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 поводження основних ймовірносно-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 $\Re = \{V_n \mid n \in 1, N\}$ – безліч маршрутизаторів у ТКС, V_n – n-й маршрутизатор, $N = |\Re|$ – число маршрутизаторів, $\Im = \{\theta_\xi \mid \xi \in 1, \Theta\}$ – 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 $\aleph = \{\eta_s \mid s \in 1, M\}$, де $\eta_s = \{\theta_{s,c} \mid \theta_{s,c} \in \Im; \quad c \in 1, \Theta\}$ – s-*й* маршрут, $s \in 1, M$, $|\eta_s| = \Psi_s$, M – кількість маршрутів, $\theta_{s,c}$ – канал зв'язку з номером *з*, що належить s-*му* маршруту, Ψ_s – кількість каналів зв'язку на s-*м* маршруті.

Формування множини $\aleph$ 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 нейромережевих експертів безпечної маршрутизації необхідно підготувати й систематизувати дані, на основі яких виробляється навчання його окремих нейромережевих 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 нейромережевих 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.

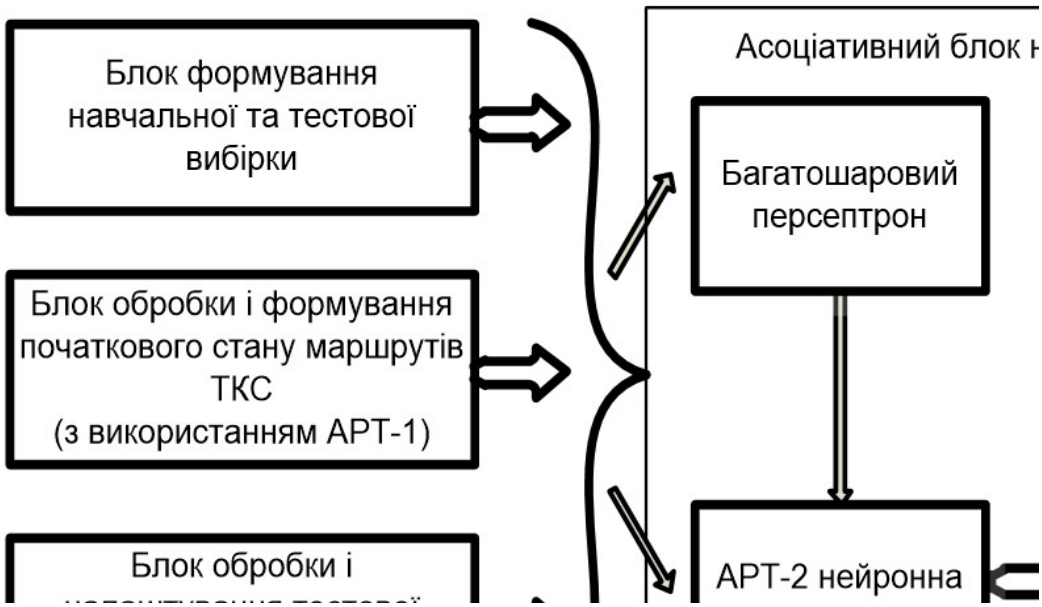

Рисунок 1 – Структурна схема системи

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 нейромережевих 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 нейромережевих 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 (логіни/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 необов'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 прогнозну 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 токенізація, 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 вразливості, 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 IT-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 IT-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 нейромережевих експертів безпечної маршрутизації у антивіруси. Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем нейромережевих експертів безпечної маршрутизації у антивіруси.

– Досліджена система нейромережевих експертів безпечної маршрутизації у антивіруси.

– На основі отриманих результатів досліджень створена програмна реалізація системи нейромережевих експертів безпечної маршрутизації у антивіруси.

Розроблені алгоритми дозволяють успішно вирішувати завдання нейромережевих 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., Корчинский В.В., Кудирко В.М., Фесенко А.О.; за заг. ред. В.М. Петрика, М.М. Присяжнюка.– К.: Видавничий центр “Кафедра”, 2025.– 320 с.
4. Усік, П.С., Смірнова, Т.В., Буравченко, К.О., Смірнов, О.А., Улічев, О.С., Смірнов, С.А. «Дослідження технологій забезпечення кібербезпеки банківських систем з використанням штучного інтелекту». Кібербезпека: освіта, наука, техніка. 2025. Том 1 № 29. С.704–716, 2025
5. Kuznetsov, O., Frontoni, E., Kuznetsova, K., Arnesano, M., Smirnov, O. «A secure biometric authentication architecture for blockchain-driven cyber-physical systems». Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications, 2025, pp. 193–224.
6. Kuznetsov, O., Atzeni, G., Arnesano, M., Randieri, C., Smirnov, O. «Secure IoT-based smart wheelchair system: From implementation to security enhancement strategy». Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications, 2025, pp. 225–257.
7. Kuznetsov, O., Smirnov, O., Kuznetsova, T., Shaikhanova, A., Svatowsky, I. «Privacy-utility trade-offs in IoT networks: A comparative analysis of differential privacy mechanisms for sensor data aggregation». Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications, 2025, pp. 589–622.
8. Lakhno, V., Malyukov, V., Smirnov, O., 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., 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., Конопліцька-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., Yenchev, 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., Chubaievskyi, V., Khorolska, K., Bebeshko, B. «Selection of a Rational Composition of İnformation Protection Means Using a Genetic Algorithm». In: Rajakumar, G., Du, KL., Vuppalapati, 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». ІІ Міжнародна науково-практична Інтернет-конференція «Інновації та перспективні шляхи ȟозвитку 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.