КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.29.934
УДК 004.056.53:004.732

Аверічев Ігор Миколайович
к.е.н., доцент кафедри Технічних систем кіберзахисту
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID ID: 0009-0008-9766-0115
iaverichev19@gmail.com

Роженко Артем Сергійович
аспірант
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID ID: 0009-0000-2900-349X
a.rozhenko@stud.duikt.edu.ua

Кихтенко Євген Миколайович
аспірант
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID ID: 0009-0008-1696-1048
firementer@gmail.com

ІННОВАЦІЙНІ ПІДХОДИ ДО ПІДВИЩЕННЯ РІВНЯ КІБЕРБЕЗПЕКИ КОРПОРАТИВНИХ МЕРЕЖ ПРИ ВИКОРИСТАННІ ХМАРНИХ ТЕХНОЛОГІЙ

Анотація. Розглянуті сучасні методи та підходи до підвищення рівня кібербезпеки корпоративних мереж у контексті використання хмарних технологій. Аналізуються загрози, пов’язані з хмарними обчисленнями, та пропонуються ефективні інноваційні моделі захисту, включаючи Zero Trust Architecture, AI-підходи до виявлення загроз, використання блокчейну, контейнерну безпеку та шифрування з політикою управління ключами, які забезпечують багаторівневу та адаптивну систему захисту, здатну оперативно реагувати на зміну типів загроз та мінімізувати потенційні ризики витоку або компрометації даних. Застосування цих підходів дозволяє створити стійке до атак середовище, в якому корпоративна інформація залишається захищеною навіть у умовах зростаючої складності та інтенсивності кібератак. Також акцентується увага на важливості інтегрованого підходу до безпеки, який поєднує технічні, організаційні та управлінські заходи. У сучасних умовах стрімкого розвитку ІТ-технологій та зростання залежності бізнесу від хмарної інфраструктури, важливо не лише впроваджувати інноваційні засоби захисту, але й забезпечити їхню інтеграцію в єдину систему управління безпекою, що охоплює всі рівні корпоративної мережі - від периферійних пристроїв до хмарних платформ, включаючи політики доступу, шифрування, автентифікацію, контроль за поведінкою користувачів та аналітику інцидентів у режимі реального часу.

Ключові слова: кібербезпека; корпоративні мережі; хмарні технології; Zero Trust; штучний інтелект; DevSecOps; хмарна безпека; кіберзагрози; захист даних; багаторівнева автентифікація.

ВСТУП

Розвиток хмарних технологій за останні роки суттєво трансформував підходи до управління корпоративними інформаційними системами. Хмара надає компаніям можливість забезпечити високу гнучкість, масштабованість та економічну ефективність, що дозволяє знизити витрати на інфраструктуру та оптимізувати операційні процеси. Однак, разом із значними перевагами, хмарні обчислення також створюють нові виклики в сфері кібербезпеки. Хмарне середовище підвищує ризики, пов’язані з вразливістю до несанкціонованого доступу, витоків даних та атак на мережеві структури, оскільки дані та додатки зберігаються на віддалених платформах, доступних через інтернет. Тому

актуальність розробки та впровадження ефективних та інноваційних підходів до захисту корпоративних мереж постійно зростає. Для забезпечення високого рівня кібербезпеки в умовах хмарних технологій необхідно впроваджувати новітні моделі захисту, такі як Zero Trust Architecture, AI-технології для виявлення загроз, використання блокчейну, контейнерну безпеку та розробку політик управління ключами шифрування [1].

Разом із впровадженням новітніх рішень у сфері інформаційної безпеки, постає завдання їх ефективної інтеграції в корпоративні інфраструктури, що динамічно змінюються. Більшість компаній стикаються з проблемами сумісності між традиційними методами захисту та новими хмарними підходами, а також із необхідністю постійного оновлення політик безпеки відповідно до нових кіберзагроз. Додатково, зростає потреба в розробці комплексних стратегій безпеки, які поєднували б технічні рішення з організаційними та управлінськими аспектами захисту даних [1]–[25]. Усе це вимагає системного підходу до аналізу та впровадження інноваційних моделей кіберзахисту в умовах хмарних обчислень.

Тому метою цієї роботи є дослідження сучасних методів та моделей, для підвищення рівня кібербезпеки корпоративних мереж при використанні хмарних технологій та формування рекомендацій щодо впровадження найбільш ефективних інноваційних рішень в існуючі інформаційні системи підприємств. Особливу увагу приділено оцінці ефективності таких підходів, як архітектура Zero Trust, штучний інтелект у виявленні загроз, блокчейн-технології, захист контейнеризованих середовищ та системи управління ключами шифрування.

У зв’язку з різким збільшенням обсягу даних і високою потребою в мобільності та гнучкості корпоративних систем, хмарні технології стали важливим елементом інфраструктури більшості сучасних компаній [3]. Вони пропонують низку переваг, таких як зниження витрат на апаратне забезпечення, спрощення масштабування ресурсів, підвищення ефективності операційних процесів і доступ до новітніх технологій. Проте разом із значними перевагами хмарні обчислення створюють нові загрози для безпеки корпоративних даних. Оскільки дані і додатки зберігаються на віддалених серверах, доступних через інтернет, виникають нові ризики, пов’язані з несанкціонованим доступом, витоками інформації, а також атаками на мережеві структури, що вимагають застосування інноваційних підходів до захисту.

Розвиток новітніх технологій безпеки, таких як Zero Trust Architecture, використання штучного інтелекту для виявлення загроз, блокчейн для підтвердження цілісності даних та контейнеризація для ізоляції додатків, є необхідною умовою для підвищення рівня кібербезпеки в хмарних середовищах. Ці інноваційні методи дозволяють створити більш надійні системи захисту, адаптовані до швидко змінюваного середовища цифрових загроз [3].

Однак попри зростаючу кількість доступних технологій, реальна ефективність забезпечення кібербезпеки в хмарних середовищах залишається проблематичною через низку чинників, таких як складність інтеграції нових систем у вже існуючі інфраструктури, швидкість адаптації до нових загроз, а також необхідність постійного вдосконалення політик безпеки на всіх рівнях організації [4]–[6].

Враховуючи постійну еволюцію кіберзагроз та необхідність швидкої адаптації до нових умов, дослідження сучасних підходів до забезпечення безпеки корпоративних мереж у хмарних технологіях є надзвичайно актуальним для розробки ефективних і практичних рішень, здатних захистити організаційні дані від можливих атак і витоків.

Загрози та виклики кібербезпеки в хмарних середовищах.

1. Невдалі конфігурації в хмарних середовищах — це одна з основних причин кіберінцидентів. Вони виникають через некоректне налаштування ресурсів, що відкриває вразливості для внутрішніх або зовнішніх загроз. Типові помилки включають: відсутність логування, відкриті порти, ненадійне управління даними, надмірні привілеї користувачів та специфічні помилки, пов'язані з провайдерами (наприклад, відкриті AWS S3 бакети). Така неправильна конфігурація часто пов'язана з браком знань, швидким розгортанням без належного контролю змін та складністю мультихмарних середовищ [7].

2. Управління ідентифікацією та доступом (IAM) у хмарі є критично важливим, але водночас складним. Різні хмарні провайдери мають унікальні системи IAM, що ускладнює контроль і може призводити до надлишкових дозволів або непослідовних політик. До того ж, короткочасність ресурсів, масштабування та гібридні середовища створюють додаткові виклики. Ефективне IAM вимагає надійної автентифікації (SSO, MFA), централізованого моніторингу й відповідності нормативним вимогам [8].

3. API та користувацькі інтерфейси (UI), які використовуються для взаємодії з хмарними ресурсами, часто мають вразливості — ненадійна автентифікація, відсутність шифрування, неконтрольований доступ. Вразливі API — популярна ціль для атак: за даними Akamai, 29% веб-інцидентів у 2023 році були спрямовані саме на API. Недостатній захист цих інтерфейсів, разом зі слабкими паролями та поганим управлінням сесіями, відкриває шлях до витоків даних і порушення сервісів. У відповідь, OWASP включила захист API до оновленого списку пріоритетів безпеки [1], [9].

4. Стратегія безпеки хмарних технологій охоплює вибір архітектури, моделей хмарних сервісів, постачальників, регіонів обслуговування та засобів контролю. Вона повинна враховувати бізнес-цілі, обмеження, пріоритети компанії, а також вплив на екологію, суспільство та національні вимоги. Така стратегія визначає майбутній IAM-дизайн, мережеві інструменти та підхід до контролю безпеки, закладаючи основу для гнучкого, поетапного впровадження хмарних рішень [10].

5. Важливою складовою є управління ризиками сторонніх ресурсів, які можуть включати бібліотеки з відкритим кодом, SaaS-продукти або API. Такі залежності часто становлять частину хмарних додатків і вважаються вразливостями ланцюга постачання. Як показують дослідження, більшість інцидентів відбувається через сторонні компоненти. Уразливість у навіть одному рядку коду може стати точкою входу для зловмисника, особливо коли йдеться про невеликих постачальників, інтегрованих у масштабні рішення [11].

6. Хоча розробники не мають на меті створювати вразливі продукти, складність хмарних середовищ і програмного забезпечення часто призводить до помилок. Для їхнього усунення потрібен захищений *SDLC*, автоматизоване тестування безпеки, інструменти IAM та постійне навчання розробників. Розподіл відповідальності між CSP і компаніями означає, що обидві сторони повинні забезпечувати безпеку: CSP — на рівні платформи, розробники — у своєму коді. Це дозволяє зосередитися на унікальній бізнес-цінності, не нехтуючи безпекою [12].

7. Ризик випадкового розголошення даних у хмарних середовищах зростає, головним чином через неправильну конфігурацію. Навіть попри наявність налаштувань за замовчуванням, що забезпечують приватність, зручність часто переважає безпеку, що призводить до витоків. Наприклад, публічні відра Amazon S3 або репозиторії GitHub можуть містити чутливу інформацію — від паспортних даних до медичних записів. Такі інциденти часто можна запобігти завдяки кращому контролю доступу та навчанню користувачів [13].

8. Системні вразливості хмарних платформ включають чотири основні категорії: неправильну конфігурацію, вразливості нульового дня, невиправлене програмне забезпечення та слабкі облікові дані. Усі ці фактори можуть бути використані зловмисниками для атак. Для зменшення ризиків потрібні регулярне сканування вразливостей, управління патчами та впровадження архітектури нульової довіри, яка забезпечує мінімальні привілеї та постійний контроль доступу [14].

9. Обмежена видимість хмарних сервісів ускладнює контроль за використанням та безпекою хмарних ресурсів. Несанкціоноване використання додатків (тіньова IT) або зловживання затвердженими сервісами загрожують витоком даних. За даними 2023 року, більшість витоків сталася через людські помилки, а значна частина атак залишилася непоміченою. Це підкреслює необхідність ефективних інструментів моніторингу, аналітики та контролю у хмарному середовищі [15].

10. Неавторизований доступ до хмарних ресурсів, таких як віртуальні машини та бази даних, може становити серйозну загрозу для безпеки. Без належної автентифікації або дотримання принципу найменших привілеїв ці ресурси можуть бути вразливими до зловмисників. Окрім базової автентифікації, для захисту даних рекомендуються методи, такі як багатофакторна автентифікація, сторонні платформи для перевірки особи користувачів, керування доступом і постійний моніторинг активності, що допомагають виявити потенційні витоки даних [16].

11. Постійні загрози від APT (Advanced Persistent Threats) залишаються серйозним ризиком для хмарних технологій. Ці складні атаки, які проводяться національними державами або організованими злочинними угрупованнями, використовують вразливості, фішинг, крадіжку облікових даних і руйнівні атаки. Щоб захиститися від таких загроз, організаціям слід застосовувати багаторівневу стратегію безпеки, яка включає розвідку про кіберзагрози, навчання команд реагування та ефективний моніторинг для виявлення і знешкодження атак [17].

Цей аналіз включає змінний ландшафт загроз безпеці хмарних технологій, зокрема постійні проблеми, як неправильні конфігурації, слабкі місця IAM, незахищені API та відсутність комплексної стратегії безпеки, що залишаються актуальними з 2022 року. Майбутні загрози будуть визначатися кількома тенденціями, зокрема зростанням складності атак, де зловмисники використовуватимуть штучний інтелект для експлуатації вразливостей, ризиками для ланцюгів поставок через складність хмарних екосистем, змінами в регуляціях щодо конфіденційності та безпеки даних, а також поширенням програм-вимагачів як послуги (RaaS), що вимагатиме надійних рішень для резервного копіювання та контролю доступу [18]. Організаціям слід адаптувати свої стратегії безпеки, щоб ефективно реагувати на ці нові виклики.

Інноваційні методи забезпечення кібербезпеки.

Інноваційні методи забезпечення кібербезпеки сприяють підвищенню рівня захисту в умовах сучасних цифрових загроз. Новітні технології, стратегії та підходи дозволяють організаціям адаптуватися до швидко змінюваного ландшафту кіберзагроз і ефективно забезпечувати безпеку своїх систем і даних. Я зосереджуся на новітніх технологіях, стратегіях та підходах, що дозволяють організаціям адаптуватися до швидко змінюваного ландшафту кіберзагроз і ефективно забезпечувати безпеку своїх систем і даних.

1. Zero Trust Architecture (ZTA)

Архітектура нульової довіри (ZTA) є підходом до забезпечення безпеки в IT-інфраструктурі організації, який ґрунтується на принципі, що жодна особа або пристрій

не повинні бути довіреними за замовчуванням. Це означає, що доступ до ресурсів надається лише після ретельної перевірки, незалежно від того, чи знаходиться користувач чи пристрій всередині чи поза межами мережі. Основні елементи ZTA включають керування ідентифікацією та доступом, багатофакторну автентифікацію, мікросегментацію, шифрування та моніторинг у реальному часі.

Ідея архітектури нульової довіри була вперше запропонована в 2011 році Джоном Кіндервагом. Вона набула актуальності в умовах цифрової трансформації та зростання мобільності і хмарних технологій. Архітектура дозволяє організаціям безпечно підтримувати доступ до ресурсів у умовах постійної зміни технологічних середовищ і віддаленої роботи [18].

Ключовими принципами ZTA є постійний моніторинг та перевірка, доступ із найменшими привілеями та припущення про порушення безпеки. Це включає автентифікацію користувачів і пристроїв, використання багатофакторної автентифікації та обмеження прав доступу до мінімуму, необхідного для виконання функцій. Окрім того, архітектура передбачає, що порушення безпеки неминучі, тому система повинна бути спроектована так, щоб мінімізувати можливі наслідки таких порушень.

На рис. 1 представлено основні логічні компоненти архітектури нульової довіри.

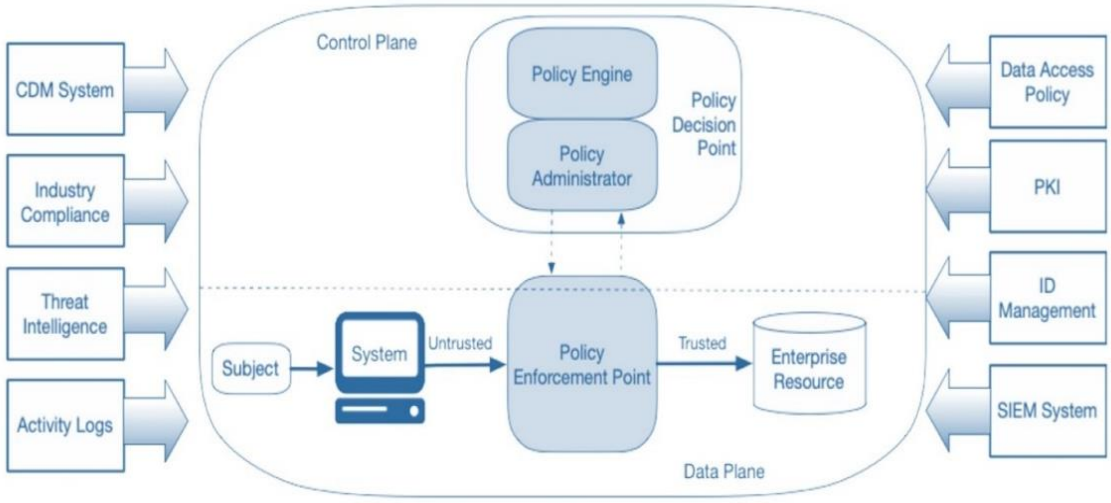

Рис. 1. Основні логічні компоненти архітектури нульової довіри

Основні переваги ZTA включають покращену безпеку завдяки постійній автентифікації та обмеженому доступу, захист від витоку даних, покращену видимість та моніторинг мережевих дій, а також зниження ризику розвитку постійних загроз. Це особливо важливо для організацій, що працюють у хмарних середовищах або підтримують віддалену роботу. Крім того, ZTA забезпечує відповідність нормативним вимогам щодо захисту даних, таких як GDPR та HIPAA [18].

Впровадження архітектури нульової довіри вимагає ретельної оцінки активів і робочих процесів, а також визначення та автоматизації політик доступу. Це також включає регулярне тестування та моніторинг системи для виявлення аномалій. Архітектура ZTA є гнучкою і масштабованою, що дозволяє ефективно реагувати на нові загрози та зберігати високий рівень безпеки навіть у складних IT-інфраструктурах.

Як приклад використання підходу архітектури нульової довіри розглянемо проєкт компанії Surespan. Компанія Surespan, яка спеціалізується на виготовленні люків для дахів та підлог, зіштовхувалася з проблемою ефективного доступу до критичних файлів

та ресурсів для своїх співробітників, які працюють у різних точках світу. Раніше компанія використовувала традиційну модель безпеки, засновану на VPN, але з ростом бізнесу і збільшенням кількості міжнародних локацій це призводило до проблем із швидкістю з'єднання та безпекою. Кожен новий об'єкт або підрядник вимагали налаштування VPN, що збільшувало час на отримання доступу до необхідних ресурсів і створювало потенційні вразливості в захисті даних.

Для вирішення цих проблем Surespan впровадила модель безпеки з нульовою довірою (ZTA) за допомогою рішення від компанії Zscaler. Ця технологія дозволяє забезпечити безпечний доступ до ресурсів компанії без необхідності постійного підключення до всієї мережі. За допомогою ZTA доступ отримують лише авторизовані користувачі, причому автентифікація відбувається на кожному етапі підключення. Це не тільки підвищує безпеку, але й дозволяє значно скоротити час на підключення, оскільки замість того, щоб перенаправляти трафік через перевантажені центральні сервери, користувачі з'єднуються безпосередньо з необхідними програмами та файлами. В результаті впровадження ZTA компанія змогла забезпечити більш швидкий та безпечний доступ до ресурсів для своїх співробітників у різних регіонах, значно покращивши ефективність роботи та зменшивши затримки при виконанні проектів [19].

Використання штучного інтелекту (AI) та машинного навчання (ML)

AI та генеративний AI внесли новий рівень загрози для традиційних атак, що ускладнило їх виявлення за допомогою класичних методів.

Використання штучного інтелекту (AI) та машинного навчання (ML) є перспективними підходами до підвищення рівня кібербезпеки корпоративних мереж, особливо в умовах швидко зростаючих загроз і складності кіберзлочинності. Застосування цих технологій дозволяє не тільки покращити виявлення та реагування на інциденти, а й автоматизувати багато аспектів безпеки, що значно зменшує навантаження на команду IT-безпеки та дозволяє оперативніше реагувати на нові загрози.

На рис. 2 показано річну кількість виявлених фішингових сайтів, бачимо що кількість збільшилась в мільйони разів.

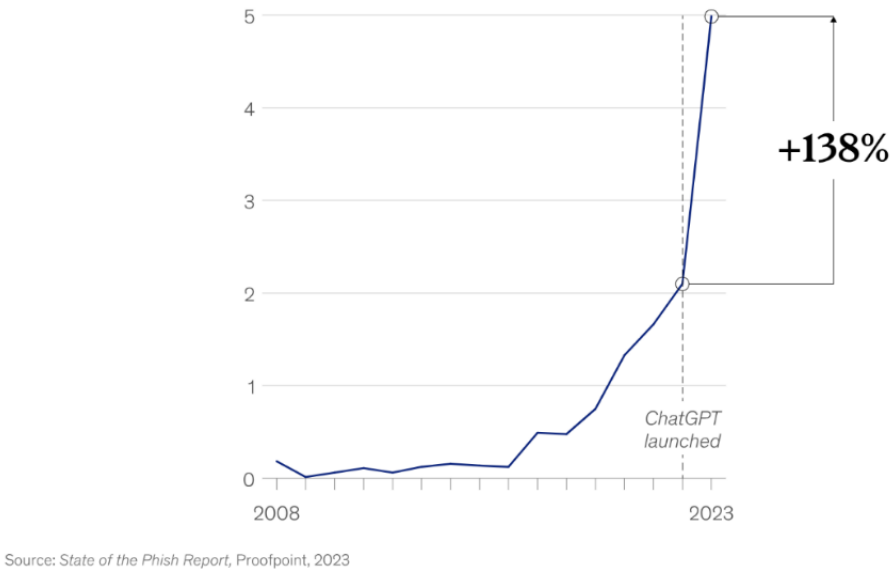

Рис. 2. Річна кількість виявлених фішингових сайтів

Одним з прикладів є використання AI для виявлення аномалій у мережевому трафіку. Такі системи можуть автоматично моніторити великий обсяг даних, виявляючи нетипові патерни поведінки, що можуть свідчити про атаки. Це дозволяє швидко реагувати на нові загрози, навіть ті, що ще не були виявлені. Так компанія IBM Security надає трансформаційні рішення на основі штучного інтелекту, які оптимізують час аналітиків — шляхом прискорення виявлення та пом'якшення загроз штучного інтелекту, прискорення реагування та захисту ідентифікаційних даних користувачів і наборів даних — водночас зберігаючи команди з кібербезпеки в курсі та контролюючих [19].

На рис. 3 показано приклад ШІ моделі для виявлення аномалій у мережевому трафіку.

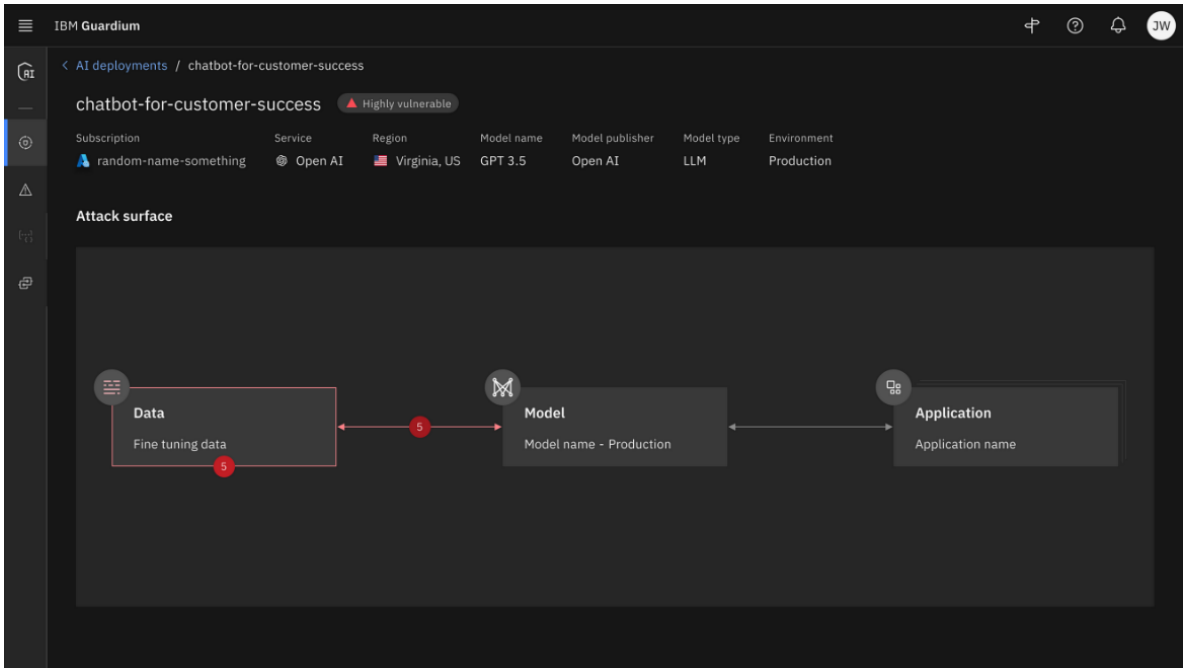

Рис. 3. Приклад ШІ моделі для виявлення аномалій у мережевому трафіку

IBM Security використовує інструменти штучного інтелекту для ідентифікації тіньових даніих, відстежування відхилення в доступі до даних і сповіщення фахівців з кібербезпеки про потенційні загрози з боку зловмисників, які отримують доступ до даних або конфіденційної інформації, заощаджуючи дорогоцінний час на виявлення та усунення проблем у режимі реального часу.

Інший приклад — застосування машинного навчання для боротьби з фішинговими атаками. Алгоритми ML можуть ефективно аналізувати електронні листи, вебсайти та інші комунікації, виявляючи типові ознаки фішингових спроб. Це дозволяє блокувати шахрайські повідомлення ще до того, як вони досягнуть користувачів, підвищуючи рівень захисту корпоративних систем. Наприклад Darktrace використовує технології AI та LLM для розпізнавання та нейтралізації кіберзагроз у реальному часі. Їхні рішення, зокрема, застосовують «автономні» алгоритми для виявлення аномальних патернів поведінки у мережах, що дозволяє оперативно виявляти й зупиняти потенційно шкідливі дії без втручання людини. Це особливо важливо для захисту від нових, раніше невідомих загроз [20].

На рис. 4 показано вбудовану на платформу автономну відповідь, яка нейтралізує зловмисну активність.

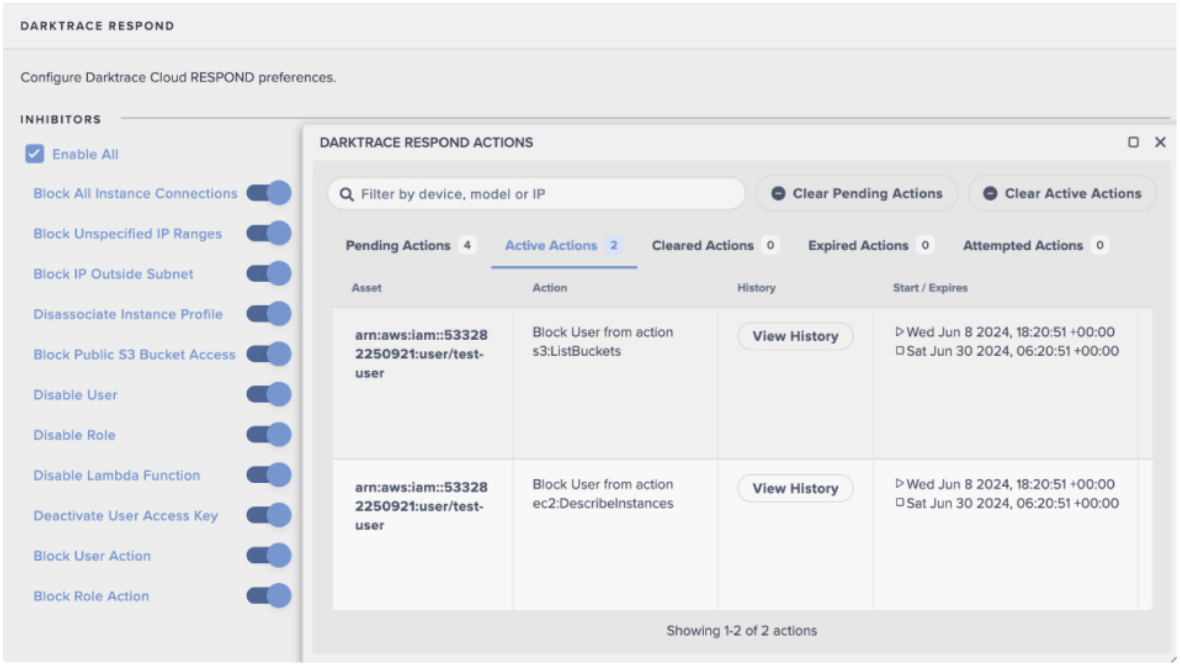

Рис. 4. Вбудована в платформу автономна відповідь, яка нейтралізує зловмисну активність

Технологія блокчейн для управління доступом

Технологія блокчейн має низку унікальних характеристик, що роблять її надзвичайно корисною для підвищення рівня кібербезпеки в корпоративних мережах. Зокрема, децентралізована структура усуває потребу в єдиному центральному органі, що значно знижує ризик виникнення єдиної точки відмови та підвищує довіру між учасниками системи. Незмінність даних гарантує, що записана інформація не може бути змінена або підроблена, що критично важливо для збереження цілісності чутливих даних. Крім того, прозора система розподіленого реєстру забезпечує можливість для всіх учасників переглядати транзакції, що підвищує підзвітність і ускладнює приховування шахрайських дій.

Окремо варто відзначити смарт-контракти — автоматизовані алгоритми, які виконують умови договору без участі посередників. Вони дозволяють спростити бізнес-процеси й одночасно підвищити безпеку, адже умови виконуються точно відповідно до прописаної логіки. Зрештою, застосування блокчейну в різних галузях — від фінансів і медицини до державного управління — вже довело його ефективність у практиці. Ці приклади підтверджують гнучкість і універсальність технології для вирішення сучасних викликів кібербезпеки.

Microsoft в свою чергу надає відкриті масштабовані платформи та послуги будь-якій компанії. Azure Blockchain Service — це повністю керований блокчейн-сервіс, який спрощує формування, управління та управління блокчейн-мережами консорціуму, щоб компанії могли зосередитися на логіці робочого процесу та розробці додатків [21].

ISSN 2663 - 4023

На рис. 5 показано рішення компанії Azure Web3, яке складається з надійного набору продуктів і послуг кіберзахисту.

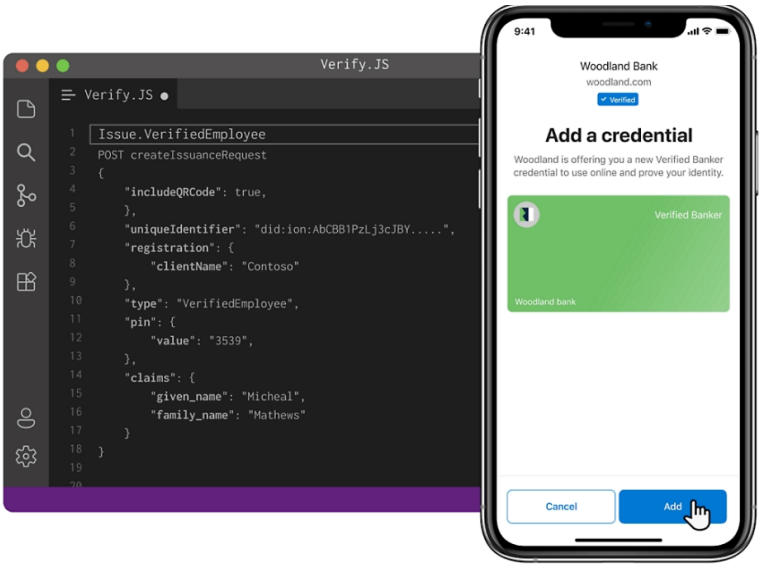

Рис. 5. Рішення компанії Azure Web3, яке складається з надійного набору продуктів і послуг кіберзахисту

Кількома простими клацаннями миші користувачі можуть створити та розгорнути дозволену блокчейн-мережу та керувати політиками консорціуму за допомогою інтуїтивно зрозумілого інтерфейсу на порталі Azure. Вбудоване керування дозволяє розробникам додавати нових учасників, встановлювати дозволи, відстежувати стан мережі та активність, а також виконувати контрольовані приватні взаємодії через інтеграцію з Azure Active Directory.

Контейнерна безпека та ізоляція середовищ

Контейнеризація — це технологія, яка дозволяє упакувати програму разом з усіма її залежностями в ізольоване середовище, що забезпечує стабільну та передбачувану роботу в будь-якому середовищі. Її використання є критично важливим для безпеки та масштабованості хмарних додатків, оскільки вона дозволяє ефективно управляти компонентами системи, мінімізуючи ризики взаємного впливу між ними [26].

На рис. 6 показано контейнери, які спільно використовують системне ядро ОС машини, на відміну від віртуальних машин.

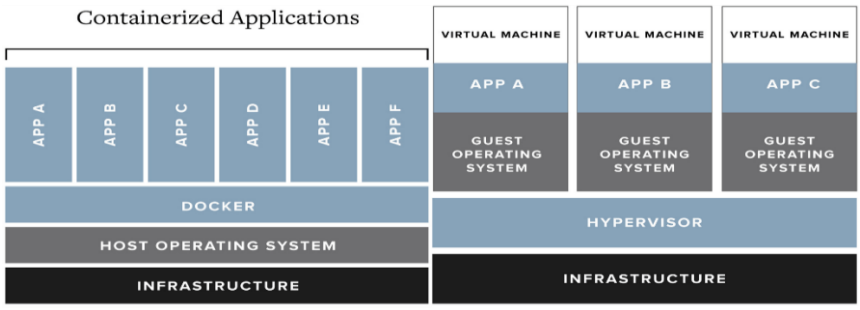

Рис. 6. Таблиця контейнерів, які спільно використовують системне ядро ОС машини, на відміну від віртуальних машин

ISSN 2663 - 4023

Kubernetes, також відомий як K8s, став потужним інструментом для розгортання контейнерних додатків і керування ними, змінюючи те, як організації керують своєю інфраструктурою. Безпека Kubernetes є складною через її розподілену природу та багатокомпонентну архітектуру, яка включає API, рівні керування, бази даних і робочі вузли. Таким чином, належні заходи безпеки відіграють вирішальну роль в управлінні ризиками, пов'язаними з розгортанням Kubernetes [22].

На рис. 7 представлена схема архітектури Kubernetes-кластера, що взаємодіє з хмарним провайдером.

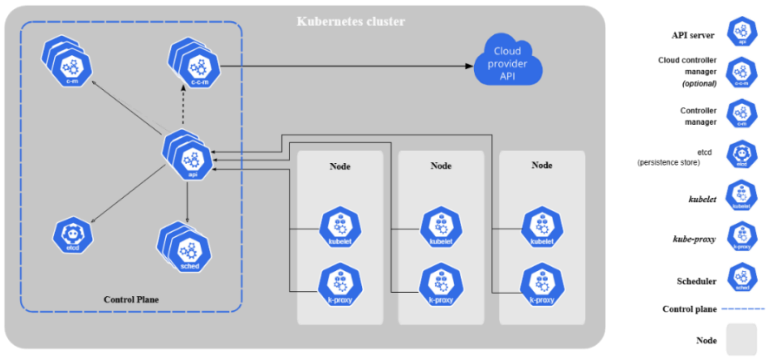

Рис. 7. Схема архітектури Kubernetes-кластера

Ця потужна платформа для оркестрації контейнеризованих додатків забезпечує автоматизацію процесів розгортання, масштабування та управління. Вона підтримує автоматизовані оновлення та відкати, дозволяючи безпечно вносити зміни до конфігурації або програмного забезпечення без зупинки всіх екземплярів одночасно. При виникненні проблем Kubernetes автоматично повертає зміни. Система також забезпечує балансування навантаження та виявлення служб, призначаючи IP-адреси та DNS-імена для подів, полегшуючи мережеву взаємодію. Завдяки підтримці різних типів сховищ (локальних, хмарних чи мережевих), Kubernetes автоматизує монтування ресурсів відповідно до потреб користувача.

Крім того, Kubernetes має потужні можливості самовідновлення: він перезапускає зламані контейнери, перепланує робочі навантаження при збоях вузлів та ізолює нестабільні модулі. Інтеграція з механізмами управління секретами дозволяє оновлювати конфігурації без перебудови контейнерів і без ризику розкриття чутливої інформації. Автоматичне пакування контейнерів оптимізує використання ресурсів, а також підтримується горизонтальне масштабування на основі навантаження. Додатково Kubernetes працює з подвійним стеком IPv4/IPv6, підтримує CI-навантаження та легко розширюється без необхідності зміни базового коду.

Шифрування та політики управління ключами

Шифрування — це процес перетворення даних у зашифрований формат, який не можна прочитати без спеціального ключа. Це один із найважливіших інструментів захисту інформації у цифровому світі. Сучасні методи шифрування дозволяють забезпечити конфіденційність навіть у випадку, якщо дані потрапляють до зловмисника.

Гомоморфне шифрування — це інноваційна технологія, яка дозволяє обчислювати зашифровані дані без їх розшифрування. Це особливо корисно у хмарних середовищах, де обробка чутливих даних може відбуватись на стороні стороннього провайдера без розкриття самих даних [23].

На рис. 8 представлено схему роботи повністю гомоморфного шифрування (Fully Homomorphic Encryption, FHE). Цей метод дозволяє виконувати обчислення над зашифрованими даними без їхнього розшифрування.

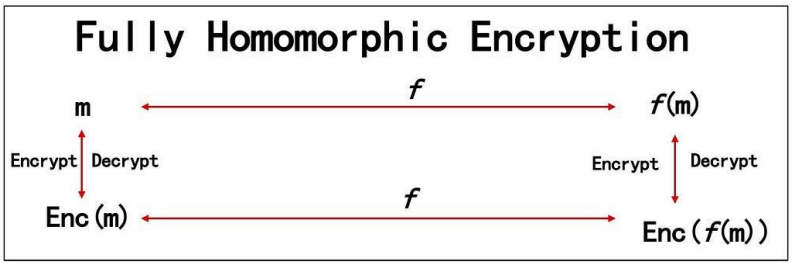

Рис. 8. Схема роботи гомоморфного шифрування

Квантово-стійкі алгоритми шифрування — це нове покоління криптографії, розроблене з урахуванням майбутньої загрози від квантових комп'ютерів, які потенційно зможуть зламувати традиційні методи шифрування.

На рис. 9 представлено рівняння інтеграції QKD (квантового розподілу ключів) у класичні протоколи мережевої безпеки.

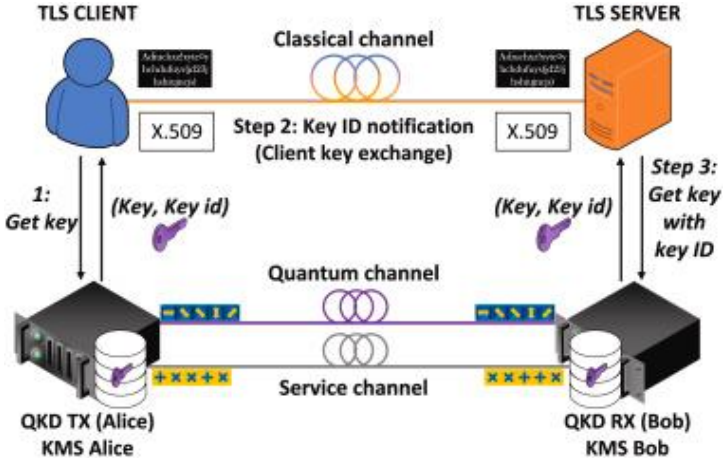

Рис. 9. Рівняння інтеграції QKD (квантового розподілу ключів) у класичні протоколи мережевої безпеки

Безпечне управління ключами шифрування — критично важлива частина кібербезпеки. Якщо ключі скомпрометовано, шифрування втрачає сенс, незалежно від його сили.

Hardware Security Modules (HSM) — це спеціалізовані фізичні пристрої, які використовуються для генерації, зберігання та управління криптографічними ключами в максимально захищеному середовищі. Вони часто використовуються банками, урядами та великими компаніями для захисту найбільш чутливих даних [24].

Отже, у сучасному світі хмарні технології стали основним інструментом для управління корпоративними інформаційними системами, надаючи організаціям гнучкість, масштабованість та економічну ефективність. Проте впровадження таких технологій також створює нові виклики для кібербезпеки, які вимагають розробки інноваційних і ефективних стратегій захисту. Зокрема, використання хмарних обчислень спричиняє нові загрози, пов'язані з можливістю витоків даних, несанкціонованим

доступом і атаками на мережеві структури, що підвищує ризики для цілісності та конфіденційності корпоративної інформації.

Інноваційні підходи, такі як Zero Trust Architecture, є важливими складовими захисту хмарних мереж. Згідно з цією архітектурою, доступ до ресурсів дозволяється лише за умови постійної перевірки кожного користувача та пристрою, що забезпечує більш високий рівень безпеки. Використання штучного інтелекту (AI) та машинного навчання (ML) дозволяє автоматично виявляти загрози, що виникають у реальному часі, та адаптувати захист до нових кіберзагроз. Крім того, технології блокчейн забезпечують високу надійність та прозорість обробки даних, а також покращують механізми аутентифікації та управління доступом [25].

Контейнеризація та відповідні технології, як-от Kubernetes, також є важливими для забезпечення безпеки в хмарному середовищі, адже вони дозволяють ізолювати робочі навантаження та зменшувати потенційний вплив атак на всю систему. Інтеграція методів шифрування та політик управління ключами, а також впровадження квантово-стійких алгоритмів для захисту даних дозволяє захистити конфіденційну інформацію навіть в умовах майбутніх кіберзагроз, зокрема в контексті розвитку квантових технологій.

Таким чином, для забезпечення належного рівня кібербезпеки в корпоративних мережах необхідно використовувати комплексний підхід, що поєднує сучасні методи захисту, такі як штучний інтелект, блокчейн, Zero Trust Architecture та інші інноваційні моделі. Лише через інтеграцію цих технологій можна забезпечити високий рівень захисту в умовах постійно зростаючих кіберзагроз та складних вимог до безпеки в хмарних середовищах. Порівняння підходів до забезпечення безпеки представлено в таблиці №1.

Таблиця 1

Порівняння підходів до забезпечення безпеки

Підхід	Опис	Переваги	Обмеження
Zero Trust Architecture	Модель безпеки, яка вимагає перевірки всіх користувачів і пристроїв незалежно від їхнього розташування	Знижує ризики несанкціонованого доступу	Висока складність впровадження
AI-підходи до виявлення загроз	Використання штучного інтелекту та машинного навчання для автоматичного аналізу даних і виявлення потенційних загроз.	Можливість виявлення нових типів атак	Імовірність хибних спрацювань
Використання блокчейну	Децентралізоване зберігання даних з використанням технології блокчейн для забезпечення їх цілісності та незмінності.	Висока стійкість до спроб модифікації даних	Значні вимоги до обчислозчильних потужностей
Контейнерна безпека	Заходи щодо захисту контейнеризованих додатків	Ефективність для середовищ мікросервісів	Необхідність постійного оновлення
Шифрування	Перетворення даних у зашифрований формат для захисту конфіденційності під час передачі або зберігання.	Захист від несанкціонованого доступу.	Складність управління ключами шифрування.

ВИСНОВКИ

Таким чином, для забезпечення належного рівня кібербезпеки в корпоративних мережах необхідно використовувати комплексний підхід, що поєднує сучасні методи захисту, такі як штучний інтелект, блокчейн, Zero Trust Architecture та інші інноваційні

моделі. Важливо також відзначити, що адаптація до нових технологій потребує постійного моніторингу та вдосконалення захисних механізмів, оскільки кіберзагрози постійно еволюціонують. Зважаючи на швидкий розвиток квантових обчислень та новітніх загроз, підприємства повинні бути готові до інтеграції квантово-стійких криптографічних алгоритмів та інших передових інструментів захисту, щоб не лише реагувати на виклики сьогодення, а й бути готовими до майбутніх загроз. Лише через інтеграцію цих технологій можна забезпечити високий рівень захисту в умовах постійно зростаючих кіберзагроз та складних вимог до безпеки в хмарних середовищах.

Було дослідження сучасні методи і моделі підвищення рівня кібербезпеки корпоративних мереж при використанні хмарних технологій, що дало визначити ознаки якими вони характеризуються для використання при розробці відповідних моделей і методів із усуненням їх недоліків.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Zhurakovskyi, B., Averichev, I., & Shakhmatov, I. (2023, November 21). Using the latest methods of cluster analysis to identify similar profiles in leading social networks. *Information Technology and Implementation (Satellite) Conference Proceedings*. https://ceur-ws.org/Vol-3646/Paper_12.pdf
2. Ponochovny, P. (2024). Low-speed HTTP DDoS attack prevention model for end users. *Cybersecurity: Education, Science, Technique, 2*(26), 291–304. https://doi.org/10.28925/2663-4023.2024.26.695
3. Hasan, M. (2024). Enhancing enterprise security with Zero Trust architecture. *arXiv Preprint, arXiv:2410.18291*. https://arxiv.org/abs/2410.18291
4. Ahmed, S., Shihab, I. F., & Khokhar, A. (2025). Quantum-driven Zero Trust framework with dynamic anomaly detection in 7G technology: A neural network approach. *arXiv Preprint, arXiv:2502.07779*. https://arxiv.org/abs/2502.07779
5. Ghasemshirazi, S., Shirvani, G., & Alipour, M. A. (2023). Zero Trust: Applications, challenges, and opportunities. *arXiv Preprint, arXiv:2309.03582*. https://arxiv.org/abs/2309.03582
6. Rahmati, M. (2025). Federated learning-driven cybersecurity framework for IoT networks with privacy-preserving and real-time threat detection capabilities. *arXiv Preprint, arXiv:2502.10599*. https://arxiv.org/abs/2502.10599
7. Cloud Security Alliance. (2025). *Top threats to cloud computing 2025*. https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-2025
8. Softprom. (2025). *The future of cloud security: 7 key trends in 2025*. https://softprom.com/the-future-of-cloud-security-7-key-trends-in-2025
9. Check Point Software Technologies Ltd. (2025). *Top cloud security trends in 2025*. https://www.checkpoint.com/cyber-hub/cloud-security/what-is-code-security/top-cloud-security-trends-in-2025/
10. MarketsandMarkets. (2024). *The evolving synergy of cybersecurity and cloud computing: Trends, opportunities, and challenges*. https://www.marketsandmarkets.com/blog/ICT/The-Evolving-Synergy-Of-Cybersecurity-And-Cloud-Computing
11. Xsoft-Tech. (2025). *Cloud security trends for 2025: Advanced strategies & solutions*. https://xsoft-tech.com/blog/top-cloud-security-strategies-solutions
12. IT Strategy News. (2025). *New cybersecurity technologies in 2025: Innovations, trends, and insights*. https://itstrategynews.com/new-cybersecurity-technologies-in-2025-innovations-trends-and-insights/
13. National Cybersecurity Center of Excellence (NCCoE). (n.d.). *Implementing a Zero Trust architecture*. https://www.nccoe.nist.gov/projects/implementing-zero-trust-architecture
14. CrowdStrike. (2025). *What is Zero Trust? – Guide to Zero Trust security*. https://www.crowdstrike.com/en-us/cybersecurity-101/zero-trust-security/
15. General Services Administration (GSA). (2025). *Zero Trust architecture*. https://www.gsa.gov/technology/it-contract-vehicles-and-purchasing-programs/it-security/zero-trust-architecture
16. Check Point Software Technologies Ltd. (2024). *Top 6 cloud security trends in 2024*. https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/top-6-cloud-security-trends-in-2024/

17. Thales Group. (2024). *2024 cloud security study – Global edition*. https://cpl.thalesgroup.com/cloud-security-research
18. Palo Alto Networks. (2024). *2024 state of cloud native security report*. https://www.paloaltonetworks.com/resources/research/state-of-cloud-native-security-2024
19. Fortinet. (2024). *Key findings from the 2024 cloud security report*. https://www.fortinet.com/blog/industry-trends/key-findings-cloud-security-report-2024
20. Morgan Stanley. (2024). *AI and cybersecurity: A new era*. https://www.morganstanley.com/articles/ai-cybersecurity-new-era
21. Darktrace. (2024). *Why artificial intelligence is the future of cybersecurity*. https://darktrace.com/blog/why-artificial-intelligence-is-the-future-of-cybersecurity
22. Statista. (2023). *Main benefits of incorporating AI into cybersecurity operations 2023*. https://www.statista.com/statistics/1425575/top-benefits-of-incorporating-ai-into-cybersecurity-operations/
23. McKinsey & Company. (2024). *The cybersecurity provider's next opportunity: Making AI safer*. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-cybersecurity-providers-next-opportunity-making-ai-safer
24. Practical DevSecOps. (2023). *Top 15 DevSecOps best practices for 2025*. https://www.practical-devsecops.com/devsecops-best-practices/
25. MITRE SAF. (2023). *DevSecOps best practices guide*. https://saf.mitre.org/DevSecOps_Best_Practices_Guide.pdf
26. Ivanchenko, Y., Shulha, V., Averichev, I., & Dubrovskyi, V. (2025). Класифікація та вплив кібератак, спрямованих на критично важливих постачальників послуг [Classification and impact of cyberattacks targeting critical service providers]. *Information Technology: Computer Science, Software Engineering and Cyber Security, 2*, 14–22. https://doi.org/10.32782/IT/2025-2-3

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023

Ihor Averichev
Candidate of economic sciences, associate professor of the Department of Technical Cyber Defense Systems
ORCID ID: 0009-0008-9766-0115
iaverichev19@gmail.com

Artem Rozhenko
Postgraduate student of the State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID ID: 0009-0000-2900-349X
a.rozhenko@stud.duikt.edu.ua

Yevhen Kykhtenko
Postgraduate student of the State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID ID: 0009-0008-1696-1048
firementer@gmail.com

INNOVATIVE APPROACHES TO IMPROVING THE LEVEL OF CYBERSECURITY OF CORPORATE NETWORKS USING CLOUD TECHNOLOGIES

Abstract. Modern methods and approaches to enhancing the level of cybersecurity in corporate networks in the context of cloud technology usage have been examined. The threats associated with cloud computing are analyzed, and effective innovative protection models are proposed, including Zero Trust Architecture, AI-based threat detection approaches, blockchain integration, container security, and encryption with key management policies. These ensure a multi-layered and adaptive security system capable of promptly responding to evolving threat types and minimizing potential risks of data leakage or compromise. The application of these approaches enables the creation of a resilient environment in which corporate information remains protected even under increasing complexity and intensity of cyberattacks. Emphasis is also placed on the importance of an integrated security approach that combines technical, organizational, and administrative measures. In today's environment of rapid IT development and growing business dependence on cloud infrastructure, it is crucial not only to implement innovative protection tools but also to ensure their integration into a unified security management system. This system should cover all levels of the corporate network—from edge devices to cloud platforms—including access policies, encryption, authentication, user behavior monitoring, and real-time incident analytics. The comprehensiveness and coherence of such solutions not only increase the level of technical protection but also promote the development of a cybersecurity culture within the organization, where every element of the infrastructure is viewed both as a potential target and as an active participant in the defensive perimeter. The following sections will examine the main threats inherent in cloud environments and provide a detailed analysis of innovative approaches to their detection and mitigation.

Keywords: cybersecurity; corporate networks; cloud technologies; Zero Trust; artificial intelligence; DevSecOps; cloud security; cyber threats; data protection; multi-factor authentication.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Zhurakovskyi, B., Averichev, I., & Shakhmatov, I. (2023, November 21). Using the latest methods of cluster analysis to identify similar profiles in leading social networks. *Information Technology and Implementation (Satellite) Conference Proceedings*. https://ceur-ws.org/Vol-3646/Paper_12.pdf
2. Ponochovny, P. (2024). Low-speed HTTP DDoS attack prevention model for end users. *Cybersecurity: Education, Science, Technique, 2*(26), 291–304. https://doi.org/10.28925/2663-4023.2024.26.695
3. Hasan, M. (2024). Enhancing enterprise security with Zero Trust architecture. *arXiv Preprint, arXiv:2410.18291*. https://arxiv.org/abs/2410.18291

4. Ahmed, S., Shihab, I. F., & Khokhar, A. (2025). Quantum-driven Zero Trust framework with dynamic anomaly detection in 7G technology: A neural network approach. *arXiv Preprint, arXiv:2502.07779*. https://arxiv.org/abs/2502.07779
5. Ghasemshirazi, S., Shirvani, G., & Alipour, M. A. (2023). Zero Trust: Applications, challenges, and opportunities. *arXiv Preprint, arXiv:2309.03582*. https://arxiv.org/abs/2309.03582
6. Rahmati, M. (2025). Federated learning-driven cybersecurity framework for IoT networks with privacy-preserving and real-time threat detection capabilities. *arXiv Preprint, arXiv:2502.10599*. https://arxiv.org/abs/2502.10599
7. Cloud Security Alliance. (2025). *Top threats to cloud computing 2025*. https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-2025
8. Softprom. (2025). *The future of cloud security: 7 key trends in 2025*. https://softprom.com/the-future-of-cloud-security-7-key-trends-in-2025
9. Check Point Software Technologies Ltd. (2025). *Top cloud security trends in 2025*. https://www.checkpoint.com/cyber-hub/cloud-security/what-is-code-security/top-cloud-security-trends-in-2025/
10. MarketsandMarkets. (2024). *The evolving synergy of cybersecurity and cloud computing: Trends, opportunities, and challenges*. https://www.marketsandmarkets.com/blog/ICT/The-Evolving-Synergy-Of-Cybersecurity-And-Cloud-Computing
11. Xsoft-Tech. (2025). *Cloud security trends for 2025: Advanced strategies & solutions*. https://xsoft-tech.com/blog/top-cloud-security-strategies-solutions
12. IT Strategy News. (2025). *New cybersecurity technologies in 2025: Innovations, trends, and insights*. https://itstrategynews.com/new-cybersecurity-technologies-in-2025-innovations-trends-and-insights/
13. National Cybersecurity Center of Excellence (NCCoE). (n.d.). *Implementing a Zero Trust architecture*. https://www.nccoe.nist.gov/projects/implementing-zero-trust-architecture
14. CrowdStrike. (2025). *What is Zero Trust? – Guide to Zero Trust security*. https://www.crowdstrike.com/en-us/cybersecurity-101/zero-trust-security/
15. General Services Administration (GSA). (2025). *Zero Trust architecture*. https://www.gsa.gov/technology/it-contract-vehicles-and-purchasing-programs/it-security/zero-trust-architecture
16. Check Point Software Technologies Ltd. (2024). *Top 6 cloud security trends in 2024*. https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/top-6-cloud-security-trends-in-2024/
17. Thales Group. (2024). *2024 cloud security study – Global edition*. https://cpl.thalesgroup.com/cloud-security-research
18. Palo Alto Networks. (2024). *2024 state of cloud native security report*. https://www.paloaltonetworks.com/resources/research/state-of-cloud-native-security-2024
19. Fortinet. (2024). *Key findings from the 2024 cloud security report*. https://www.fortinet.com/blog/industry-trends/key-findings-cloud-security-report-2024
20. Morgan Stanley. (2024). *AI and cybersecurity: A new era*. https://www.morganstanley.com/articles/ai-cybersecurity-new-era
21. Darktrace. (2024). *Why artificial intelligence is the future of cybersecurity*. https://darktrace.com/blog/why-artificial-intelligence-is-the-future-of-cybersecurity
22. Statista. (2023). *Main benefits of incorporating AI into cybersecurity operations 2023*. https://www.statista.com/statistics/1425575/top-benefits-of-incorporating-ai-into-cybersecurity-operations/
23. McKinsey & Company. (2024). *The cybersecurity provider's next opportunity: Making AI safer*. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-cybersecurity-providers-next-opportunity-making-ai-safer
24. Practical DevSecOps. (2023). *Top 15 DevSecOps best practices for 2025*. https://www.practical-devsecops.com/devsecops-best-practices/
25. MITRE SAF. (2023). *DevSecOps best practices guide*. https://saf.mitre.org/DevSecOps_Best_Practices_Guide.pdf
26. Ivanchenko, Y., Shulha, V., Averichev, I., & Dubrovskyi, V. (2025). Класифікація та вплив кібератак, спрямованих на критично важливих постачальників послуг [Classification and impact of cyberattacks targeting critical service providers]. *Information Technology: Computer Science, Software Engineering and Cyber Security, 2*, 14–22. https://doi.org/10.32782/IT/2025-2-3