ресурсів шляхом централізованого призначення політик і контролю їхнього виконання. Але дана технологія сполучена з більшими проблемами, пов'язаними з експлуатацією й обслуговуванням мереж.

У порівнянні із традиційними мережами, SDN відрізняються наступними особливостями:

- Збільшення масштабу центра обробки даних. Візуалізація приводить до лінійного збільшення числа керованих вузлів ЦОДа. Для більше ефективного керування мережа SDN повинна одержувати інформацію про міграцію віртуальних машин.

– Динамічний статус мережі. Об'єкти керування в SDN змінилися – замість мережевих елементів використовуються логічні й фізичні мережі. При цьому стан мережі постійно змінюється у зв'язку з появою або зміною великої кількості послуг орендарів. Це робить тяжковимірюваною якість і доступність мережі.

– Відгук у реальному часі. У зв'язку з об'єднанням ресурсів центра обробки даних і ущільненням сервісів користувачам потрібно більш швидкий відгук мережі й оперативні методи відновлення після збоїв.

Рішення Fabric Insight Huawei з архітектурою платформи експлуатації й обслуговування наступного покоління забезпечує відгук у режимі реального часу у великих динамічних мережах, що допомагає вирішувати пов'язані з експлуатацією й техобслуговуванням проблеми в мережах SDN.

Рішення Fabric Insight забезпечує візуалізацію на фізичному, логічному й прикладному рівнях, інтелектуальні механізми локалізації несправностей і проактивну оптимізацію шляхом збору й аналізу Великих даних і використання додатків системи експлуатації й обслуговування. Це значно підвищує ефективність експлуатації й техобслуговування в мережах SDN.

Трирівнева візуалізація мережі, чітке відображення параметрів якості мережі

Рішення Fabric Insight підтримує відображення мережі на трьох рівнях – фізичн, логічному й прикладному, а також показує всі маршрути мережі. Крім того, дане рішення підтримує виявлення подій, що тривають усього декілька мілісекунд (наприклад, мікроперегони трафіку) і малі втрати пакетів (менш 10^{-4}), а також надмірно більші або надмірно маленькі потоки. Повна візуалізація стану мережі і її якостей дозволяє мережевим адміністраторам і користувачам підвищувати ефективність керування мережею.

Аналітика Великих даних, виявлення несправностей за кілька хвилин

Рішення Fabric Insight сканує всі маршрути. Періодично проводиться повне сканування маршрутів всієї мережі для своєчасного виявлення проблем, що викликають зниження якості. Результати перевірки допомагають мережевим адміністраторам визначати стан мережі й розпізнавати точки відмови.

Рішення Fabric Insight забезпечує моніторинг додатків для контролю всіх сервісних потоків мережі. При зниженні якості потоку послуг Fabric Insight швидко знаходить новий маршрут, на який переадресується потік, і, відслідковуючи зв'язку між сервісом і мережею, визначає причину зниження якості. Це скорочує час розпізнавання несправності до декількох хвилин.

Проактивна оптимізація, забезпечення високої якості послуг

Архітектура Fabric Insight надає можливості прогнозування несправностей, автоматичного аналізу й проактивної оптимізації. Платформа Великих даних використовується для розпізнавання можливих ризиків, таких як незбалансований розподіл трафіку й перевантаження по трафіку, не допускаючи впливу на послуги. На базі аналізу Великих даних рішення Fabric Insight визначає головну причину потенційних ризиків і генерує пропозиції по їхньому усуненню. Більші дані також допомагають прогнозувати трафік послуг мережі для реалізації політик динамічного розподілу навантаження (Dynamic Load Balancing; DLB) з метою забезпечення балансу трафіку.

Архітектура наступного покоління Fabric Insight Huawei використовується разом із платформами Великих даних для підвищення ефективності процесів експлуатації й обслуговування, а також скорочення витрат на реалізацію.

Agile Controller для мереж ЦОД

Рішення CloudFabric від Huawei з інтелектуальними функціями експлуатації й обслуговування спрощує розгортання мережі, надає можливість організації зверхширокополосних з'єднань і створення відкритої екосистеми для мереж центрів обробки даних нового покоління, що підтримують моментальний запуск корпоративних хмарних сервісів.

Автоматизація процесів

Agile Controller для мереж ЦОД дозволяє створювати логічні мережеві моделі й мережеві конфігурації на базі вимог до сервісів з наступною їхньою передачею на пристрої в пакетному режимі, завдяки чому період розгортання послуг скорочується з декількох тижнів до декількох хвилин.

Надійність

На базі Agile Controller для мереж ЦОД можливе створення високонадійного кластера. Agile Controller здатний обробляти послуги північного й південного інтерфейсів у режимі балансування навантаження, а робота в режимі активний/резервний забезпечує вилучене аварійне відновлення, що відповідає вимогам до надійності послуг центра обробки даних.

Безпека

Безпека з мінімальним рівнем гранулярності для мереж центрів обробки даних. Мікросегментація IP-адрес, імен хостів і імен віртуальних машин і деталізована ізоляція доменів для запобігання погроз і забезпечення безпеки.

Cloud Fabric – сервісне рішення для ЦОД

Huawei Cloud Fabric має властивості:

- Гнучкість: висока масштабованість хмарних сервісів і канали для передачі Великих даних (Big Data).
- Спрощення процесів: хмарне рішення для мережі Huawei в 10 разів прискорює активацію хмарних сервісів.
- Відкритість: спрощення хмарних обчислень за рахунок безшовного підключення до основних хмарних платформ.

Рішення Huawei Cloud Fabric покоління допомагає створити гнучку, зручну в керуванні, відкриту мережу для стабільного розвитку хмарних сервісів.

Структурна схема рішення Huawei Cloud Fabric наведена на рисунку 1.

У міру росту популярності хмарних сервісів і додатків SDN центри даних еволюціонують у бік Великих даних, послуг і розмаїтості систем.

Але є кілька проблем:

- застосування Великих даних пов'язане з інтенсивним збільшенням мережевого трафіку;
- ІТ-системи повинні швидко реагувати на більше швидкі й часті відновлення послуг;
- для хмарних екосистем потрібні більше відкриті мережі;

Хмарне рішення допомагає створювати гнучкі, прості, відкриті мережі центрів даних з підтримкою стабільного розвитку хмарних послуг.

Система передачі, маршрутизації, безпеки й мережевого керування – комплексне рішення мережі центра даних. Воно складається з декількох допоміжних рішень:

- З'єднання усередині центра даних (рішення хмарного зв'язку).
- З'єднання між центрами даних з відновленням після збоїв.
- Оптимізація захисту центра даних і його додатків.
- Керування мережею центра даних.

Компанія Huawei 18 червня 2018 року оголосила про комплексне відновлення рішення CloudFabric, що покликано спростити процес впровадження IDN-Технологій (Intent-Driven Network) у центрах обробки даних. Крім того, компанія представила 400-гігабітну платформу для ядра комутації із кращими експлуатаційними характеристиками в галузі.

Рішення Huawei Intent-Driven Networking для CloudFabric дозволяє підприємствам ідентифікувати необхідність застосування автоматичних мережевих конфігурацій, предиктивного аналізу й інтелектуальної експлуатації. Крім того, рішення забезпечує фізичну можливість ультраширокополосної мережевої взаємодії з низькою затримкою й нульовою втратою пакетів інформації. Intent-Driven Networking для CloudFabric, засноване на принципах інтелектуальності, простоти, ультраширокополосності, відкритості й безпеці,

оптимізується завдяки контролеру Agile Controller. Це рішення також використовує мережевий аналізатор ЦОД FabricInsight для впровадження предиктивного аналізу й автоматичного виявлення відхилень. Згодом це стане основою для створення автоматичної, саморегулюючої системи замкнутого циклу, що для користувача стане ще більш зручною.



Рисунок 1 – Структурна схема системи

Список функцій і ключових компонентів Intent-Driven Networking:

- IDN-автоматизація.
- Agile Controller дозволяє автоматично завершувати планування мережі з урахуванням сервісних мет і намірів користувача, що підвищує якість обслуговування. Один кластер може управляти 3 тис. вузлів на рівні доступу й може бути масштабований до 100 тис.серверів. Крім того, кластер контролера, що працює в активному й резервному режимі в співвідношенні 1:1, підвищує доступність системи й гарантує відсутність перебоїв в обслуговуванні при автоматичному перемиканні між активними й резервними вузлами. Agile Controller може взаємодіяти із численними хмарними платформами для гнучкого планування й розподілу ресурсів.
- Предиктивний аналіз і виявлення відхилень.
- Аналізатор FabricInsight устанавлює модель мережевого поведіння на підставі аналізу Великих даних і технології машинного навчання, безупинно контролює статус мережі для підтримки діагностичного технічного обслуговування й виявлення мережевих відхилень у лічені секунди, а також автоматично зв'язує мережеві відхилення (напр. перевантаження) з ураженими сервісами, що допомагає клієнтам оперативно виявляти й виправляти помилки.
- 400-гігабітна платформа для ядра комутації із кращими експлуатаційними характеристиками в галузі.
- Комутатор CE12800 підтримує 36 400-гігабітних мережевих карт і 400-гігабітне наскрізна взаємодія. Це дозволяє уникати недоскоп пропускної здатності, знижує вартість трафіку на 20% і забезпечує можливість подальшого розвитку на найближчі 10 років, затверджують в Huawei.

Рішення Huawei Intent-Driven Networking для CloudFabric, в основі якого лежить концепція IDN, відкриває доступ до передових рішень і продуктів для сервісів-провайдерів, великих корпорацій і середнього бізнесу, дозволяючи виявляти бізнес-наміру й мети клієнтів і домогтися автоматичного й інтелектуального розгортання й роботи мережі. На думку Huawei, завдяки цьому центри обробки даних стануть центрами комерційного потенціалу.

20 вересня 2017 року компанія Huawei представила рішення CloudFabric, створене на основі концепції модульних мереж, оптимізоване для конкретних сценаріїв. CloudFabric допомагає створювати центри обробки даних зі зверхспрощеними дизайном, розгортанням, технічним обслуговуванням і експлуатацією.

Як пояснили в компанії, хмарні обчислення стали ключовим двигуном цифрової трансформації, у результаті від дата-центрів потрібно, щоб вони були орієнтовані на конкретні сценарії. Однак цьому перешкоджає низька операційна ефективність традиційних універсальних рішень. Huawei CloudFabric покликаний допомогти підприємствам швидко створити зверхспрощені хмарні мережі ЦОД.

Моделі фабрик

Huawei CloudFabric надає три сценарії-орієнтовані моделі фабрик:

- Модель «Фабрика високої доступності/відказостійкості» (High Availability Fabric) орієнтована на мережі ЦОД з підвищеними вимогами по надійності й безпеці, а також інтелектуальною системою технічного обслуговування й експлуатації, що забезпечує цілодобову роботу критичних важливих сервісів у фінансовому секторі та ін.

- Модель «Фабрика гіпермасштабованості» (Hyperscale Fabric) орієнтована на гіпермасштабовані й мережі, що не блокують, ЦОД з безліччю хмар автоматизованого керування.

- Модель «Фабрика високопродуктивних обчислень» (HPC Fabric) орієнтована на ЦОД, де необхідні високопродуктивні обчислення, і може бути використана в таких секторах, як супутникове картографування, визначення енергії (energy detection) і медико-біологічні науки, оскільки відповідає вимогам нульової втрати пакетів інформації й низького значення затримки в Ethernet-фабриках.

У той час, як цифрова трансформація підприємств прискорюється, переклад сервісів у хмару не обмежується інтернет-галуззю – він охоплює фінансовий, промисловий, енергетичний сектора. Відповідно, сценарії використання хмарних мереж ЦОД стають усе більше різноманітними. Підприємства в кожній галузі намагаються ефективніше використовувати хмарні технології для досягнення прогресу в галузі й підвищення операційної ефективності. Huawei CloudFabric визначає сценарій-орієнтовані моделі фабрик, концентрується на мережі й додатках, а не мережевих елементах, і допомагає підприємствам швидко створити мережі на базі хмари з обліком конкретних сервісних сценаріїв і майбутнього розвитку, тим самим прискорюючи цифрову трансформацію.

За твердженням Huawei, рішення CloudFabric здатне спростити мережеву архітектуру й скоротити період проектування від декількох місяців до декількох днів. Крім того, завдяки відкритій SDN-архітектурі й автоматичній доставці мережевих налаштувань і правил забезпечення безпеки, це рішення скорочує час надання послуги від декількох тижнів до декількох хвилин, тим самим забезпечуючи зверхспрощене розгортання.

Нарешті, завдяки інтелектуальному мережевому аналізу й платформі FabricInsight продукт CloudFabric оптимізує прийняття рішень і скорочує строк виявлення збоїв від декількох годин до декількох хвилин.

5 вересня 2016 року компанія Huawei повідомила про випуск версії Cloud Fabric 5.0 для хмарних сервісів на платформі Huawei Fabric Insight Refined Operations and Maintenance (O&M).

Мережеве рішення для центра обробки даних Huawei Cloud Fabric

Серія комутаторів Huawei CloudEngine являє собою кілька лінійок комутаторів, що базуються на новітній апаратній архітектурі. Це найбільш продуктивні із представлених на ринку комутаторів базової мережі. Серія містить у собі чотири різні лінійки.

Лінійка PE12800 містить у собі високопродуктивні комутатори, які орієнтовані на експлуатацію в мережах центрів обробки даних і високошвидкісних мереж освітніх установ.

Ці комутатори базуються на новітній апаратній архітектурі й забезпечують комутаційну ємність 64 Тб/с. Кожний пристрій цієї серії укомплектовано 192 портами Ethernet 100 Гб, 384 портами Ethernet 40 Гб або 1536 портами Ethernet 10 Гб.

Інноваційна система охолодження забезпечує надійність корпоративного рівня. Крім того підтримується безліч передових технологій, що забезпечують економію споживаної енергії.

Лінійка CE7800 відмінно підходить для використання як основні комутатори або комутаторів агрегування в рамках університетських мереж або в центрах обробки даних.

Ці пристрої базуються на інноваційній архітектурі. Вони надають 40 високоплотних портів GE QSFP+, дозволяючи здійснювати комутацію другого й третього рівня зі швидкістю середовища передачі. Характеризуються відмінною енергоефективністю.

Лінійка CE6800 підтримує найвищу в галузі щільність 10 портів доступу GE. Підтримується реалізація великої кількості функцій ЦОД і можливість ефективного стекування. Інноваційна система охолодження, що дозволяє змінювати напрямок повітряного потоку, забезпечує надійну й стабільну роботу протягом тривалого часу.

Лінійка CE5800 – це перша в галузі серія комутаторів з 40 портами висхідної передачі GE. Інноваційний дизайн забезпечує виняткову щільність портів доступу. Це чудові комутатори для оптимізації мережевих інфраструктур рівня ЦОД або мереж університетів.

Серія комутаторів Huawei CloudEngine – це надійні, інноваційні й продуктивні рішення.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів SDN на основі Huawei Cloud Fabric. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем SDN на основі Huawei Cloud Fabric.
- Досліджена система SDN на основі Huawei Cloud Fabric.
- На основі отриманих результатів досліджень створена програмна реалізація системи SDN на основі Huawei Cloud Fabric. Розроблені алгоритми дозволяють успішно вирішувати завдання SDN на основі Huawei Cloud Fabric. 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., 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.
 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». Центральноукраїнський 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.
33. 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

К.Кузьмін, магістр гр. КІ-24М,

Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ВІДДАЛЕНОГО КОНТРОЛЮ НА ОСНОВІ ТЕХНОЛОГІЇ INTEL ME

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

система віддаленого контролю, Intel ME

Постановка проблеми. Технологія Intel ME (або AMT, Active Management Technology) є одним із самих загадкових і потужних елементів сучасних x 86-платформ. Інструмент споконвічно створювалося як рішення для віддаленого адміністрування. Однак він має настільки потужну функціональність і настільки непідконтрольний користувачам Intel-based пристроїв, що багато хто з них хотіли б відключити цю технологію, що зробити не так-те просто.

Підсистема Intel Management Engine (ME) являє собою додатковий «схований» процесор, що є присутнім у всіх пристроях на базі чипсетів Intel (не тільки в PC і ноутбуках, але й у серверах).

Середовище виконання ME ніколи не «спить» і працює навіть при виключеному комп'ютері (при наявності чергової напруги), а також має доступ до оперативної пам'яті, мережного інтерфейсу, USB контролера й убудованого графічного адаптера.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи віддаленого контролю на основі технології Intel ME.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи віддаленого контролю на основі технології Intel ME.

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

- Огляд існуючих систем віддаленого контролю на основі технології Intel ME.
- Дослідження системи віддаленого контролю на основі технології Intel ME.
- Програмна реалізація системи віддаленого контролю на основі технології Intel ME.

Об'єктом дослідження є процес віддаленого контролю на основі технології Intel ME.

Предметом дослідження є методи віддаленого контролю на основі технології Intel ME.

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

Виклад основного матеріалу. Незважаючи на настільки великі можливості Intel Management Engine (ME), існують питання до рівня захищеності ME – раніше дослідники вже знаходили серйозні уразливості й вектори атак. Крім того, підсистема

містить потенційно небезпечні функції – віддалене керування, NFC, схований сервісний розділ (hidden service partition). Інтерфейси підсистеми ME недокументовані, а реалізація закрита.

Всі ці причини приводять до того, що багато хто розглядають технологію ME у якості «апаратної закладки». Ситуацію збільшує той факт, що з однієї сторони в користувача пристрою немає можливостей по відключенню цієї функціональності, а з інший виробник устаткування може допустити помилки в конфігурації ME.

Гарна новина полягає в тому, що способи відключення ME все-таки існують.

Техніки відключення Intel ME

Фахівці описали трохи технік відключення даної підсистеми:

- Засновані на збої ініціалізації ME.
- Через механізм відновлення мікропрограми ME.
- Недокументовані команди.
- Недокументований механізм, призначений для розроблювачів апаратури –

Manufacture Mode.

Дослідники встановили, що розроблювачі апаратних платформ часто забувають виключати режим Manufacture Mode, що дозволяє використовувати останній метод на великій кількості комп'ютерів без яких або додаткових витрат у режимі «реального часу».

Більшість методів відключення використовують убудовані механізми ME, розроблені для вендорів пристроїв на платформі Intel.

І проте, виникає резонне питання: «чи дійсно ME перестає працювати в повному обсязі при використанні її убудованих механізмів відключення?» Як доказ факту відключення ME дослідники приводять наступний аргумент: ME працює у двох режимах використання пам'яті: тільки SRAM (убудований в ME) і SRAM + UMA. UMA – це частина пам'яті хоста, що використовується пам'ять, що підкачується як (swap). Після ініціалізації DRAM-контролера хостом ME завжди перемикається в режим SRAM + UMA.

Таким чином, якщо ME дійсно виключена, то при відключенні на апаратному рівні доступу ME до UMA-Пам'яті в довільний момент (засобами каналу VCm), у ME не буде відбуватися апаратних збоїв, пов'язаних з відсутністю даних і коду, які були витиснуті в UMA пам'ять (такі апаратні збої приводять до аварійного відключення живлення з основних апаратних компонентів платформи). З іншої сторони застосування цих методів дозволяє здійснити DoS-атаки на технологію AMT у випадку її застосування для віддаленого керування.

В 2005 році компанія Intel представила Active Management Technology (AMT) версії 1.0 – рішення для віддаленого адміністрування (керування, інвентаризація, відновлення, діагностика, усунення неполадок і т.д.) і захисту десктопних комп'ютерних систем, свого роду аналог технології Intelligent Platform Management Interface (IPMI), що використовується в серверах.

Архітектура AMT 1.0 ґрунтується на інтегрованому в чипсет мікроконтролері (Management Engine), наділеному досить вражаючими можливостями, наприклад:

- позаполосний (out-of-band) доступ до мережного інтерфейсу (Ethernet), що він розділяє з основним CPU, але, маючи власний контролер каналного рівня, здійснює моніторинг усього вхідного мережного трафіку, з якого «вирізує» (за допомогою Packet Filter) пакети, призначені для нього. Для ОС (наявність і стан якої, до речі, на роботу AMT ніяк не впливає) цей трафік уже не видний;

- внутрішній веб-сервер з TLS-шифруванням;
- доступ до периферійного встаткування, одержання й зберігання в енергонезалежній пам'яті (там же, де і його прошивання) інформації про нього.

А ще цей мікроконтролер починає працювати при подачі живлення на материнську плату комп'ютерної системи (тобто при підключенні комп'ютера до електричної мережі, ще до того, як користувач натисне кнопку Power).

Отже, Management Engine завжди включений, але використання можливостей AMT вимагає активації (має на увазі завдання пароля, мережних параметрів,...) в BIOS setup, а точніше в MEBx setup.

Похвально, що дефолтний пароль («admin») при першому вході обов'язково потрібно змінити на новим, задовольняючим певним вимогам: мінімум 8 символів, серед яких повинні бути присутнім хоча б одна цифра, одна заголовна буква й один спец. символ.

Після налаштування AMT-сумісної комп'ютерної системи, віддаленому адміністраторові стають доступними мережні функції (для їхнього використання потрібен введення логіна й пароля):

- інвентаризація апаратного забезпечення;
- веб-інтерфейс (по HTTP через порт 16992);
- Serial Over LAN (SOL) – віртуальний COM-Порт через мережу, що дозволяє включати / перезавантажувати / виключати комп'ютер, одержувати доступ до меню BIOS setup;
- IDE-Redirection (IDE-R) – опція перенапрямку завантаження з локального завантажувального пристрою на віддалене (попередньо підготовлений образ системи).

AMT 1.0 була реалізована на інтегрованому в південний міст чипсета (Input / Output Controller Hub, ICH) мережному модулі Intel 82573E series Gigabit Ethernet Controller.

Потім, в 2006 році, починаючи з AMT версії 2.0, мікроконтролер перенесли в північний міст чипсета (Graphics and Memory Controller Hub, GMCH). Саме тоді підсистему найменували в Intel Management Engine (ME) версії 2.0.

Одночасно із цим з'явився бренд Intel vPro, що позначав комплекс реалізованих на основі Intel ME технологій: AMT, Trusted Execution Technology (TXT) і Virtualization Technology (VT). Пізніше в цей список увійшли Identity Protection Technology (IPT) і Anti-Theft (AT).

Тоді ж Intel ME наділили ще більшою кількістю вражаючих можливостей, серед яких – повний доступ до всього вмісту оперативної пам'яті комп'ютера через внутрішній DMA-контролер, а надалі з'явилася можливість моніторингу відеопотоку, що виводиться на монітор (правда, тільки у випадку використання убудованого графічного ядра).

Поступово на цю підсистему стали навішувати усе більше різних системних функцій (деякими раніше займався BIOS) для забезпечення працездатності комп'ютерної платформи:

- частина функцій Advanced Control and Power Interface (ACPI) і Alert Standard Format (ASF);
- Quiet System Technology (QST);
- Integrated Clock Control (ICC);
- Trusted Platform Module (TPM);
- і інших технологій.

AMT теж не стояла на місці й активно розвивалася: змінювався состав використовуваних протоколів (наприклад, додалася підтримка HTTPS через порт 16993), у версії 6.0 для віддаленого адміністратора з'явилася фіча Remote Desktop, вона ж KVM (Keyboard Video Mouse), та інше.

Проте, через високу вартість реалізації, ця підсистема була присутня, за декількома виключеннями, тільки на материнських платах із чипсетами Intel лінійки Q.

Тоді до чого вся ця специфіка заліза із шильдиком vPro, що мало хто здобував через високу вартість (ну й інших причин)?

Справа в тому, що, починаючи з 2010 року, разом з переносом частини функціональних блоків північного мосту (графічне ядро, контролер пам'яті, ...) у корпус CPU, підсистему Intel ME стали вбудовувати в усі чипсети виробництва Intel. При цьому ME-контролер залишився в корпусі чипсета – в Platform Controller Hub (PCH). Це чипсети 5 серії й вище.

Функціональність AMT донині залишається доступною тільки на чипсетах лінійки Q, тобто тільки на встаткуванні із шильдиком vPro.

Думаєте тільки десктопи й ноутбуки? Ні, Intel-а відповідь!

Та ж доля осягла й серверні платформи від Intel: підсистема убудована в них, але під іншим ім'ям – Intel Server Platform Services (SPS). Відбулася поява й в SoC (on-a-Chip) під ім'ям Intel Trusted Execution Engine (TXE).

У підсумку архітектура кожної сучасної мобільної / лаптопної / десктопної / серверної комп'ютерної платформи із чипсетом / SoC від Intel містить у собі саму потайливу (від користувача системи) і привілейоване середовище виконання – підсистему Intel ME. Не дивно, що розробляючи цю архітектуру, компанія Intel була змушена серйозно попрацювати над її захистом від компрометації.

Розглянемо архітектуру цієї підсистеми, щоб розібратися в застосованій моделі безпеки.

Архітектура Intel ME

Intel Management Engine (ME) – убудована в комп'ютерні платформи підсистема, що забезпечує апаратно-програмну підтримку різних технологій Intel.

Як уже було сказано, перші версії цієї підсистеми були засновані на двокорпусних чипсетах Intel. Тоді як базова модель ME-контролера використовувався ARCTangent-A4 зі стандартною системою команд ARC32.

В однокорпусних чипсетах уже використовувалися ARCTangent-A5 / ARC600 з компактною системою команд ARCcompact (ARC16/32).

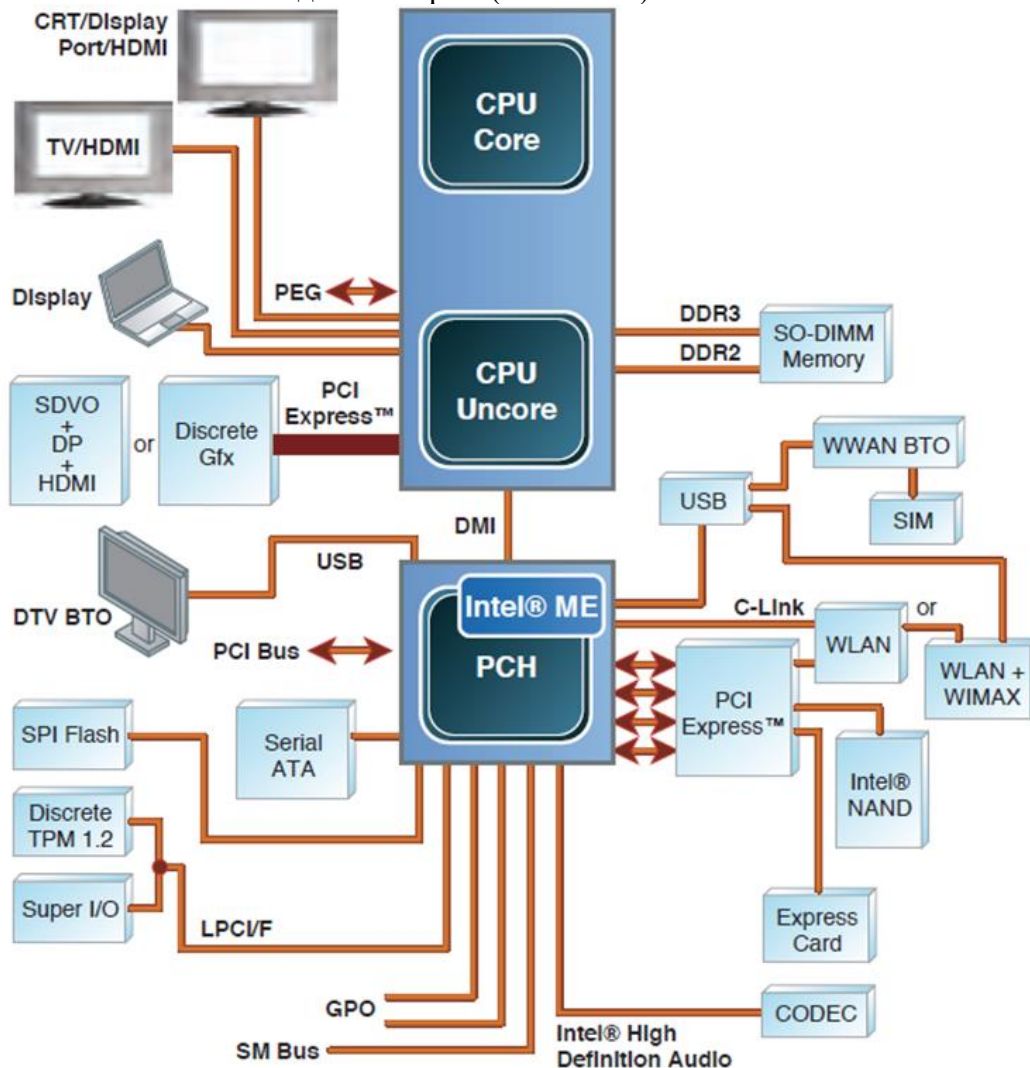


Рисунок 1 – Структурна схема системи

В Intel SoC (там де ця підсистема називається Intel TXE) як базова модель для ME-контролера використовується SPARC.

Нічого страшного, в Intel про це подбали: у самих останніх платформах (Skylake, чипсети 100 серії, Intel ME 11.x) ME-контролер має архітектуру... x86! У чипсетах тепер живе ще один x86.

Втім, состав компонентів підсистеми Intel ME (з версії 2.0) не змінювався. Це:

1. **ME-контролер** – убудований у чипсет 32-розрядний мікроконтролер типу RISC, що має внутрішні ROM і SRAM.

2. **Регіон ME в SPI флеш-пам'яті**, у якому зберігається розроблена й підписана компанією Intel прошивання ME-контролера (тому, саме Intel ME firmware).

3. **ME UMA** – схована від усіх, крім ME-контролера, область (16 – 32 МБ) в оперативній пам'яті комп'ютера, який він користується в якості runtime-memory для розміщення й запуску прошивання.

4. **Management Engine Interface (MEI)**, раніше відомий як **Host Embedded Controller Interface (HECI)**, – набір регістрів у конфігураційному просторі PCI і область в MMIO, що представляють собою інтерфейс для обміну інформацією з ME-контролером (по суті, єдиний канал зв'язку софту, що виконується на CPU, з підсистемою Intel ME).

5. **Окремий MAC** – контролер каналного рівня, що надає ME-контролеру out-of-band доступ до загального фізичного мережного інтерфейсу для віддаленого адміністрування комп'ютерною системою.

6. **Деякі модулі в BIOS**, відповідальні за ініціалізацію платформи й, що повідомляють про результати своєї роботи ME-контролеру через MEI.

У випадку наявності шильдика Intel vPro, до складу підсистеми Intel ME додатково входить BIOS-модуль **ME BIOS Extension (MEBx)**, що надає графічний інтерфейс (показаний вище), а також здійснює включення й конфігурування АМТ через MEI.

Таким чином, у нас є середовище виконання ring -3 (так її умовно називають) – 1 штука. Її привілейованість обумовлює здатностями, якими наділений ME-контролер (про їх написане вище), а скритність – повною відсутністю можливості контролювати програмними (і навіть апаратними, в production-версіях плат) засобами.

Архітектура ME-контролера

У середині ME-контролера, крім мікропроцесора ARC / SPARC / x86:

– ME ROM – енергонезалежна неперезаписувана пам'ять, що, у якій зберігається стартовий код ME-контролера;

– ME SRAM – оперативна пам'ять використовується ME-контролером при неприступності ME UMA, наприклад, на ранніх етапах роботи;

– кеш коду й кеш даних, для підвищення продуктивності при роботі з пам'яттю;

– C-Link (Controller Link) – шина, що дозволяє ME-контролеру взаємодіяти з периферійним апаратним забезпеченням у режимах S5 (System shutdown) / S3 (Sleep mode);

Різні апаратні блоки:

– високоточний таймер і WDT;

– контролер переривань;

– контролери пам'яті й DMA;

– інтерфейс HECI / MEI;

– RNG, акселератор криптографічних функцій і функцій стиску.

Самий час розібратися в тому, як від модифікацій захищений код, що управляє всім цим багатством.

Прошивання Intel ME

Intel ME firmware, залежно від наповнення, розрізняють двох типів:

– 1.5 МБ, урізані версії;

– 5 МБ, повні версії.

Тип прошивання визначає состав прикладних модулів, у яких реалізовані певні технології (наприклад, АМТ, ІРТ і т.д.). Хоча є й базова частина, однакова для різних прошивань:

- Bring Up, перший запускатися модуль, що, із прошивання.
- Kernel, ядро ОСРВ Thread.
- Деякі драйвери й служби.

В SPI флеш-пам'яті є кілька регіонів:

– Flash Descriptors, у якому зберігаються покажчики на всі інші регіони, а також read / write привілею для користувачів цієї пам'яті. Відзначимо, що звичайно цими дескрипторами забороняється перезапис ME регіону всім, за винятком самого ME-контролера;

- Gb (Gigabit Ethernet);
- ME, тут зберігається прошивання ME-контролера;
- BIOS;
- 3PDS (Third Party Data Storage), опціональний регіон.

Тепер глянемо на сам регіон ME. Це Flash Partition Table (FPT) – таблиця розділів ME firmware. У ній зберігаються покажчики на різного типу (код, дані, віртуальна область, ...) розділи і їхні параметри. Цілісність цієї таблиці контролюється одним байтом чексумми по зсуву 1Bh.

Нас цікавлять executable-розділи, тобто ті, що зберігають здійснений код. Їх звичайно трохи, розглянемо один з них.

На початку кодового розділу розташовується маніфест, що складається із заголовка (зі службовими даними й ЕЦП) і таблиці модулів.

У наведеному дампі можна побачити 2048-бітний відкритий RSA ключ (модуль за зсувом 80h відносно початку розділу й експонента за зсувом 180h). Далі треба 256 байт сигнатури.

Своїм закритим ключем компанія Intel підписує частина заголовка маніфесту й таблицю модулів, прикладаючи отриманий підпис і відкритий ключ для перевірки.

А от і фрагмент таблиці модулів розглянутого розділу. Ця таблиця містить заголовки модулів, де зазначені деякі параметри й хеш-сума SHA256 (за зсувом 14h усередині заголовка).

Згенерувати власну пару ключів RSA-2048 і підписати ними розділ не вийде через те, що цілісність прикладеного відкритого ключа перевіряється стартовим кодом в ME ROM, у якому зберігається хеш-сума SHA256 відкритого ключа компанії Intel.

Цього цілком достатньо для захисту прошивання від підроблення. Програмно перезаписати ME регіон SPI флеш-пам'яті не можна (пам'ятаємо про дозволи в Flash Descriptors), апаратні засоби, звичайно дозволяють обійти це обмеження, але контроль дійсності не виключити.

Подивимося убік захисту від бінарних уразливостей.

Ми побачили, що весь здійснений код ME firmware розбитий на модулі різного призначення.

В ME-контролера є два режими роботи: привілейовані й користувальницький (аналоги kernel mode і user mode для CPU). Привілейований режим відрізняє, насамперед, можливість доступу до апаратних ресурсів і можливість обігу по адресах поза відведеним цим модулем діапазону пам'яті.

Кожний модуль запускається й працює в заданому (у заголовку цього модуля) режимі.

Распарсив весь ME регіон можна побачити, що привілейований режим використовується ядром ОСРВ і деякими драйверами. Службам і прикладними модулям, як і покладено, приділяється тільки користувальницький режим.

Ми показали, що підсистема Intel ME є невід'ємною частиною архітектури сучасних комп'ютерних платформ (на основі чипсетів / SoC Intel). Очевидно, що її компрометація надає потенційному злоумисникові безмежні можливості контролю над платформою: доступ

до всього вмісту оперативної пам'яті (системна пам'ять, пам'ять гіпервізора, SMRAM, ACRAM, виділювана пам'ять для графічного ядра – GFX UMA), out-of-band доступ до мережного інтерфейсу (моніторинг усього мережного трафіку), віддалений контроль як частина штатної функціональності АМТ, перезапис будь-яких регіонів SPI флеш-пам'яті. Бонусом до цього є повна відсутність можливостей виявлення.

Це є вагомою причиною для наявності в Intel ME серйозного захисту. Ми вважаємо, що вендори будь-якого мережного встаткування, що вбудовується, повинні прагнути до описаної моделі безпеки. Її характеризують наступні принципи:

- заборона на використання дефолтного пароля, примус до установки сильного пароля (відповідного певним вимогам);
- використання функцій шифрування в мережних протоколах;
- контроль цілісності й дійсності всього здійсненого коду прошивання;
- механізми захисту від експлуатації бінарних уразливостей.

Заздалегідь прокоментую можливі заклики використовувати комп'ютерні платформи на основі CPU і чипсетів від AMD: у них є дуже схожа технологія, називається Platform Security Processor (PSP). Представлена не дуже давно, в 2013 році.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів віддаленого контролю на основі технології Intel ME. Рішення даного завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем віддаленого контролю на основі технології Intel ME.
- Досліджена система віддаленого контролю на основі технології Intel ME.
- На основі отриманих результатів досліджень створена програмна реалізація системи віддаленого контролю на основі технології Intel ME. Розроблені алгоритми дозволяють успішно вирішувати завдання віддаленого контролю на основі технології Intel ME. 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». 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., 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.

ЗМІСТ

<i>О.Коломієць, В. Рябовол</i>	ВИКОРИСТАННЯ ЗАРУБІЖНОГО ДОСВІДУ КОНТРОЛЮ ЯКОСТІ ОСВІТНЬОЇ ДІЯЛЬНОСТІ	4
<i>О.Коломієць, К. Сипко</i>	ШТУЧНИЙ ІНТЕЛЕКТ ЯК ІНСТРУМЕНТ ПІДТРИМКИ ІНФОРМАЦІЙНОГО ОБСЛУГОВУВАННЯ КОРИСТУВАЧІВ	8
<i>О. Коломієць, Т. Щетініна</i>	ПРАВОВІ ЗАСАДИ ДОКУМЕНТАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ЗВЕРНЕНЬ ГРОМАДЯН В ОРГАНИ ПУБЛІЧНОЇ ВЛАДИ	11
<i>Є. Сергієнко, О. Скібінський, В. Селєхова</i>	ВДОСКОНАЛЕННЯ КОНСТРУКЦІЇ РІЗЬБОВОЇ ФРЕЗИ	14
<i>Б. Андрусик</i>	ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ СКРЕМБЛЮВАННЯ ЦИФРОВОГО СИГНАЛУ НА МОБІЛЬНИХ ПРИСТРОЯХ	17
<i>П.Арсієвич</i>	ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ВІДЕОНАГЛЯДУ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ HD-SDI	26
<i>С.Батрак</i>	ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ПРОАКТИВНОГО МОНІТОРИНГУ МЕРЕЖЕВОГО ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ	34
<i>Д.Бобровський</i>	ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ЗАХИСТУ ДАНИХ GPRS-МЕРЕЖІ, РОЗГОРНУТОЇ НА ПРИСТРОЯХ, ЯКІ ПРАЦЮЮТЬ ПІД ОС ANDROID	42
<i>О.Бойко</i>	ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ КЛІЄНТА ВКЗ ЗА ДОПОМОГОЮ ТЕХНОЛОГІЇ WEBRTC	55
<i>Л.Буханенко</i>	ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ МЕРЕЖЕВОЇ БЕЗПЕКИ ПОБУДОВАНОЇ НА ОСНОВІ РІШЕНЬ AXIS	66
<i>К.Василенко</i>	ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У МЕРЕЖЕВИХ CLOUD-СИСТЕМАХ	74
<i>І.Воропай</i>	ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ВИЯВЛЕННЯ УРАЗЛИВИХ ДОДАТКІВ У МЕРЕЖЕВИХ CLOUD-СЕРВІСАХ	89
<i>С.Главнов</i>	ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ МЕРЕЖЕВОЇ SIEM ДЛЯ АНАЛІЗУ ЗАГРОЗ БЕЗПЕЦІ КОРПОРАТИВНОЇ ІТ-ІНФРАСТРУКТУРИ	99
<i>М.Грищенко</i>	ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ МЕРЕЖЕВОГО АНТИВІРУСНОГО КОМПЛЕКСУ ДАТА-ЦЕНТРУ	109

А.Дабич

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ АУДИТУ БЕЗПЕКИ МЕРЕЖЕВИХ ICS/SCADA 115

Н.Дворцов

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ІНТЕЛЕКТУАЛЬНОГО РОЗПІЗНАВАННЯ З ВИКОРИСТАННЯМ ОСОБЛИВИХ ТОЧОК 126

О.Драганець

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ГІПЕРКОНВЕРГЕНТНОЇ ІНФРАСТРУКТУРНОЇ ПЛАТФОРМИ 135

М.Дроздов

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ЗАХИСТУ КОРПОРАТИВНИХ ДОДАТКІВ, ЯКІ РОЗРОБЛЯЮТЬСЯ ЗА ДОПОМОГОЮ МЕТОДОЛОГІЇ AGILE 148

Є.Завірюха

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ ПРОГРАМНО-АПАРАТНОГО КОМПЛЕКСУ МОНІТОРИНГУ ЖИТТЄВИХ ПОКАЗНИКІВ ПАЦІЄНТІВ ІЗ ПЕРЕДАЧЕЮ ДАНИХ НА РОБОЧЕ МІСЦЕ ЛІКАРЯ 159

М.Іванченко

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ МЕРЕЖЕВОГО КОРПОРАТИВНОГО ЦЕНТРУ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ (SOC) 168

Н.Касьянов

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ВИЗНАЧЕННЯ МІСЦЕЗНАХОДЖЕННЯ ЗА ДОПОМОГОЮ ПРОТОКОЛУ APPLE LOCATION SERVICES PROTOCOL 182

Д.Каишуровський

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ МЕРЕЖЕВОГО МОНІТОРИНГУ ТА КОНТРОЛЮ СТАНУ ІТ 192

І.Кіблик

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ ТА АУДИТУ ДІЙ ПРИ РОБОТІ З МЕРЕЖЕВОЮ БАЗОЮ ДАНИХ 203

Т.Кіріченко

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ НЕЙРОМЕРЕЖЕВИХ ЕКСПЕРТІВ БЕЗПЕЧНОЇ МАРШРУТИЗАЦІЇ У АНТИВІРУСИ 210

Д.Ковальов

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ МЕРЕЖЕВОГО ВІДЕОПОСТЕРЕЖЕННЯ ДЛЯ РЕАЛІЗАЦІЇ СТРАТЕГІЇ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПІДПРИЄМСТВА 221

В.Ковальчук

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ПОВЕДІНКОВОГО АНАЛІЗУ КОРИСТУВАЧІВ ЗА ДОПОМОГОЮ КОНЦЕПЦІЇ UEBA 229

Д.Ковтуненко

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ІНТЕЛЕКТУАЛЬНОЇ ІНТЕГРАЦІЇ ІСНУЮЧИХ КОМПОНЕНТ ІТ-СИСТЕМИ З ХМАРНИМИ СЛУЖБАМИ НАСТУПНОГО ПОКОЛІННЯ 241

Д.Колесник

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ПРОТИДІЇ ДЕТЕКТУВАННЮ АНТИВІРУСНОЮ СИСТЕМОЮ ЗА ДОПОМОГОЮ ШТУЧНОГО ІНТЕЛЕКТУ 250

С.Коробка

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ
КРИТИЧНИХ РЕСУРСІВ АСУ ТП 263

В.Кравченко

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ІНТЕЛЕКТУАЛЬНОЇ
ОПТИМІЗАЦІЇ ПРОДУКТИВНОСТІ ТА НАДІЙНОСТІ ХМАРНИХ МЕРЕЖЕВИХ СИСТЕМ
ЗБЕРІГАННЯ ДАНИХ 272

О.Кривда

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ДЕДУПЛІКАЦІЇ В
ІНФРАСТРУКТУРІ РЕЗЕРВНОГО КОПІЮВАННЯ 280

В.Кривожиha

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ SDN НА ОСНОВІ HUAWEI CLOUD
FABRIC 288

К.Кузьмін

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ВІДДАЛЕНОГО КОНТРОЛЮ НА
ОСНОВІ ТЕХНОЛОГІЇ INTEL ME 297