ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

ВСЕУКРАЇНСЬКА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

«АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ»

Тези доповідей

29 жовтня
2025

м. Київ

Рекомендовано до друку кафедрою Сиситем та технологій Державного університету інформаційно-комунікаційних технологійй (протокол № 4 від 04.11.2025 р.)

Актуальні проблеми кібербезпеки: Матеріали Всеукраїнської науково-практичної конференції (м. Київ, 29 жовтня 2025 року). Навчально-науковий інститут кібербезпеки та захисту інформації, Державний університет інформаційно-комунікаційних технологій. Київ, 2025. 269 с. Збірник призначений для науковців, викладачів, докторантів, аспірантів і студентів закладів вищої освіти, фахівців з кібербезпеки та захисту інформації, працівників органів державної влади та місцевого самоврядування. Редакційна колегія не несе відповідальності за зміст матеріалів, що опубліковані у збірнику. Тези подані в авторській редакції та відображають персональну позицію учасників конференції.

ЗМІСТ

Клименко Ярослав Валерійович
студент групи БСДМ-63, ННІЗІ ДУІКТ, Київ, Україна

ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ГІБРИДНОГО РОБОЧОГО СЕРЕДОВИЩА ЗА ДОПОМОГОЮ СИСТЕМ SIEM

*Зі стрімким поширенням моделі **гібридної роботи**, яка поєднує віддалену діяльність співробітників із фізичною присутністю в офісі, питання кібербезпеки набуло нової актуальності. Розподілена IT-інфраструктура, численні точки доступу, робота з корпоративними системами з персональних пристроїв — усе це значно ускладнює процес захисту даних, мереж та систем. В умовах, коли класичні засоби безпеки втрачають ефективність, все більше організацій впроваджують **системи управління інформацією та подіями безпеки (SIEM)** як основу для побудови адаптивної моделі захисту.*

SIEM-системи дозволяють централізовано обробляти великі обсяги журналів подій (logs) з різних джерел — від endpoint-пристроїв до хмарних платформ, VPN-шлюзів і мобільних пристроїв. У контексті **гібридної моделі роботи** це критично важливо, адже поведінка працівників може значно варіюватися залежно від місця та способу підключення. Використовуючи можливості Splunk щодо виявлення аномалій, організації можуть ідентифікувати нетипову активність, наприклад: підключення з незвичних геолокацій, спроби доступу до конфіденційної інформації в нестандартний час, чи багаторазові невдалі спроби входу до систем. Ключовою перевагою SIEM-рішень є **автоматизація виявлення та реагування на інциденти безпеки (SOAR)**. Splunk пропонує інтеграцію з різноманітними джерелами загроз (threat intelligence feeds), що дозволяє не лише виявляти потенційні атаки, але й автоматично блокувати підозрілий трафік, змінювати політики доступу або сповіщати відповідальних фахівців. У гібридному середовищі, де час реакції має критичне значення, така автоматизація значно підвищує стійкість організації до атак. Особливо важливим є **захист персональних пристроїв співробітників (BYOD — Bring Your Own Device)**, які часто є вектором атак через відсутність централізованого контролю. Splunk дозволяє інтегрувати дані з агентів, встановлених на кінцевих пристроях, для постійного моніторингу процесів, запуску програм, підключень до зовнішніх серверів тощо. Таким чином формується **єдина картина безпеки** для кожного користувача, незалежно від того, де він фізично знаходиться. Незважаючи на переваги, впровадження SIEM у гібридному середовищі має свої виклики.

Рис.1 — Архітектура SIEM-рішення

По-перше, це **високі вимоги до обчислювальних ресурсів** — обробка великих обсягів логів вимагає масштабованої інфраструктури, особливо при використанні модулів машинного навчання. По-друге, **необхідність налаштування кореляційних правил і сценаріїв реагування** вимагає високої кваліфікації аналітиків безпеки. По-третє, організаціям необхідно забезпечити відповідність вимогам щодо **захисту персональних даних** при зборі інформації з пристроїв працівників. У підсумку, використання систем SIEM є одним із найефективніших підходів до забезпечення **комплексного захисту гібридної IT-інфраструктури**. Завдяки централізованому моніторингу, аналітиці поведінки користувачів, автоматичному реагуванню на загрози та інтеграції з іншими системами безпеки, SIEM дозволяє організаціям ефективно управляти кіберризиками у нових умовах цифрової трансформації. Подальші дослідження в цій сфері сприятимуть розвитку інтелектуальних засобів обробки подій, вдосконаленню механізмів захисту особистих даних та впровадженню адаптивних політик безпеки для динамічного середовища роботи.

Перелік посилань:

1. Splunk Inc. "The Essential Guide to Security", 2023. [splunk.com]
2. Kavanagh K., Bussa T. "Market Guide for Security Information and Event Management (SIEM)" // Gartner, 2022.
3. Задорожний І. "SIEM-системи в умовах гібридної роботи: аналітика та автоматизація безпеки" // Інформаційні технології, 2024.
4. Коваль В., Тимчук О. "Забезпечення кіберзахисту в умовах дистанційної праці" // Журнал кібербезпеки та захисту інформації, 2023.

Бригинець Анастасія Адріївна
студентка групи БСДМ-61, ННІКБЗІ,
Київ,Україна

ГРАФОВІ НЕЙРОННІ МЕРЕЖІ ЯК ОСНОВА ДЛЯ ВИЯВЛЕННЯ ШКІДЛИВОГО ПЗ У ДОКУМЕНТАХ PDF ТА OFFICE

Сучасні тенденції розвитку кіберзагроз демонструють зростання кількості атак, спрямованих на документи офісних форматів. Це пояснюється їхньою повсюдною поширеністю та довірою користувачів до такого контенту. Проблема ускладнюється тим, що файли PDF та Office є багаторівневими структурами, які можуть приховувати шкідливі об'єкти у вигляді скриптів, макросів чи вкладених ресурсів. Тому ефективний захист потребує методів, здатних аналізувати взаємозв'язки між різнорідними компонентами документа, а не лише їхні окремі характеристики.

Графові нейронні мережі відкривають нові можливості у виявленні аномалій, адже вони дозволяють працювати безпосередньо з графовими моделями даних. Такий підхід забезпечує гнучкість і адаптивність, що є критично важливим для протидії новим типам загроз. Використання GCN для документів PDF/Office формує основу для створення практичних систем, які можуть інтегруватися у процеси аналізу інцидентів та підсилювати стратегії кіберзахисту організацій.

Ключові слова: графові нейронні мережі, шкідливе програмне забезпечення, PDF, Office.

Кібератаки все частіше використовують документи Office та PDF як носії шкідливого коду, особливо в фішингових розсилках та APT-атаках. За даними досліджень, понад 91% цілеспрямованих атак (APT) починаються із фішингового електронного листа з шкідливим вкладенням, причому понад 65% таких вкладень становлять документи Microsoft Office. PDF-файли так само широко застосовуються зловмисниками, оскільки виглядають як безпечні ділові документи і можуть містити вбудовані сценарії (JavaScript) та експлойти. Відкриваючи такий файл, користувач несвідомо активує шкідливий код. Зважаючи на масштаби загрози, проблема виявлення шкідливого програмного забезпечення (ПЗ) у форматах PDF/Office є надзвичайно актуальною.

Традиційні методи захисту, як-то антивірусні сигнатури та евристики, часто не встигають за новими зразками шкідливого ПЗ і можуть бути легко обійдені обфускацією. З іншого боку, динамічний аналіз (запуск документів у ізольованому середовищі) здатний виявляти приховану шкідливу активність, але потребує значних ресурсів і часу. До того ж, багато існуючих рішень сфокусовано або на статичних ознаках документа, або на спостереженні окремих сценаріїв (наприклад, виконання JavaScript у PDF). Такий підхід має обмеження: статичні сканери вразливі до приховання коду, а динамічні – можуть не помітити «приховану» шкідливість, що проявляється неявно чи при нестандартних умовах.

За останнє десятиліття успішно застосовуються методи машинного навчання для виявлення шкідливого ПЗ, які навчаються на ознаках файлів і адаптуються до нових атак. Серед них особливий інтерес становлять графові нейронні мережі (Graph Neural Networks, GNN) – глибокі моделі, що працюють з даними у вигляді графів. На відміну від традиційних підходів, GNN здатні враховувати зв'язки між об'єктами та складну структуру даних, що дозволяє виявляти приховані патерни шкідливості (рис. 1).

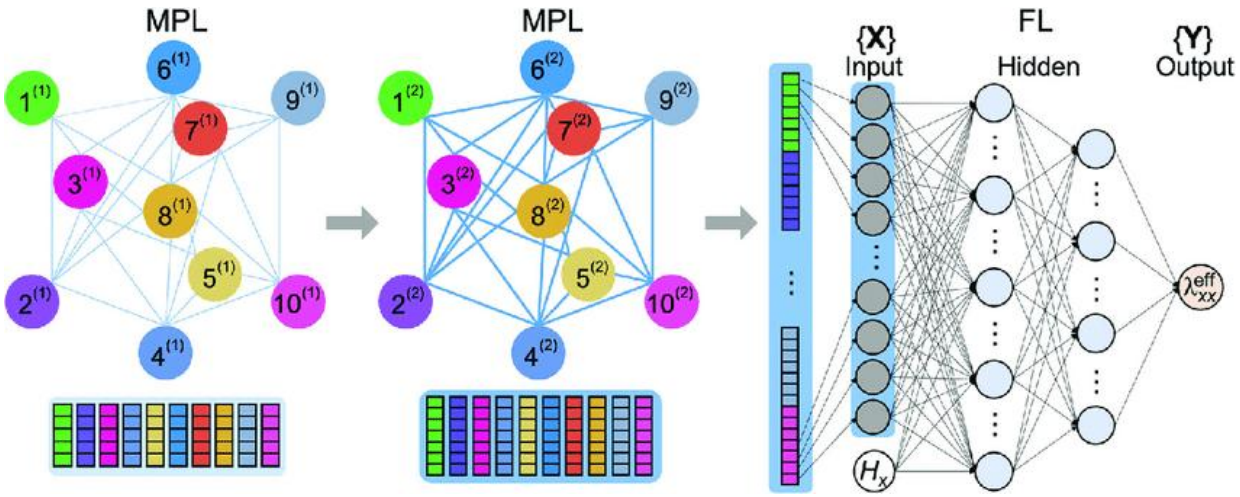

Рис. 1. Мережева архітектура GNN [5]

Графові нейронні мережі успішно застосовуються для класифікації програмного коду та мережевого трафіку, показуючи високу ефективність у виявленні шкідливих зразків. Ідея полягає в тому, щоб подати структуру документа у вигляді графа, вершини якого відповідають елементам або подіям, а ребра – їхнім взаємозв'язкам. Для складних форматів файлів, таких як PDF і Office, такий підхід є природним: документ містить багато взаємопов'язаних компонентів (об'єкти, потоки, макроси, вбудовані файли), що формують граф структури. Наприклад, PDF-документ можна подати як граф об'єктів (структурні об'єкти PDF, посилання між ними, виконувані скрипти), а файл MS Office у форматі OOXML – як граф вкладених XML-вузлів і взаємних посилань.

На такому графі Graph Convolutional Network (GCN) виконує згорткове перетворення: кожен шар мережі агрегує ознаки вузлів з їхніх сусідів, виділяючи все більш високорівневі патерни. Після кількох шарів GCN одержує інтегральне представлення всього графа, яке далі подається на класифікатор. Завдяки цьому модель здатна виявляти комплексні ознаки шкідливості, що охоплюють взаємозв'язки між компонентами документа (наприклад, макрос, який створює файл і запускає зовнішній процес, або PDF-об'єкт, що містить зашифрований скрипт). Дослідження показують, що збільшення глибини GCN (кількості шарів) підвищує якість виявлення складних шкідливих документів, поки не досягне насичення на певній глибині (близько 5 шарів) [2].

Практичне застосування GNN у кібербезпеці демонструє високу результативність. Зокрема, у [3] було запропоновано систему GLDOC для виявлення приховано шкідливих документів MS Office на основі двоканальної GCN-моделі. У цьому підході документ виконується у sandbox-середовищі, фіксується граф системних викликів MS Word та граф процесів, після чого дві GCN (по одному на кожен граф) генерують ознаки, що об'єднуються для остаточної класифікації. Модель GLDOC досягла точності ~95% при низькому рівні хибних спрацьовувань, перевершивши традиційні методи. Важливо, що такий підхід здатен виявляти невідомі раніше загрози (нульові дні), оскільки модель навчена розпізнавати не конкретні сигнатури, а загальні аномальні взаємозв'язки в поведінці документа [4].

Інший напрям – статичний аналіз структури файлів – також виграє від

представленння у вигляді графів. Раніше для Office-документів пропонувалося видобувати ознаки із внутрішнього XML (кількість вкладених елементів, наявність OLE-об’єктів, макросів тощо) і будувати модель на їх основі. Зокрема, у рамках *ALDOCX* [1] реалізовано активне навчання для поступового вдосконалення класифікатора, що аналізує структурні ознаки docx-файлів. Використання ж графових нейромереж дозволяє піти далі: не вручну інженерити ознаки, а навчити модель автоматично «витягувати» їх із графа. Таким чином, GNN-підхід є гнучкішим і масштабується на різні формати документів.

Запропонований підхід має значні переваги у виявленні нових та модифікованих загроз, оскільки модель навчена узагальнювати поведінкові патерни, а не окремі сигнатури. У той же час він потребує підтримки актуальності: зі виникненням нових технік атак може знадобитися донавчання моделі на оновлених даних. Перспективним напрямом розвитку є об’єднання статичного та динамічного графового аналізу – наприклад, врахування одночасно і структури документа, і поведінки під час відкриття.

Також заслуговує уваги застосування методів інтерпретації GNN-моделей, аби автоматично виділяти підграфи, що відповідають за класифікацію як шкідливу (це ще більше підвищить довіру до системи та зрозумілість її рішень). Загалом, графові нейронні мережі вже зараз виступають потужним інструментом кібербезпеки, що дозволяє підняти рівень захисту від прихованих загроз у повсякденних на вигляд документах.

Перелік посилань:

1. Nissim N., Cohen A., Elovici Y. ALDOCX: Detection of Unknown Malicious Microsoft Office Documents Using Designated Active Learning Methods Based on New Structural Feature Extraction Methodology // IEEE Transactions on Information Forensics and Security. – 2017. – Vol. 12, No. 3. – P. 631–646.
2. Li S., Zhou Q., Zhou R., Lv Q. Intelligent malware detection based on graph convolutional network // The Journal of Supercomputing. – 2022. – Vol. 78, No. 3. – P. 4182–4198.
3. Wang W., Yi P., Kou T., Han W., Wang C. GLDOC: detection of implicitly malicious MS-Office documents using graph convolutional networks // Cybersecurity. – 2024. – Vol. 7, Article No. 48. – Режим доступу: https://doi.org/10.1186/s42400-024-00243-7 (дата звернення: 13.09.2025).
4. Bilot T., El Madhoun N., Al Agha K., Zouaoui A. A Survey on Malware Detection with Graph Representation Learning // ACM Computing Surveys. – 2024. – Vol. 56, No. 11. – P. 1–36.
5. Network architecture of the GNN model [Електронний ресурс] // ResearchGate. – Режим доступу: https://www.researchgate.net/figure/Network-architecture-of-the-GNN-model-A-series-of-message-passing-layers-MPLs-are_fig2_353136116 (дата звернення: 13.09.2025).

Бражник Артем Михайлович
студент групи БСДМ-52, ННІКБЗІ ДУІКТ,
Київ, Україна

ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ТА УПРАВЛІННЯ ДОСТУПОМ У ХМАРНИХ СЕРВІСАХ: СПІЛЬНА ВІДПОВІДАЛЬНІСТЬ І ZERO TRUST ЯК ПРАКТИЧНІ РІШЕННЯ

У статті розглянуто актуальні проблеми забезпечення конфіденційності та управління доступом у хмарних сервісах. Проаналізовано основні ризики, такі як несанкціонований доступ, помилки конфігурації та вразливості сторонніх сервісів. Запропоновано використання моделі спільної відповідальності між провайдером і клієнтом та впровадження архітектури Zero Trust як ефективних підходів до захисту. Визначено ключові заходи безпеки: багатофакторна автентифікація, сегментація мережі, шифрування даних та моніторинг. Доведено, що поєднання цих підходів дозволяє створити гнучку й надійну систему захисту.

Ключові слова: хмарна безпека, Zero Trust, спільна відповідальність, управління доступом.

Хмарні технології сьогодні є основою цифрової інфраструктури більшості організацій. Вони дозволяють масштабувати сервіси, зберігати великі обсяги даних та забезпечують віддалений доступ. Проте такі переваги одночасно відкривають нові вектори атак. Основними ризиками є несанкціонований доступ, людський фактор, помилки конфігурацій та вразливості сторонніх сервісів [1].

Для ефективного захисту хмарних середовищ застосовується модель спільної відповідальності, яка чітко визначає зони безпеки провайдера та користувача. Провайдер відповідає за фізичну безпеку інфраструктури, мережеві контролі та базові сервіси, тоді як користувач зобов’язаний правильно налаштовувати політики доступу, шифрування, автентифікацію та керування даними [2].

Важливим компонентом є впровадження Zero Trust-архітектури — підходу, що базується на принципі «нікому не довіряй, завжди перевіряй». Кожен запит до системи перевіряється незалежно від місцезнаходження користувача або пристрою. Це знижує ризик компрометації облікових даних та забезпечує багаторівневий контроль доступу [3].

Рис.1 - Ключові компоненти архітектури Zero Trust

До ключових заходів захисту належать:
– багатофакторна автентифікація (MFA);
– сегментація мережі та контроль доступу (IAM);
– шифрування даних у стані спокою та передачі;
– постійний моніторинг конфігурацій (CSPM) та журналів безпеки (SIEM);
– резервне копіювання та план відновлення після інцидентів.

Поєднання моделі спільної відповідальності та Zero Trust дає змогу створити гнучку й надійну систему захисту, де безпека не залежить від одного елемента, а забезпечується комплексом взаємодіючих механізмів [4].

Перелік посилань:

1. Cloud Security Alliance. Security Guidance for Critical Areas of Focus in Cloud Computing v4.0. URL: https://cloudsecurityalliance.org (дата звернення: 08.10.2025).
2. Microsoft Learn. Shared responsibility in the cloud. URL: https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibily (дата звернення: 08.10.2025).
3. NIST. Zero Trust Architecture. SP 800-207. URL: https://csrc.nist.gov/publications/detail/sp/800-207/final (дата звернення: 08.10.2025).
4. IBM Security. Cost of a Data Breach Report 2024. URL: https://www.ibm.com/security/data-breach (дата звернення: 08.10.2025).

Рейнська В.Б.,
к.е.н., доц. НУВГП,
Рівне, Україна
Жулавнік А.С.
Студентка групи КІ-41, ННІКІТІ НУВГП,
Рівне, Україна

СУЧАСНІ ТЕХНІЧНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНОМУ БІЗНЕСІ

У сучасному цифровому середовищі інформація є стратегічним активом кожного підприємства, а її захист - ключовим чинником стабільності бізнесу. Активне впровадження інноваційних технологій і зростання кіберзагроз вимагають створення надійних технічних систем безпеки, які поєднують апаратні, програмні та організаційні рішення. В Україні питання кіберзахисту набуває особливого значення через воєнні дії та зростання кількості кібератак на державні й комерційні ресурси. Ефективна система захисту інформації є запорукою довіри, конкурентоспроможності та стійкості бізнесу в умовах цифрової економіки.

Ключові слова: кібербезпека, інформаційний бізнес, технічні системи захисту, штучний інтелект, кібератаки.

1. Актуальні кіберзагрози та виклики для інформаційного бізнесу

Інформаційний бізнес у XXI столітті все частіше стає об’єктом цілеспрямованих та складноорганізованих атак з боку кіберзлочинців та державних структур, що використовують цифрові інструменти як засіб економічного і політичного впливу. Серед основних кіберзагроз, з якими стикаються компанії, варто виокремити фішингові атаки, застосування програм-вимагачів, крадіжку персональних та фінансових даних, а також масові DDoS-атаки, що здатні паралізувати роботу онлайн-платформ та електронних сервісів [1,5].

Особливе занепокоєння викликають атаки на хмарні сервіси, оскільки вони стали ключовою складовою сучасних бізнес-процесів. У квітні 2024 року українські фахівці з кібербезпеки спільно з кібердепартаментом СБУ провели операцію, в результаті якої було знищено російський дата-центр, що обслуговував понад 10 тисяч підприємств військово-промислового комплексу та великих корпорацій енергетичної галузі [2,5]. Цей інцидент засвідчив, що кібератаки сьогодні можуть мати не лише економічні, а й безпосередньо військово-політичні наслідки, впливаючи на стабільність національної та міжнародної економіки.

2. Технічні системи захисту інформації: напрями розвитку та впровадження

Технічні засоби забезпечення кібербезпеки охоплюють широкий спектр рішень, що працюють на різних рівнях захисту. До апаратних засобів належать мережеві екрани, системи запобігання вторгненням, пристрої багатофакторної автентифікації та криптографічні модулі. Програмні рішення представлені антивірусними платформами, системами виявлення аномалій та інструментами шифрування даних. Важливим етапом розвитку є інтеграція хмарних сервісів кібермоніторингу та використання комплексних платформ управління безпекою типу SIEM та SOAR.

Останнім часом особливої уваги заслуговує впровадження технологій штучного інтелекту у процеси виявлення та нейтралізації загроз. Алгоритми машинного навчання дозволяють оперативно аналізувати великі масиви даних, визначати потенційні вразливості та прогнозувати сценарії кібератак у режимі реального часу. Це відкриває нові перспективи для проактивного захисту інформаційних ресурсів бізнесу та підвищення ефективності реагування на інциденти.

3. Міжнародні стандарти та глобальне співробітництво у сфері кіберзахисту

Розвиток ефективних систем кіберзахисту неможливий без інтеграції міжнародного досвіду та впровадження загальноприйнятих стандартів. Найпоширенішими у світі є стандарти ISO/IEC 27001 та рекомендації NIST Cybersecurity Framework, що визначають ключові підходи до управління інформаційною безпекою. У квітні 2024 року Міністерство оборони України ухвалило нову політику у сфері кібербезпеки, яка гармонізована з нормами НАТО та враховує міжнародні найкращі практики [3,5].

Важливим напрямом є міжнародна співпраця у протидії глобальним кіберзагрозам. Так, у 2024 році Національний банк України та Міністерство фінансів США підписали Меморандум про взаємодію, який передбачає обмін інформацією, спільні тренінги та підвищення стійкості фінансового сектору до кібератак [4,5].

4. Перспективи розвитку кіберзахисту в бізнесі

Подальший розвиток технічних систем захисту інформації пов'язаний із впровадженням інноваційних технологій. Зокрема, все більшого поширення набуватиме використання хмарних платформ для зберігання та обробки даних, а також технологій блокчейн, що забезпечують прозорість та незмінність інформації. Одним із нових напрямів стане розвиток кіберстрахування, яке дозволить бізнесу мінімізувати фінансові втрати від кібератак. Очікується, що поєднання технологій штучного інтелекту та автоматизованих систем управління кібербезпекою забезпечить принципово новий рівень захисту.

5. Сучасний стан українського інформаційного бізнесу та роль технічного захисту

У 2025 році український інформаційний бізнес включає провідні міжнародні та продуктові компанії — GlobalLogic Україна, EPAM Systems, Intellias, SoftServe, Luxoft, Fintech Band (mono) — а також сотні нових стартапів і малих IT-компаній. За першу половину року зареєстровано 848 нових IT-компаній, а кількість активних IT-ФОПів перевищила 262 тисячі [5]. Такий ріст бізнесу підвищує навантаження на інформаційну інфраструктуру та потребує впровадження сучасних технічних систем захисту, які забезпечують безперервність роботи, збереження клієнтських даних і відповідність міжнародним стандартам.

Великий акцент робиться на автоматизації безпеки, інтеграції SIEM-платформ, DLP-систем і захисту хмарних сховищ. Особливої уваги набуває

безпека у фінтех-секторі, де працюють компанії mono, Revolut, EasyPay та інші, оскільки саме фінансові сервіси найчастіше стають об’єктом атак.

ВИСНОВКИ

Отже, сучасні технічні системи кіберзахисту є невід’ємним елементом функціонування інформаційного бізнесу в умовах зростаючих кіберзагроз. Для ефективного захисту необхідна інтеграція інноваційних технологій, міжнародних стандартів та професійних знань фахівців. Україна має значний потенціал для розвитку власної кібербезпекової інфраструктури, проте потребує більшої координації між державними та приватними структурами. Водночас динамічний розвиток IT-бізнесу у 2025 році потребує впровадження нового рівня технічного захисту, орієнтованого на автоматизацію, моніторинг і кіберстійкість підприємств [5].

Список використаних джерел:

1. Законодавче визначення кібервійни допоможе українському кібернаступу – експерт. Укрінформ. 02.04.2024. URL: https://www.ukrinform.ua/rubric-technology/3847725-zakonodavce-viznacenna-kibervijni-dopomoze-ukrainskomu-kibernastupu-ekspert.html (дата звернення: 28.09.2025).
2. СБУ ідентифікувала хакерів російського ГРУ, які атакували «Київстар», і передасть матеріали справи в Гаагу – Ілля Вітюк. Служба безпеки України. 04.04.2024. URL: https://ssu.gov.ua/novyny/sbu-identyfikuvala-khakeriv-rosiiskoho-hru-yaki-atakuvaly-kyivstar-i-peredast-materialy-spravy-v-haahu-illia-vitiuk (дата звернення: 28.09.2025).
3. Bitdefender Releases 2024 Consumer Cybersecurity Assessment Report. Bitdefender. 03.04.2024. URL: https://www.bitdefender.com/blog/hotforsecurity/bitdefender-releases-2024-consumer-cybersecurity-assessment-report (дата звернення: 28.09.2025).
4. США допоможуть захистити банки та фінустанови України від кіберзагроз: деталі. Деньги.ua. 08.04.2024. URL: https://dengi.ua/ua/finance/7501735-ssha-pomogut-zaschitit-banki-i-finuchrezhdeniya-ukrainy-ot-kiberugroz (дата звернення: 28.09.2025).
5. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О. Довгань; упоряд. О. Довгань, Л. Литвинова, С. Дорогих. Київ: Державна наукова установа «Інститут інформації, безпеки і права НАПрН України», Національна бібліотека України імені В. І. Вернадського, 2024. № 4 (квітень). 320 с.

Петухова М.О.
студентка групи БСДМ-62, ННІКБЗІ ДУІКТ,
Київ,Україна
Мазур А.Т. студент групи БСДМ-62, ННІКБЗІ
ДУІКТ, Київ, Україна

ТЕХНОЛОГІЯ УПРАВЛІННЯ ПРИВІЛЕЙОВАНИМ ДОСТУПОМ: ПОРІВНЯННЯ РІШЕНЬ

Управління привілейованим доступом еволюціонувало від простого інструменту для зберігання паролів до фундаментального компонента архітектури Zero Trust і стратегії кіберстійкості. Сучасні організації стикаються з подвійним викликом, який полягає в організації захисту високоцінних привілейованих облікових записів від компрометації зловмисниками та потребою ефективно керувати цим доступом у складних, гетерогенних IT-системах, що охоплюють локальні середовища (on-premise), хмару та IT-системи.

Ключові слова: кібербезпека, управління, привілеї, доступ, , користувачі, інформаційна ситема.

Кількість бізнес-активів та інфраструктурних ресурсів, яким володіють організаці постійно зростають. Паралельно зростає і автоматизація процесів та впровадженням хмарних технологій, які створють динамічні середовища привілейованого доступу. Сучасні рішення PAM мають не тільки забезпечувати управління обліковими даними та сесіями, але й інтегрувати такі механізми, як адаптивна автентифікація, контекстно-орієнтований контроль і доступ Just-in-Time (JIT) для усунення постійних (standing) привілеїв. Ефективність PAM напряму впливає на здатність організації протистояти атакам, таким як Ransomware, які часто використовують привілейовані облікові записи для латерального переміщення [1].

Впровадження технології привілейованого доступу в інформаційній системі організації надають ряд переваг:

Безпечне керування привілейованим доступом

Забезпечує доступ до конфіденційних даних та критично важливих систем лише уповноваженим особам, запобігаючи несанкціонованому доступу та підвищуючи безпеку даних[2].

Моніторинг та аудит сеансів

Завдяки моніторингу сеансів у режимі реального часу та функціям детального ведення журналу активності, дії користувачів відстежуються миттєво. Це пришвидшує процес виявлення порушень безпеки та дозволяє негайно втрутитися [2].

Надійний захист з автентифікацією

Підвищує безпеку за допомогою багатофакторної автентифікації (MFA) та інших методів автентифікації. Це ускладнює доступ зловмисникам і додає додатковий рівень безпеки до процесів доступу.

Підтримка відповідності вимогам

Відповідає законодавчим нормам, таким як KVKK та GDPR. Автоматизує привілейований доступ та управління безпекою даних, допомагаючи організаціям легко виконувати свої зобов'язання щодо дотримання нормативних вимог.

Зменшення ризиків

Мінімізує ризики безпеки для привілейованих облікових записів. Контроль над обліковими записами високого рівня, які часто стають ціллю зловмисників, запобігає витоку даних та вразливостям системи.

Централізоване управління та простий аудит

Керуючи всіма привілейованими доступами з центральної точки, IT-команди можуть легко контролювати процеси доступу та заощаджувати час під час процедур аудиту.

На ринку рішень привілейованого доступу представлено багато рішень. Для проведення порівняльного аналізу в таблиці 1 представлено лідерів PAM рішень та результати аналізу щодо недоліків та переваг таких систем в розрізі вимог організацій до архітектури, компонент, ціноутворення [1].

Таблиця 1

Аналіз переваг та недоліків

Рішення	**Ключові Переваги (Advantages)**	**Ключові Недоліки (Disadvantages)**
ARCON	Конкурентоспроможне ціноутворення. Гнучке віртуальне групування ресурсів. Активний розвиток JIT та хмарних інтеграцій. Відкрита підтримка онбордингу з AWS, Azure, GCP.	Значний дефіцит у якості підтримки та централізованого управління . Слабша реалізація MFA порівняно з конкурентом. Ризик збільшення OpEx через складність адміністрування.
BeyondTrust	Найкраща у своєму класі EPM/Least Privilege. Виняткова якість аудиту та моніторингу сесій. Уніфікована платформа, готова до ITDR, OT та AI, що забезпечує майбутню стійкість. Високий рейтинг MFA та централізованого управління.	Висока вартість володіння (преміум-сегмент). Складність орієнтації у продуктовій лінійці через велику кількість спеціалізованих інструментів.
One Identity Safeguard	Спеціалізована кластерна архітектура для максимальної HA та DR (SPP/SPS). Розділення функцій (Passwords/Sessions) для підвищеної стійкості.	Непублічне ціноутворення. Вимагає більших інвестицій у спеціалізовані ресурси (аплайнси) та їхнє обслуговування.

Перелік посилань:

1. Кращі рішення PAM. URL: https://oberig-it.com/statti/12-najkrashhyh-prykladiv-vykorystannya-ram/ .
2. Переваги PAM. URL: https://www.gardiyan.com/en/products/gardiyan-pam/overview .

Корж А.Ю.
студентка групи БСДМ-51,
ННКБЗІ ДУІКТ, Київ, Україна

ЕТИЧНІ АСПЕКТИ ЗБОРУ ТА ВИКОРИСТАННЯ ІНФОРМАЦІЇ З ВІДКРИТИХ ДЖЕРЕЛ

Розвиток інформаційних технологій і соціальних медіа зробив відкриті дані потужним інструментом для аналізу, досліджень і забезпечення безпеки. Сьогодні методи OSINT (Open Source Intelligence) активно використовуються у сфері кібербезпеки, журналістики, бізнес-аналітики та державного управління. Водночас постає низка етичних питань, пов'язаних із тим, як саме збирають, аналізують і поширюють відкриту інформацію, зокрема персональні дані.

Ключові слова: кібербезпека, OSINT, етика

Хоча інформація у відкритому доступі формально вважається публічною, її масовий збір, систематизація та подальший аналіз можуть призводити до порушення етичних норм. Наприклад, дослідник чи аналітик може випадково опрацювати персональні відомості, які користувач не призначав для широкого розповсюдження, або зробити висновки, що створюють ризик для безпеки особи. Крім того, відкриті джерела можуть містити дезінформацію, тому етичний фахівець OSINT зобов'язаний перевіряти достовірність отриманих даних і не поширювати неперевірені факти. [1]

Окремої уваги потребує питання цільового використання OSINT. Етичне застосування передбачає збір даних лише з метою захисту, дослідження або інформування суспільства. Використання цих даних для маніпуляцій, шантажу чи дискредитації осіб є грубим порушенням принципів відкритої розвідки. Водночас OSINT може бути важливим інструментом для викриття злочинів або порушень прав людини, що підкреслює значення етичної відповідальності дослідника за наслідки своїх дій.

Міжнародні стандарти, такі як GDPR у Європейському Союзі, регулюють захист персональних даних і встановлюють чіткі вимоги до їх обробки. Для фахівців із кібербезпеки це означає необхідність поєднання правових норм із етичними принципами: прозорість, законність, пропорційність і мінімізація втручання в приватне життя.

Процес роботи з відкритими джерелами інформації складається з кількох послідовних етапів, які утворюють так званий OSINT-цикл. Кожен із них має своє завдання і важливе значення для достовірності результатів.[2]

Direction & Planning (визначення напрямів і планування) На цьому етапі формулюється мета дослідження: що саме потрібно з'ясувати, які питання стоять перед аналітиком і які джерела можуть бути корисними. Правильне планування дозволяє уникнути зайвого збору даних і сконцентрувати зусилля на найбільш важливій інформації.

Collection (збір даних) Відповідно до визначеної мети відбувається збір відкритих даних із різних джерел — соціальних мереж, офіційних реєстрів, новинних ресурсів, форумів, публічних баз тощо. На цьому етапі важливо дотримуватися етичних норм і не виходити за межі законного доступу.

Processing & Collation (обробка і впорядкування даних) Зібрані матеріали зазвичай містять надлишкову або неструктуровану інформацію. Тому наступним кроком є очищення даних, усунення повторів, перевірка достовірності та приведення матеріалу до зручного формату для подальшого аналізу.

Analysis & Integration (аналіз та інтеграція) На цьому етапі аналітик оцінює зміст отриманих даних, порівнює різні джерела, виявляє закономірності, зв'язки, тенденції. Важливо інтегрувати різні фрагменти інформації в єдину картину, щоб отримати узагальнений висновок або прогноз.

Production & Dissemination (підготовка результатів та поширення) Заключний етап передбачає оформлення результатів OSINT-аналізу у вигляді звіту, аналітичної довідки або рекомендацій. Інформація передається замовнику, організації або публікується для широкої аудиторії — залежно від мети дослідження.

Усі ці етапи взаємопов'язані та утворюють циклічний процес: отримані результати можуть ініціювати новий цикл збору та перевірки даних. Такий підхід забезпечує системність, точність і об'єктивність аналітичної роботи у сфері відкритої розвідки.[3]

Рис. 1. Життєвий цикл OSINT

Отже, етичні аспекти OSINT є одним з ключових елементів професійної культури в сфері кібербезпеки. Відповідальне використання відкритих джерел не лише забезпечує законність дій, а й формує довіру суспільства до аналітичної діяльності. Майбутні фахівці повинні розуміти, що технології відкритої розвідки — це не лише інструмент збору інформації, а й сфера моральної відповідальності.

Перелік посилань:

1.SANS Institute. What is Open Source Intelligence? – URL: https://www.sans.org/blog/what-is-open-source-intelligence (дата звернення: 06.10.2025).

2.European Union. General Data Protection Regulation (GDPR). – URL: https://gdpr.eu (дата звернення: 06.10.2025).

3.Bellingcat. Ethical Guidelines for Open Source Investigations. – URL: https://www.bellingcat.com/resources/how-tos/2023/03/12/ethics-in-osint (дата звернення: 06.10.2025).

Комісар В.Д.

студент групи БСДМ-63 ННІКБЗІ ДУІКТ,
Київ, Україна

ТЕХНОЛОГІЯ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА ІНЦИДЕНТИ НА ОСНОВІ ПЛАТФОРМИ ELASTIC STACK

Стрімке зростання кіберінцидентів на світовій арені, які, за прогнозами, спричинять збитки на суму близько $10,5 трильйонів USD до 2025 року, підкреслює критичну вразливість сучасних цифрових інфраструктур. В умовах, коли кіберзагрози стають все більш складними, автоматизованими та цілеспрямованими, традиційні підходи до безпеки, що базуються на реактивному моніторингу, виявляються недостатніми. Головною вимогою до сучасних систем захисту є здатність забезпечувати виявлення в режимі реального часу, оперативний аналіз та автоматизоване реагування.

Ключові слова: інцидент, реагування на інциденти, безпека

Зростання кіберінцидентів на світовій арені у період 2023–2025 років характеризується не лише збільшенням їхньої кількості, але й критичним зростанням їхньої складності та фінансових збитків, що підкреслює глобальну необхідність вдосконалення технологій виявлення та реагування.

Інцидент варто визначити як незаплановану подію або низку взаємопов'язаних подій у сфері інформаційної безпеки, яка порушує або загрожує порушити встановлені політики безпеки, спричиняючи негативний вплив на конфіденційність, цілісність чи доступність (CIA) інформаційних активів, систем чи мереж організації. Актуальність теми зумовлена необхідністю швидкого і точного виявлення загроз, оскільки зростання обсягів даних і складності сучасних IT-інфраструктур вимагає автоматизованих, високопродуктивних рішень.

Платформа Elastic Stack є ключовою технологічною основою для створення ефективної системи виявлення та реагування на інциденти. Вона функціонує як SIEM (Security Information and Event Management) та SOAR (Security Orchestration, Automation, and Response) інструмент. [1]

Архітектура Elastic Stack побудована навколо трьох основних компонентів: Elasticsearch (розподілена пошукова та аналітична система), Logstash (інструмент для вилучення, трансформації та завантаження даних) та Kibana (платформа для візуалізації даних). Цей стек дозволяє збирати, зберігати, аналізувати та візуалізувати дані з різних джерел у режимі реального часу, що робить його ефективним інструментом для моніторингу, аналізу логів та вирішення інших завдань у IT-інфраструктурі. [2]

- Elasticsearch: Серце стека, розподілена система пошуку та аналізу, що використовує технологію Apache Lucene. Вона дозволяє індексувати, зберігати та швидко знаходити великі обсяги даних.
- Logstash: Інструмент, який збирає дані з різних джерел (логи, метрики), перетворює їх (очищає, збагачує, форматує) і потім відправляє до Elasticsearch чи інших місць призначення.

- Kibana: Веб-інтерфейс, призначений для роботи з даними, що зберігаються в Elasticsearch. З його допомогою можна створювати інтерактивні дашборди, звіти та візуалізації для моніторингу та аналізу даних.

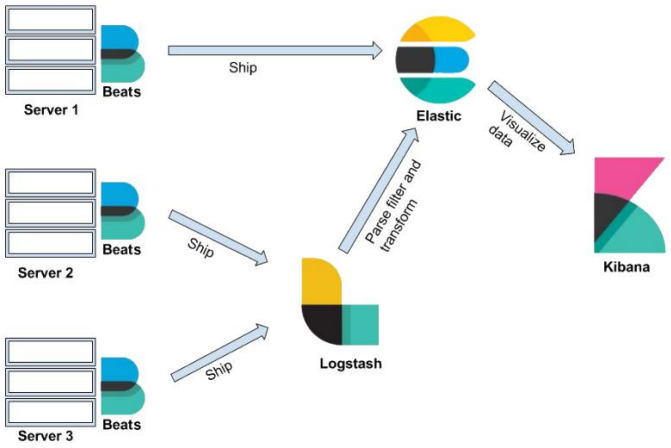

Рис. 1. Архітектура Elastic Stack

Використання платформи Elastic Stack є критично важливим та надзвичайно зручним для реагування на кіберінциденти, оскільки вона надає єдиний, високомасштабований інструментарій для роботи з даними. Зручність починається з централізації логів: компоненти Beats та Logstash збирають, нормалізують і консолідують величезні обсяги журналів, метрик та мережевого трафіку з усієї інфраструктури (серверів, хмарних систем, кінцевих точок) у єдиному репозиторії Elasticsearch. Це усуває потребу в ручному перемиканні між десятками систем, забезпечуючи аналітику «єдине вікно» для всіх доказів інциденту. Далі, Elasticsearch забезпечує високошвидкісний повнотекстовий пошук і складні запити за мілісекунди, що є життєво необхідним для скорочення часу реагування (MTTR), адже дозволяє миттєво знаходити індикатори компрометації (IoC), такі як скомпрометовані IP-адреси чи хеші. Ця швидкість посилюється інтегрованим модулем Elastic Security (SIEM), який автоматично виявляє складні загрози, використовуючи машинне навчання для ідентифікації аномалій та підозрілої поведінки користувачів, що є необхідним для перехоплення атаки на ранній стадії. Зрештою, Kibana візуалізує ці дані за допомогою інтерактивних дашбордів та графіків, перетворюючи сирі події на зрозумілу часову послідовність атаки, що спрощує криміналістичний аналіз та дозволяє команді безпеки не просто моніторити, а активно та оперативно реагувати на інциденти, локалізуючи загрозу і забезпечуючи швидке відновлення.

Перелік посилань:
1. Elastic Stack. URL https://www.elastic.co/elastic-stack
2. Аналіз інцидентів. URL: https://elartu.tntu.edu.ua/handle/lib/41680

Забенко Ілля Олексійович
студент групи БСДМ-63, ННІЗІ ДУІКТ,
Київ, Україна

ФОРМУВАННЯ ЦІЛЬОВОГО ПРОФІЛЮ БЕЗПЕКИ ЯК ЕТАП РОЗРОБКИ АВТОРИЗОВАНОЇ СИСТЕМИ З БЕЗПЕКИ

В Україні, згідно чинного законодавства у сфері захисту інформації, інформація поділяється на відкриту та з обмеженим доступом. Уся інформація з обмеженим доступом підлягає захисту та обробці у спеціально захищених інформаційно-комунікаційних системах, захищеність яких є підтвердженою шляхом занесення системи дописку систем, що авторизовані з безпеки. Одним з ключових етапі створення подібних систем є формування цільового профілю безпеки з подальшою його реалізацією.

Ключові слова: профіль безпеки, заходи захисту, автоматизована система.

Цільовий профіль безпеки – це перелік вимог (далі – заходів захисту) до системи, її окремих інженерно-технічних рішень, програмно-апаратних засобів або організаційних заходів, що спрямовані на захист конфіденційності, цілісності та доступності інформації яка зберігається або обробляється в межах автоматизованої системи.

Цільовий профіль безпеки формується на основі базового профілю безпеки, що містить заходи захисту які необхідно реалізувати незалежно від особливостей системи, оцінки середовища функціонування інформаційно-комунікаційної системи та оцінки ризиків, що перелічує найнебезпечніші або найвірогідніше ризики які можуть загрожувати конкретній системі, а також надає рекомендації що до нівелювання виявлених ризиків або зменшення показника їхньої небезпечності для автоматизованої системи. Для деяких інформаційно-комунікаційних систем також може бути представлений галузевий профіль безпеки.

Галузевий профіль безпеки – це визначений набір заходів захисту, посилень заходів захисту та додаткових рекомендацій, отриманих на основі налаштування й уточнення базового профілю безпеки з урахуванням особливостей галузі. Галузевий профіль безпеки містить налаштування та уточнення заходів захисту базового профілю безпеки, додаткові заходи захисту (або обґрунтоване вилучення заходів захисту), які обґрунтовані для конкретних технологій, робочих середовищ, типів інформаційних систем, типів функцій/завдань/операцій, режимів роботи, які є специфічними для галузі, та встановлених галузевими стандартами або нормативними документами вимог [2].

У рамках формування цільового профілю безпеки до базового профілю безпеки (або за наявності галузевого) додаються заходи захисту, що спрямовані на захист від ризиків та загроз що були виявлені та проаналізовані на попередньому етапі.

Усі можливі для вибору заходи захисту згруповані до одного з 20 класів захисту.

№ з/п	ID класу	Назва класу
1.	AC	Управління доступом
2.	AT	Обізнаність і навчання
3.	AU	Аудит і підзвітність
4.	CA	Оцінювання, акредитація та моніторинг безпеки
5.	CM	Управління конфігурацією
6.	CP	Планування безперервної роботи
7.	IA	Ідентифікація та автентифікація
8.	IR	Реагування на інциденти
9.	MA	Технічне обслуговування
10.	MP	Захист носіїв інформації
11.	PE	Фізичний захист і захист робочого середовища
12.	PL	Планування безпеки
13.	PM	Менеджмент інформаційної безпеки
14.	PS	Кадрова безпека
15.	PT	Повноваження на обробку персональних даних
16.	RA	Оцінка ризику
17.	SA	Придбання системи та послуг
18.	SC	Системний і комунікаційний захист
19.	SI	Цілісність системи та інформації
20.	SR	Управління ризиками ланцюга поставок

Рис. 1. Класи захисту

В межах майже усіх заходів захисту присутні посилення, що дають можливість конкретизувати або доповнити вимогами основний захід захисту. Деякі посилення заходів захисту містяться у базовому профілі безпеки та є обов’язковими до реалізації, але лише разом з основним заходом захисту, посиленням якого вони є.

Перелік посилань:

1. НД ТЗІ 3.6-006-24 Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=66109 (date of access: 05.10.2025).
2. Закон України Про захист інформації в інформаційно-комунікаційних системах. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (date of access: 05.10.2025).

Ігнатенко Г.Л.
студент групи 125-22-1,
НТУ «Дніпровська політехніка»,
Дніпро, Україна

Мєшков В.І.
старший викладач каф. БІТ,
НТУ «Дніпровська політехніка»,
Дніпро, Україна

ВИКОРИСТАННЯ SIEM-СИСТЕМ ДЛЯ МОНІТОРИНГУ ПОДІЙ БЕЗПЕКИ ТА УПРАВЛІННЯ ІНЦИДЕНТАМИ В ОРГАНІЗАЦІЯХ

У роботі розглянуто роль та значення SIEM-систем у забезпеченні інформаційної безпеки організацій. Проаналізовано архітектуру, функціональні можливості та принципи роботи SIEM, а також їх інтеграцію з іншими компонентами систем кіберзахисту (IDS/IPS, SOAR, XDR). Особливу увагу приділено процесам моніторингу подій, управлінню інцидентами та автоматизації реагування. Визначено основні переваги, виклики та вимоги до впровадження таких систем, а також перспективи їх розвитку з урахуванням технологій штучного інтелекту та хмарних рішень.

Ключові слова: SIEM, інформаційна безпека, моніторинг подій, управління інцидентами, SOAR, XDR, штучний інтелект, кіберзахист.

Security Information and Event Management (SIEM) є одним із ключових інструментів сучасної архітектури кіберзахисту, що забезпечує централізований збір, кореляцію та аналіз подій інформаційної безпеки [1]. У контексті постійного зростання кількості кібератак та ускладнення методів їх реалізації, SIEM-системи стають невід'ємною складовою стратегії інформаційної безпеки організацій [3]. Їх основне завдання полягає у виявленні, запобіганні та реагуванні на загрози до того, як вони можуть вплинути на критичні бізнес-процеси. Централізований моніторинг безпеки вже не є опцією, а необхідною умовою ефективного управління ризиками в інформаційному середовищі.

Події інформаційної безпеки являють собою ідентифіковані стани систем або мереж, які можуть свідчити про потенційне порушення політики безпеки, відмову засобів захисту чи інші небезпечні відхилення. Інцидентом інформаційної безпеки вважається подія або сукупність подій, що мають значну ймовірність впливу на функціонування бізнесу та компрометацію даних. Таким чином, події є первинними сигналами можливих загроз, а інциденти – підтвердженими проявами порушення безпеки, які потребують негайного реагування.

Типова SIEM-система складається з декількох взаємопов'язаних компонентів: джерел даних, модулів збору та зберігання журналів, механізмів нормалізації та аналітичних модулів. Система отримує інформацію з різних джерел – серверів, мережевих пристроїв, міжмережевих екранів, антивірусних засобів, систем автентифікації, а також з IDS/IPS. Уніфікація форматів даних забезпечує можливість їхньої подальшої кореляції, тобто встановлення взаємозв'язків між подіями, які окремо можуть здаватися незначними, але разом утворюють картину атаки. Наприклад, велика кількість невдалих спроб входу з однієї IP-адреси, за якою згодом відбувається успішний логін, може бути ознакою атаки типу brute force.

Управління інцидентами безпеки ґрунтується на підходах, визначених міжнародним стандартом ISO/IEC 27035 «Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 1. Принципи та процес» [4]. Він передбачає п’ять ключових етапів: підготовку, виявлення і звітування, оцінку інциденту, реагування, а також аналіз і вдосконалення процесів. Підготовчий етап охоплює формування політик безпеки, навчання персоналу та впровадження інструментів моніторингу. На етапі виявлення проводиться реєстрація події та визначення її характеру, після чого здійснюється оцінка критичності. Реагування передбачає локалізацію інциденту, усунення наслідків та відновлення функціонування системи. Заключний етап, спрямований на аналіз і вдосконалення, забезпечує накопичення досвіду та підвищення зрілості процесів реагування.

Ефективність SIEM істотно підвищується при інтеграції з іншими системами кіберзахисту. Поєднання SIEM з IDS/IPS дозволяє не лише фіксувати атаку, але й блокувати її в реальному часі. Спільна робота з DLP-системами забезпечує контроль над рухом конфіденційної інформації та запобігання її витоку. Інтеграція з SOAR дає змогу автоматизувати реагування на події, зокрема виконувати блокування облікових записів, ізоляцію заражених пристроїв або блокування підозрілих IP-адрес. Взаємодія з XDR-рішеннями надає змогу отримувати розширений контекст інцидентів, аналізувати поведінкові аномалії та виявляти складні багаторівневі атаки.

Процес впровадження SIEM в організації потребує врахування низки технічних, організаційних та кадрових вимог. До технічних належать наявність відповідних серверних ресурсів, достатній обсяг пам’яті, а також резервування сховищ даних для журналів подій. Організаційні вимоги включають розробку регламентів реагування, визначення зон відповідальності та механізмів ескалації інцидентів. Важливим фактором є наявність кваліфікованих фахівців, здатних налаштовувати правила кореляції, аналізувати сповіщення та приймати рішення щодо реагування. Серед основних викликів можна виокремити високу вартість рішень, складність налаштування, велику кількість хибних спрацьовувань при недосконалих правилах кореляції та значні вимоги до обчислювальних потужностей.

Незважаючи на ці труднощі, переваги SIEM є очевидними. Вони забезпечують централізований моніторинг усієї інфраструктури, зменшують час виявлення загроз, покращують обізнаність про поточний стан безпеки та підвищують рівень контролю за виконанням політик. Завдяки інтеграції з системами автоматизованого реагування знижується вплив людського фактора, а ефективність аналітиків SOC (Security Operations Center) істотно зростає.

Сучасні тенденції розвитку SIEM пов’язані з активним використанням технологій штучного інтелекту та машинного навчання. Алгоритми аналізу поведінкових патернів дозволяють виявляти нетипові дії користувачів, автоматично формувати пріоритетність сповіщень і скорочувати кількість хибних тривог [2]. Впровадження хмарних технологій сприяє розвитку так званих cloud-SIEM-рішень, які надають можливість масштабування під потреби

бізнесу без значних капітальних витрат. Прикладами таких рішень є Microsoft Sentinel і Google Chronicle, що реалізують підхід «SIEM as a Service» із вбудованими засобами штучного інтелекту для аналізу подій у реальному часі.

Проведене дослідження підтверджує, що системи класу SIEM відіграють ключову роль у формуванні ефективної стратегії кіберзахисту сучасних організацій. Вони забезпечують централізований збір, нормалізацію та аналіз подій безпеки, створюючи цілісну картину стану інформаційної інфраструктури. Завдяки поєднанню аналітичних механізмів, засобів кореляції та автоматизованого реагування SIEM-системи дозволяють оперативно виявляти загрози, мінімізувати наслідки інцидентів і підвищувати рівень зрілості процесів управління безпекою. Інтеграція SIEM з іншими інструментами кіберзахисту, такими як IDS/IPS, SOAR, XDR, а також застосування штучного інтелекту й машинного навчання, розширюють можливості таких рішень у напрямку інтелектуального моніторингу та автоматизованого реагування. Незважаючи на високу вартість впровадження та складність налаштування, переваги SIEM у зниженні ризиків і забезпеченні безперервного контролю інформаційних систем є беззаперечними. Подальший розвиток SIEM-технологій орієнтований на інтеграцію з хмарними сервісами, створення гібридних моделей моніторингу, удосконалення алгоритмів поведінкового аналізу та прогнозування інцидентів, що уможливлює побудову більш гнучких, адаптивних та інтелектуальних систем кіберзахисту, здатних ефективно протидіяти динамічним і складним загрозам інформаційній безпеці.

Перелік посилань:

1. What is security information and event management (SIEM)? IBM. IBM Mediacenter. URL: https://mediacenter.ibm.com/media/What%2BIs%2BSIEM/1_98oa8pnb (дата звернення: 07.10.2025).

2. González-Granadillo, G., González-Zarzosa, S., Diaz, R. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. Sensors, 2021, 21(14):4759. DOI:10.3390/s21144759.

3. ДСТУ ISO/IEC 27001:2015 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги» (ISO/IEC 27001:2013/Cor 2:2015).

4. ДСТУ ISO/IEC 27035-1:2021 (ISO/IEC 27035-1:2016, IDT). Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 1. Принципи та процес. – К.: ДП «УкрНДНЦ», 2021. – 54 с.

Ганжа М.Д.
студент групи 125-22-1,
НТУ «Дніпровська політехніка»,
Дніпро, Україна

Мєшков В.І.
старший викладач каф. БІТ,
НТУ «Дніпровська політехніка»,
Дніпро, Україна

ВПРОВАДЖЕННЯ ПОЛІТИК РЕЗЕРВНОГО КОПІЮВАННЯ ТА ВІДНОВЛЕННЯ ДАНИХ ЯК СКЛАДОВОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

У роботі розглянуто впровадження політик резервного копіювання та відновлення даних як ключового елемента інформаційної безпеки підприємства. Проаналізовано типи резервного копіювання, принципи зберігання, зокрема правило «3-2-1» і його розширену модель «3-2-1-1-0». Розкрито значення показників RTO та RPO для планування відновлення після інцидентів. Обґрунтовано роль політик резервного копіювання у підтриманні безперервності бізнес-процесів, відповідності вимогам міжнародних стандартів ISO/IEC 27001 та GDPR і мінімізації ризиків втрати даних.

Ключові слова: резервне копіювання, відновлення даних, інформаційна безпека, безперервність бізнесу, RTO, RPO.

У сучасному цифровому середовищі дані є одним із найцінніших активів будь-якого підприємства, а їхня втрата може спричинити серйозні фінансові, операційні та репутаційні збитки. Зі зростанням кількості та складності кіберзагроз питання захисту інформації стає все більш актуальним. Програми-вимагачі, шкідливе програмне забезпечення, збої обладнання, людські помилки та природні катастрофи становлять безпосередню загрозу збереженню даних. Втрата навіть невеликої частини критичної інформації може призвести до зупинки бізнес-процесів, порушення договірних зобов’язань і втрати довіри клієнтів. У таких умовах політики резервного копіювання та відновлення даних є не додатковим, а обов’язковим елементом системи управління інформаційною безпекою підприємства.

Резервне копіювання забезпечує можливість відновлення інформації після реалізації інцидентів різного типу та дозволяє мінімізувати наслідки кібератак, технічних відмов і людського фактору. Основною метою є створення надійної інфраструктури зберігання даних, здатної забезпечити відновлення систем до робочого стану з мінімальними втратами. Серед основних загроз, що впливають на безпеку даних, варто виокремити шкідливе програмне забезпечення, зокрема програми-вимагачі (ransomware), які шифрують дані та блокують доступ до них, а також атаки типу wiper, спрямовані на повне знищення або пошкодження інформації. Додаткову небезпеку становлять помилки користувачів, випадкове або навмисне видалення файлів, вихід з ладу обладнання через знос чи зовнішні чинники, фізичні інциденти, пов’язані з пожежами, затопленням чи перебоями електропостачання, а також несанкціонований доступ до інформаційних систем унаслідок компрометації облікових даних. Ці ризики свідчать про те, що жодна

система не може бути повністю захищеною, а резервне копіювання виступає останньою лінією оборони, яка гарантує відновлення інформації після інциденту.

Вибір типу копіювання залежить від специфіки підприємства, частоти змін даних і доступних ресурсів. Повне копіювання створює точну копію всієї системи, що забезпечує максимальну надійність, але потребує значного обсягу пам’яті та часу. Інкрементальне копіювання є більш ефективним, адже зберігає лише ті файли, що були змінені після останнього резервування, тоді як диференційне копіювання дозволяє швидше відновлювати дані, оскільки охоплює зміни, зроблені після останнього повного копіювання. Поєднання цих типів у рамках єдиної стратегії резервування забезпечує баланс між швидкістю, вартістю та надійністю процесу.

Важливу роль відіграє також вибір місця зберігання копій. Для підвищення надійності рекомендується поєднувати локальні та віддалені (зокрема хмарні) сховища, що гарантує як оперативне відновлення даних у межах підприємства, так і захист від фізичних пошкоджень або локальних кібератак. Оптимальним підходом вважається дотримання правила «3-2-1», яке передбачає наявність трьох копій даних, розміщених на двох різних носіях, одна з яких має зберігатися поза межами основної інфраструктури [1]. На практиці дедалі більшого поширення набуває розширене правило «3-2-1-1-0», що доповнює класичну модель додатковою копією, захищеною від змін, та регулярним тестуванням процесів відновлення для забезпечення нульового рівня помилок.

Наявність копій даних не гарантує можливості їх успішного відновлення без чітко визначеної стратегії. Для цього використовуються показники RTO (Recovery Time Objective) та RPO (Recovery Point Objective), які визначають максимально допустимий час простою системи й обсяг даних, що може бути втрачений без критичного впливу на діяльність організації [2]. Оптимізація цих параметрів дозволяє збалансувати витрати на зберігання з реальними потребами у швидкості відновлення бізнес-процесів.

Політика резервного копіювання має бути інтегрована у систему управління ризиками підприємства та узгоджена з планами забезпечення безперервності бізнесу. Вона повинна охоплювати класифікацію даних за критичністю, визначення періодичності копіювання, регламент доступу до резервів, застосування шифрування, а також регулярне тестування процесів відновлення. Дотримання таких вимог гарантує готовність компанії до реагування на інциденти будь-якого масштабу.

Важливим нормативним аспектом є відповідність міжнародним стандартам і законодавчим вимогам. Згідно з ISO/IEC 27001 резервне копіювання розглядається як складова системи управління інформаційною безпекою (ISMS) та є необхідною умовою для підтримання безперервності діяльності організації [3]. Крім того, положення Загального регламенту про захист даних (GDPR) зобов’язують компанії забезпечувати здатність відновлювати доступність персональних даних і підтримувати їхню цілісність

після кіберінцидентів [4]. Таким чином, впровадження ефективних політик резервного копіювання не лише знижує технічні ризики, а й сприяє дотриманню законодавчих норм і збереженню репутаційної довіри до компанії.

Комплексна політика резервного копіювання та відновлення даних є фундаментальною складовою інформаційної безпеки підприємства. Її впровадження забезпечує стійкість до кібератак, мінімізує наслідки людських помилок, технічних відмов і фізичних інцидентів, а також дозволяє підтримувати безперервність бізнес-процесів навіть у кризових умовах. Поєднання технічних засобів із організаційними процедурами, регулярне оновлення та тестування політик формують основу ефективної системи захисту даних і забезпечують стабільність діяльності підприємства у сучасному цифровому середовищі.

Перелік посилань:

1. Що таке «стратегія резервного копіювання за правилом 3-2-1» і як її використовувати? Dropbox [Електронний ресурс]. – Режим доступу: https://experience.dropbox.com/uk-ua/resources/3-2-1-backup-strategy (дата звернення: 02.10.2025).

2. Звягінцева О. RTO та RPO: що треба знати про резервне копіювання даних. Kyivstar Business Hub [Електронний ресурс]. – Режим доступу: https://hub.kyivstar.ua/articles/rto-ta-rpo-shho-treba-znati-pro-rezervne-kopiyuvannya-danih (дата звернення: 02.10.2025).

3. Bobro N. ISO/IEC 27001 та важливість резервного копіювання: всебічний огляд з Langmeier Backup. Langmeier Software [Електронний ресурс]. – Режим доступу: https://www.langmeier-software.com/uk/seiten/datensicherung/iso-270001-datensicherung# (дата звернення: 02.10.2025).

4. General Data Protection Regulation (GDPR). Regulation (EU) 2016/679 від 27.04.2016 [Електронний ресурс]. – Режим доступу: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679 (дата звернення: 02.10.2025).

Дєдіщев Денис Олегович
студент групи БСДМ-63, ННІЗІ ДУІКТ, Київ, Україна

BREACH AND ATTACK SIMULATION (BAS): РОЛЬ У ВАЛІДАЦІЇ КОНТРОЛІВ SIEM ТА ПЕРЕВІРЦІ ЕФЕКТИВНОСТІ EDR

У сучасних корпоративних мережах формальна наявність засобів захисту не гарантує їх фактичної дієздатності. Breach and Attack Simulation (BAS) — це підхід до безперервної перевірки безпеки, який автоматизовано відтворює тактики, техніки та процедури (TTP) з реального арсеналу зловмисників, аби підтвердити працездатність наявних контролів і виміряти здатність організації виявляти та стримувати атаки. На відміну від разових пентестів чи сканувань вразливостей, BAS надає регулярну, метрикоорієнтовану перевірку якості логування, кореляційних правил SIEM і можливостей EDR у режимах detect/block.

Для валідації SIEM BAS виконує сценарії, скомпоновані за MITRE ATT&CK (наприклад, T1059 — Command and Scripting, T1218 — Signed Binary Proxy Execution, T1041 — Exfiltration Over C2 Channel), та перевіряє три рівні успіху: (1) наявність телеметрії у відповідних джерелах (Sysmon/Windows Event Logs, auditd, мережеві логи, EDR-датчики); (2) спрацьовування парсерів/нормалізації та наповнення полів, необхідних для кореляції; (3) спрацьовування правил/детекторів з очікуваним пріоритетом інциденту. Результати агрегуються у показники покриття матриці MITRE ATT&CK, MTTD, частку «німого» логування (телеметрія без алерту) та рівень хибних спрацювань після тюнінгу.

Перевірка EDR з BAS охоплює виявлення на різних етапах (pre-execution, on-execution, post-execution) і реакції (kill, quarantine, network isolation, rollback). Для кожного TTP фіксуються: чи був артефакт заборонений/знешкоджений, чи сформовано аналітичний сигнал для SOC, як маркується загроза (тег/класифікація), і чи коректно передано подію в SIEM. Окремо оцінюють чутливість політик (thresholds), наявність евристичних/поведінкових детекцій та вплив на продуктивність. Ефективний цикл BAS включає: визначення бізнес-критичних сценаріїв (шляхи атаки на найцінніші активи/сервіси та ексфільтрація), базову перевірку готовності логування (часова синхронізація, цілісність індексів, схеми полів), мапінг на ATT&CK/D3FEND, запуск модулів (endpoint, email, lateral movement, data exfiltration, cloud), верифікацію спрацювань та пріоритизацію фіксів. Дана практика перетворює отримані результати на наступні покращення: увімкнення відсутніх джерел, корекція парсерів, підсилення кореляційних правил, оптимізація EDR-політик і плейбуків реагування. Переваги підходу — визначення ефективності контролів, раннє виявлення «дрейфу конфігурацій», зниження MTTD/MTTR та доказове підвищення кіберстійкості без ризикованих ручних експериментів.

Перелік посилань:

1. MITRE ATT&CK®: Adversarial Tactics, Techniques, and Common Knowledge. The MITRE Corporation, 2025..
2. NIST SP 800-61 Rev.2. Computer Security Incident Handling Guide. NIST, 2012.
3. NIST SP 800-53 Rev.5. Security and Privacy Controls for Information Systems and Organizations. NIST, 2020.
4. ISO/IEC 27001:2022. Information security management systems — Requirements. ISO, 202 2020.
5.

Авраменко Андрій Юрійович
студент групи ІСДм-62,
ННІІТ ДУІКТ, Київ, Україна

СМАРТ-ТЕХНОЛОГІЇ ТА ІНТЕРНЕТ РЕЧЕЙ

Що ми розуміємо під смарт-технологіями та Інтернетом речей? "Розумний будинок" — це об'єднана система датчиків та техніки, що дозволяє автоматизувати повсякденні завдання, керувати пристроями зі смартфона чи планшета, а також підвищувати комфорт, безпеку та енергоефективність оселі. Ця технологія включає управління освітленням, кліматом, безпекою, мультимедіа та побутовою технікою, працюючи через централізований центр керування та підтримуючи дистанційний контроль через інтернет.

Ключові слова: смарт-технологія, інтернет речей, кібербезпека, розумний будинок.

У сучасному світі технології стають дедалі інтегрованішими в повсякденне життя. Одним з найперспективніших напрямів інноваційного розвитку є Інтернет речей (Internet of Things, IoT), що передбачає об’єднання фізичних пристроїв у єдину мережу для взаємодії та обміну даними. Особливо актуальним є впровадження IoT у побут — у так звані «розумні будинки», які дозволяють автоматизувати управління різними системами: освітленням, опаленням, безпекою, вентиляцією, побутовими приладами тощо.

«Розумний будинок» — це не лише набір автоматизованих рішень, а й інтегрована екосистема, що підвищує якість життя, забезпечує безпеку мешканців, дозволяє ефективно використовувати енергоресурси та зменшити

витрати. Але попри значний прогрес у цій сфері, досі існують проблеми, пов’язані з сумісністю пристроїв, стандартизацією протоколів зв’язку, питаннями приватності та кібербезпеки, а також доступністю таких систем для широкого кола споживачів.

Таким чином, завдання полягає у дослідженні можливостей застосування IoT-технологій у побуті, розробці прототипу «розумного будинку» та оцінці його ефективності з практичної точки зору.

Метою даного дослідження є аналіз сучасних апаратних та програмних засобів для реалізації систем «розумного будинку» на базі IoT, проєктування і створення функціонального прототипу з використанням доступних технологій, а також проведення оцінки отриманих результатів у контексті енергоефективності, безпеки, зручності експлуатації та потенціалу для масштабування.

У ході дослідження було проведено аналіз існуючих IoT-платформ (наприклад, Arduino, Raspberry Pi, ESP8266/ESP32) та протоколів зв’язку (MQTT, ZigBee, Z-Wave, Wi-Fi), що найбільш часто застосовуються в системах «розумного будинку».

Розроблено прототип системи «розумного будинку» на базі мікроконтролера ESP32 з підтримкою Wi-Fi, до якого підключено сенсори температури, вологості, датчик руху та реле керування освітленням. Для передачі даних використано протокол MQTT, а керування здійснюється через мобільний додаток та веб-інтерфейс.

Було реалізовано функції автоматичного регулювання температури, виявлення руху з активацією сигналізації, віддаленого керування освітленням та оповіщення користувача у разі аномальних ситуацій. Система дозволила знизити енергоспоживання на 18% за рахунок автоматичного вимкнення освітлення та електроприладів при відсутності людей у приміщенні.

Також проаналізовано питання кібербезпеки: впроваджено базові заходи захисту — шифрування трафіку, автентифікацію користувачів, сегментацію мережі IoT-пристроїв.

Проведене дослідження підтвердило, що використання IoT-технологій у сфері «розумного будинку» є доцільним, ефективним та перспективним. Розроблений прототип показав, що навіть із доступних компонентів можливо створити надійну систему автоматизації побутових процесів, яка дозволяє економити ресурси, підвищує рівень комфорту та безпеки, а також легко масштабовується.

У подальших дослідженнях планується:

- додавання функцій машинного навчання для адаптивного керування;
- інтеграція з відновлюваними джерелами енергії (сонячні панелі);
- розробка користувацького інтерфейсу з голосовим керуванням;
- розширення системи на багатоквартирні будинки або комерційні об'єкти.
- наявні проекти про створення «Розумної пожежної частини»

Таким чином, IoT відкриває широкі можливості для розвитку інтелектуальних екосистем у повсякденному житті.

Перелік посилань:

1. Home Assistant. (n.d.). *Open source home automation that puts local control and privacy first*. https://www.home-assistant.io/
2. GitHub. (n.d.). *Smart Home Projects*. https://github.com/topics/smart-home
3. **Спосіб організації системи управління «Розумний дім»** — Семенюк В. В. (магістерська дисертація)
4. Композитний підхід до системи управління. https://ela.kpi.ua/items/b69a2158-09d4-4265-b9d0-9d6087b218c8

Єсакова В.В.,
студентка групи 125-22-1,
Гаріфулін Д.С.,
студент групи 125-22-2,
НТУ «Дніпровська політехніка»,
Дніпро, Україна

Мєшков В.І.
старший викладач каф. БІТ,
НТУ «Дніпровська політехніка»,
Дніпро, Україна

СОЦІАЛЬНА ІНЖЕНЕРІЯ В КІБЕРАТАКАХ: ПСИХОЛОГІЧНІ МЕТОДИ МАНІПУЛЯЦІЇ ТА ШЛЯХИ ПРОТИДІЇ

У роботі досліджено психологічні методи маніпуляції, що використовуються у соціально-інженерних кібератаках. Проаналізовано механізми впливу на поведінку людини, типові когнітивні упередження, що сприяють успішності атак, а також наведено приклади реальних інцидентів. Запропоновано підходи до підвищення психологічної стійкості користувачів і формування ефективних заходів протидії.

Ключові слова: соціальна інженерія, психологічні тригери, когнітивні упередження, кібератаки, поведінкова безпека.

Соціальна інженерія у контексті інформаційної безпеки визначається як сукупність методів психологічного впливу, спрямованих на отримання конфіденційних даних або доступу до інформаційних систем шляхом маніпуляції поведінкою людини. На відміну від класичних кібератак, орієнтованих на технологічні вразливості, соціально-інженерні атаки експлуатують психологічні особливості сприйняття, емоційного реагування та когнітивного мислення [1].

Науковий інтерес до цього явища зростає, оскільки саме людський фактор є визначальним у понад 70% інцидентів інформаційної безпеки (згідно з Verizon DBIR 2024). Соціальна інженерія апелює до базових соціальних інстинктів людини – довіри, авторитету, взаємності, страху або співчуття – що робить її надзвичайно ефективним інструментом злочинців. У психологічному сенсі, ефективність таких атак пояснюється використанням когнітивних упереджень – стійких систематичних помилок у сприйнятті інформації, описаних у працях Д. Канемана та Р. Чалдіні. Зловмисники активно застосовують ефект терміновості

(створення відчуття обмеженого часу для прийняття рішення), ефект авторитету (посилання на офіційні джерела або керівників), ефект дефіциту (обмежена можливість доступу), а також соціальне підтвердження (приклади дій «інших користувачів») [2; 3].

Історично одним із перших проявів масового використання емоційних тригерів став комп'ютерний черв'як ILOVEYOU (2000 рік), що розповсюджувався через електронну пошту у вигляді «листа кохання». Отримувачі відкривали вкладення, вважаючи його особистим повідомленням, після чого програма завдавала шкоди системі Windows і пересилала себе далі через адресну книгу Outlook [4]. Цей інцидент продемонстрував, що емоційна довіра до відправника є настільки сильною, що може повністю обійти технічні засоби захисту.

У сучасному цифровому середовищі соціально-інженерні атаки набувають дедалі складніших форм. Прикладом є зафіксована у 2025 році схема «Конкурс дитячого малюнка», виявлена Центром кіберзахисту НБУ. Учасників соціальних мереж закликали проголосувати за дитячі роботи, після чого їм пропонувалося перейти за посиланням, відсканувати QR-код або ввести номер телефону. Це дозволяло зловмисникам під'єднати власний пристрій до акаунта користувача та отримати доступ до його особистих даних [5]. Таким чином, шахрайство поєднувало емоційну маніпуляцію (співчуття до дітей) із технічним прийомом автентифікації через месенджер, що відображає тенденцію до появи гібридних соціально-інженерних атак.

З метою протидії соціальній інженерії необхідно формувати комплексну поведінкову безпеку, що охоплює освітні, організаційні та технічні заходи. Ключову роль відіграє психологічна підготовка користувачів – розвиток критичного мислення, навичок емоційної саморегуляції та здатності розпізнавати маніпулятивні повідомлення. Згідно з рекомендаціями NIST SP 800-50 і ENISA Cybersecurity Training Guidelines, навчання користувачів повинно проводитись на регулярній основі у формі тренінгів, моделювання фішингових ситуацій та інтерактивних курсів із кібергігієни [6; 7].

Соціальна інженерія є складним багатофакторним явищем, у якому переплітаються психологічні, соціальні та інформаційні аспекти впливу на людину. Її результативність зумовлена здатністю зловмисників використовувати когнітивні упередження, емоційні реакції та поведінкові особливості користувачів для досягнення своїх цілей. Забезпечення ефективного захисту від таких загроз потребує формування високого рівня психологічної готовності персоналу, розвитку критичного мислення та впровадження безперервних освітніх програм з кібергігієни й поведінкової безпеки.

Перелік посилань:

1. Mitnick, K. D., Simon, W. L. The Art of Deception: Controlling the Human Element of Security. – Indianapolis: Wiley, 2003. – 352 p.

2. Hadnagy, C. Social Engineering: The Science of Human Hacking. – 2nd ed. – Wiley, 2018. – 320 p.

3. Cialdini, R. Influence: Science and Practice. – 5th ed. – Pearson Education, 2009. – 272 p.

4. Software Engineering Institute, Carnegie Mellon University. CERT® Advisory CA-2000-04 Love Letter Worm [Електронний ресурс]. – 2000. – Режим доступу: https://www.sei.cmu.edu/documents/507/2000_019_001_496188.pdf (дата звернення: 12.10.2025).

5. Центр кіберзахисту Національного банку України. Шахрайська схема “Конкурс дитячого малюнка” [Електронний ресурс]. – 23.05.2025. – Режим доступу: https://cyber.bank.gov.ua/news/179 (дата звернення: 12.10.2025).

6. National Institute of Standards and Technology (NIST). Special Publication 800-50: Building an Information Technology Security Awareness and Training Program. – Gaithersburg: NIST, 2022. – 56 p.

7. European Union Agency for Cybersecurity (ENISA). Cybersecurity Training Guidelines [Електронний ресурс]. – 2023. – Режим доступу: https://www.enisa.europa.eu/ (дата звернення: 12.10.2025).

Суботенко Р.Р.,
студент групи БСДМ-63,
ННКБЗІ ДУІКТ, Київ, Україна

ПІДХОДИ ДО ЗАХИСТУ КОРПОРАТИВНОЇ ПОШТИ ОРГАНІЗАЦІЇ

Безпека електронної пошти має першорядне значення в сучасному світі. Шлюз безпеки електронної пошти Barracuda забезпечує максимальний захист ваших електронних листів, гарантуючи, що у корпоративнуелектронну пошту потраплятимуть лише безпечні та легітимні повідомлення. Завдяки використанню сучасних підходів, таких як, розширенее виявлення загроз, фільтрація спаму, запобігання втратам даних, шлюз безпеки електронної пошти Barracuda пропонує комплексне рішення для організацій будь-якого розміру.

Ключові слова: кібербезпека, захист, загрози, електронна пошта

Шлюз безпеки електронної пошти є ключовим компонентом захисту корпоративної електронної пошти. Він діє як фільтр між Інтернетом та корпоративним поштовим сервером, блокуючи потенційні загрози, такі як спам, віруси та спроби фішингу. Скануючи вхідні та вихідні електронні листи, шлюз безпеки електронної пошти гарантує, що до корпоративної поштової скриньки потраплять лише безпечні та легітимні повідомлення.

Шлюз безпеки електронної пошти Barracuda — це хмарне рішення, розроблене для захисту як вхідної, так і вихідної електронної пошти від широкого спектру ризиків, включаючи спам, віруси, черв’яків, фішингові атаки та інциденти відмови в обслуговуванні. Фільтруючи та очищуючи кожен електронний лист, перш ніж він потрапить до поштової скриньки, Barracuda забезпечує надійний захист від шкідливого контенту, гарантуючи безпеку та конфіденційність вашого спілкування.

Рис. 1. Архітектура шлюзу безпеки електронної пошти Barracuda

Barracuda використовує термін «Email Gateway Defense» для позначення хмарного (cloud-based) сервісу, який є частиною ширшого пакету «Barracuda Email Protection».

Email Gateway Defense призначено для захистує як вхідної, так і вихідної електронної пошти від сучасних атак, таких як спамів, вірусів, черв'яків, фішингу, атак типу «відмова в обслуговуванні» та загроз «нульового дня». Email Gateway Defense — це служба пропускання, яка діє як фільтр перед вашою розміщеною поштовою службою або серверами.

Email Gateway Defense надає наступні підходи щодо захисту корпоративної пошти організації:

Отримує вхідну електронну пошту від імені організації, захищаючи поштовий сервер від отримання прямих інтернет-з'єднань та пов'язаних із ними загроз.

Використовує фільтрацію контенту для виявлення та блокування небажаних електронних листів, перш ніж прийняти їхнє тіло для подальшої обробки.

Використовує засоби контролю вхідної та вихідної пошти для захисту вашої поштової інфраструктури від автоматизованого програмного забезпечення для розсилки спаму, а потім виконує подальший аналіз IP-адрес електронних листів.

Забезпечує автентифікацію відправника, таку як Sender Policy Framework (SPF), для вхідної пошти з метою перевірки відправників; застосовує політики та прогнозне профілювання відправників для визначення поведінки відправника та відхилення з'єднань та/або повідомлень від спамерів.

Використовує три рівні сканування на віруси: вірусні визначення з відкритим кодом від спільноти розробників відкритого коду, власні вірусні визначення від Barracuda Central та систему реального часу Barracuda (BRTS), яка забезпечує аналіз відбитків пальців, захист від вірусів та аналіз намірів.

Пропонує розширений захист від загроз (ATP) на основі підписки для аналізу вхідних вкладень електронної пошти в окремому захищеному хмарному середовищі з метою виявлення нових загроз.

Надсилає користувачам сповіщення про карантин та блокування контенту.

Обравши шлюз безпеки електронної пошти Barracuda як основну лінію захисту, організацію отримують намтупні *переваги*:

Шлюз безпеки електронної пошти організації захищає від загроз, що поширюються електронною поштою, таких як спам, віруси та фішингові атаки.

Підвищена продуктивність досягається завдяки зменшенню кількості спаму та шкідливих електронних листів, що потрапляють електронної пошти, що дозволить співробітникам зосередитися на завданнях без відволікаючих факторів.

Запобігти витокам даних та забезпечення дотримання нормам та стандартам щодо впровадження заходів запобігання втраті даних.

Ці переваги роблять шлюз безпеки електронної пошти Barracuda важливим інструментом для організацій, які прагнуть посилити безпеку своєї електронної пошти.

Перелік посилань:
1. Шлюз безпеки електронної пошти Barracuda – URL: https://www.datalinknetworks.net/dln_blog/barracudas-email-security-gateway-your-first-line-of-defense (дата звернення: 13.10.2025).
2. Про захист шлюзу електронної пошти. – URL: https://campus.barracuda.com/product/emailgatewaydefense/ (дата звернення: 13.10.2025).

Сердюков І. В.
студент групи 125-22-1,
НТУ «Дніпровська політехніка»,
Дніпро, Україна

Мєшков В.І.
старший викладач каф. БІТ,
НТУ «Дніпровська політехніка»,
Дніпро, Україна

АНАЛІЗ КОНЦЕПЦІЇ ZERO TRUST ЯК ОСНОВИ СУЧАСНОЇ СТРАТЕГІЇ ЗАХИСТУ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Кіберзагрози постійно ускладнюються, а традиційні моделі захисту не завжди забезпечують належний рівень безпеки. Колишня впевненість, що внутрішня мережа є безпечною за замовчуванням, втрачає актуальність у сучасному цифровому середовищі, де доступ до даних і сервісів можливий з будь-якої точки світу. На зміну класичним периметровим підходам приходить концепція Zero Trust («нульова довіра»), відповідно до якої кожен запит вважається потенційно підозрілим і підлягає перевірці. Безпека перестає бути одноразовою процедурою контролю на вході, натомість перетворюється на безперервний процес аутентифікації, авторизації та моніторингу кожного користувача, пристрою та застосунку.

Ключові слова: Zero Trust, нульова довіра, кібербезпека, найменші привілеї, мікросегментація, багато-факторна автентифікація.

Упродовж останніх років зростає кількість віддалених працівників, активніше використовуються хмарні сервіси, з’являється велика кількість мобільних і IoT-пристроїв. Такі зміни зробили традиційну модель «замок і рів» недостатньою, оскільки компрометація одного вузла дозволяє зловмиснику рухатися мережею латерально та отримувати ширший доступ до ресурсів. Тому довіра, заснована лише на перебуванні користувача всередині корпоративного периметра, більше не працює. Концепція Zero Trust заперечує будь-яку неявну довіру і вимагає перевірки кожної взаємодії незалежно від джерела запиту [1; 2].

Zero Trust розглядає ідентичність користувача та пристрою, контекст сесії й чутливість даних як основу для прийняття рішення про дозвіл, обмеження або заборону доступу. Відповідно до стандарту NIST SP 800-207, акцент переноситься з мережевого периметра на ідентичності, пристрої, застосунки та

дані, а політики доступу мають бути динамічними та орієнтованими на ризик [1]. У сучасних рекомендаціях наголошується на принципі assume breach, який передбачає, що кожен запит необхідно автентифікувати, авторизувати й шифрувати, оскільки мережа розглядається як потенційно скомпрометована [2].

З позиції підприємства Zero Trust передбачає усунення неявної довіри шляхом використання багато-факторної автентифікації (MFA), реалізації принципу найменших привілеїв із регулярним переглядом прав доступу, мікросегментації мережі для локалізації інцидентів і обмеження горизонтального переміщення зловмисників у внутрішньому середовищі, а також безперервного моніторингу активності користувачів і пристроїв. Аналітика подій та автоматизована реакція на інциденти дозволяють оперативно виявляти та блокувати підозрілу поведінку. Політики доступу в системі Zero Trust враховують не лише роль користувача, а й його місцезнаходження, стан пристрою, рівень ризику та чутливість запитуваних даних. [1; 2].

Архітектурно Zero Trust реалізується через Policy Decision Point (PDP) і Policy Enforcement Point (PEP) – точки прийняття та виконання політик, які наближені до ресурсу, що захищається [1]. Практичне впровадження моделі починається з інвентаризації активів і визначення чутливих даних, які потребують підвищеного рівня захисту. Наступними кроками є створення єдиної системи ідентичності (IAM, SSO), активація MFA для всіх користувачів, мінімізація привілеїв, впровадження сегментації та формування динамічних політик доступу. Важливо також перейти від концепції мережевого доступу до Zero Trust Network Access (ZTNA), яка надає користувачеві лише необхідні застосунки, зменшуючи площу атаки порівняно з традиційними VPN-рішеннями [3].

Технологічно концепція Zero Trust спирається на широкий набір рішень:

IAM і SSO – централізоване управління обліковими записами;

PAM – контроль привілейованих користувачів;

SIEM, UEBA і SOAR – моніторинг, аналіз поведінки та автоматизація реагування;

EDR/XDR – захист кінцевих точок;

CASB – контроль хмарних сервісів;

DLP – запобігання витокам даних.

Мережа при цьому поділяється на сегменти, а внутрішній трафік шифрується, що дозволяє реалізувати політики в реальному часі за результатом багатофакторної оцінки ризику [1; 2].

Попри очевидні переваги, впровадження Zero Trust супроводжується низкою викликів. По-перше, потрібні значні інвестиції у модернізацію інфраструктури та перебудову мережевої архітектури. По-друге, у великих розподілених середовищах необхідно враховувати затримки, які виникають через постійні перевірки, і завчасно планувати масштабування систем авторизації. По-третє, інтеграція Zero Trust із наявними системами вимагає поетапного підходу та адаптації. Не менш важливим залишається людський

фактор: без навчання персоналу постійні перевірки можуть сприйматися як бюрократія й викликати опір [4].

З огляду на це, впровадження Zero Trust доцільно здійснювати поступово. На початковому етапі варто зосередитися на швидких результатах – впровадженні MFA, усуненні надлишкових прав, базовій сегментації критичних зон. Наступними кроками мають бути формування централізованих політик доступу, розширення моніторингу подій, автоматизація реагування та інтеграція хмарних середовищ до єдиної моделі безпеки. Такий підхід дозволяє зменшити площу атаки, підвищити керованість доступом, скоротити час реагування на інциденти й забезпечити відповідність міжнародним стандартам інформаційної безпеки.

Розвиток концепції Zero Trust відображає еволюцію підходів до кіберзахисту – від захисту периметра до моделі, орієнтованої на ідентичність, дані та контекст взаємодії. Така архітектура дозволяє організаціям створювати динамічні системи контролю доступу, що реагують на зміну ризиків у реальному часі. Інтеграція принципів нульової довіри з технологіями моніторингу, аналітики та автоматизації формує цілісну екосистему безпеки, у якій кожна дія перевіряється, а довіра вибудовується поступово. У перспективі саме Zero Trust стане базовою моделлю корпоративного кіберзахисту, здатною забезпечити стійкість інформаційних систем до загроз майбутнього.

Перелік посилань:

1. National Institute of Standards and Technology (NIST). Special Publication 800-207: Zero Trust Architecture [Електронний ресурс]. – Gaithersburg: NIST, 2020. – 50 p. – Режим доступу: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf (дата звернення: 12.10.2025).
2. Microsoft Learn. What is Zero Trust? [Електронний ресурс]. – 2024. – Режим доступу: https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-overview (дата звернення: 12.10.2025).
3. Zscaler. How Does ZTNA Replace Traditional VPN Solutions? [Електронний ресурс]. – 2024. – Режим доступу: https://www.zscaler.com/zpedia/how-does-ztna-replace-traditional-vpn-solutions (дата звернення: 12.10.2025).
4. AgileBlue. Zero-Trust Architecture: Implementation and Challenges [Електронний ресурс]. – 2024. – Режим доступу: https://agileblue.com/resource/zero-trust-architecture-implementation-and-challenges-2/ (дата звернення: 12.10.2025).

Ісаєнко І.І.,
студент групи БСДМ-62,
ННКБЗІ ДУІКТ, Київ, Україна

УПРАВЛІННЯ МОБІЛЬНИМИ ПРИСТРОЯМИ В СУЧАСНОМУ КОРПОРАТИВНОМУ СЕРЕДОВИЩІ: ВИКЛИКИ СЬОГОДЕННЯ ТА СТРАТЕГІЇ ПОДОЛАННЯ

Широке використання мобільних пристроїв в організаціях дозволяє працівникам бути більш продуктивними, дозволяючи їх залишатися на зв'язку та працювати з корпоративними даними з будь-якої точки світу. Проте, ця революція мобільності породила комплексні та багатогранні виклики у сфері управління та кібербезпеки. Сучасна організація стоїть перед дилемою: як максимально використати переваги мобільності, не скомпрометувавши при цьому цілісність, конфіденційність та доступність критично важливих корпоративних даних.

Ключові слова: кібербезпека, управління, мобільні пристрої, BYOD

Стрімкий розвиток інформаційних технологій і тотальна мобільність робочої сили перетворили мобільні пристрої — смартфони, планшети, ноутбуки — на невід'ємний інструмент ведення бізнесу. Ключова проблема в управління мобільними пристроями полягає у необхідності встановити єдиний, надійний та гнучкий механізм контролю над усім різноманіттям мобільних кінцевих точок, що функціонують у мережі. Цей виклик посилюється явищем BYOD (Bring Your Own Device – використовуй власний пристрій), коли особисті гаджети співробітників отримують доступ до корпоративних ресурсів. У таких умовах розмивається межа між особистим та робочим простором, що створює значний ризик витоку даних, несанкціонованого доступу та інфікування корпоративної мережі шкідливим програмним забезпеченням. Традиційні методи захисту периметра стають неефективними перед такою децентралізації.

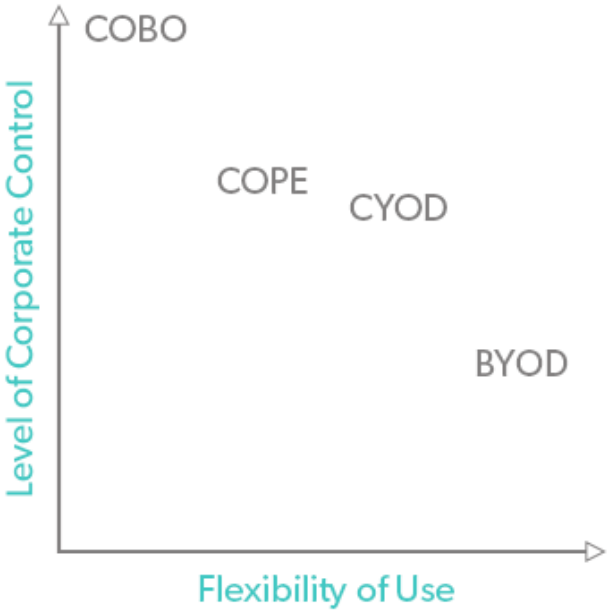

Рис. 1. Концепції використання мобільних пристроїв

Навіть у випадку використання корпоративних пристроїв (COPE – Corporate-Owned, Personally-Enabled) виникає потреба в балансі між безпекою та зручністю користувача. Занадто суворі політики можуть викликати

незадоволення персоналу та знизити продуктивність, тоді як послаблення контролю прямо веде до зростання вразливостей. Серед конкретних технічних та організаційних проблем слід виділити:

– забезпечення актуальності оновлень операційних систем та додатків; керування різними операційними системами (iOS, Android, Windows) з їх унікальними вимогами до безпеки;

– забезпечення відповідності нормативним вимогам, таким як GDPR чи HIPAA;

– необхідність віддаленого стирання даних у разі втрати або крадіжки пристрою.

– навчання персоналу основам кібергігієни, оскільки людський фактор часто є найслабшою ланкою в системі захисту.

Шляхи вирішення цієї комплексної проблеми лежать у площині стратегічного впровадження інтегрованих систем управління та багаторівневого підходу до безпеки. Фундаментом є впровадження спеціалізованих рішень для управління мобільними пристроями (Mobile Device Management, MDM) або, що більш прогресивно, уніфікованого управління кінцевими точками (Unified Endpoint Management, UEM).

Рішення UEM/MDM дозволяє централізовано застосовувати політики безпеки, незалежно від типу пристрою чи операційної системи. Це включає: примусове встановлення складних паролів та шифрування даних на пристрої; контроль над встановленням додатків та доступом до корпоративних ресурсів; віддалену конфігурацію параметрів мережі та пошти; а також функцію геозонування та віддаленого блокування або повного очищення даних у критичних ситуаціях.

Особлива увага має бути приділена методології управління, яка враховує специфіку використання. У сценаріях BYOD ключовим є концепція контейнеризації або розділення даних. Це означає створення захищеного, ізольованого робочого простору на особистому пристрої, який містить лише корпоративні дані та програми. Це дозволяє IT-відділу керувати та захищати виключно корпоративний сегмент, не втручаючись в особисте життя співробітника та не порушуючи його конфіденційності.

Перелік посилань:

3. Коцепції використання мобільних пристроїв – URL: https://www.datalinknetworks.net/dln_blog/barracudas-email-security-gateway-your-first-line-of-defense (дата звернення: 13.10.2025).

4. What is mobile device management (MDM)? – URL: https://www.techtarget.com/searchmobilecomputing/definition/mobile-device-management (дата звернення: 13.10.2025).

Тітова А.М.
студентка групи 125-22-2,
НТУ «Дніпровська політехніка»,
Дніпро, Україна

Мєшков В.І.
старший викладач каф. БІТ,
НТУ «Дніпровська політехніка»,
Дніпро, Україна

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ КВАНТОВИХ ТЕХНОЛОГІЙ У РОЗВИТКУ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Стрімкий розвиток квантових обчислень ставить під сумнів надійність класичних криптографічних систем, зокрема RSA та ECC, що десятиліттями слугували основою захисту даних. Потенційна здатність квантових комп'ютерів розв'язувати задачі факторизації та дискретного логарифмування створює нові виклики для сфери інформаційної безпеки та потребує переходу до квантово-стійких рішень. Водночас квантові технології відкривають можливості для створення принципово нових підходів до захисту інформації – від квантової криптографії до генерації істинно випадкових чисел. Мета – окреслити потенціал і перспективи застосування квантових технологій у формуванні майбутніх систем безпеки даних.

Ключові слова: квантові обчислення, квантова криптографія, постквантова криптографія, квантовий розподіл ключів, QRNG, інформаційна безпека.

Алгоритм Шора показав, що на квантовому комп'ютері задачі факторизації та дискретного логарифма розв'язуються за поліноміальний час, що фундаментально підриває стійкість RSA, класичного Diffie–Hellman та еліптичної криптографії за умови появи масштабних, низькопохибкових квантових пристроїв. Для симетричних схем алгоритм Гровера теоретично забезпечує квадратичне прискорення повного перебору (з 2^n до $\sim 2^{n/2}$), тож «ефективна» безпека AES-256 наближається до рівня ~128-бітного класичного шифрування. Водночас NIST наголошує: з огляду на ресурсні вимоги та складність паралелізації практичний вплив Гровера може бути обмеженим, і AES-128, ймовірно, залишатиметься безпечним упродовж десятиліть [1-3].

Поряд із цими ризиками квантові технології формують нову парадигму безпеки. Найбільш зрілим напрямом є квантова криптографія, зокрема квантовий розподіл ключів (QKD). Протокол BB84, розроблений Беннетом і Брассаром у 1984 році, базується на принципі неможливості клонування квантових станів: будь-яка спроба перехоплення сигналу змінює його параметри, що дає змогу зафіксувати факт втручання [4].

На практиці такі системи вже впроваджуються у Південній Кореї – компанією ID Quantique спільно зі SK Broadband створено національну мережу квантового зв'язку довжиною понад 800 км; у Європейському Союзі реалізується проєкт EuroQCI, спрямований на розбудову єдиної європейської квантової інфраструктури; у США – програма National Quantum Initiative фінансує створення експериментальних квантових каналів зв'язку між науковими та державними установами [5; 6].

Другий ключовий напрям – постквантова криптографія (Post-Quantum Cryptography, PQC), тобто алгоритми, стійкі до атак квантових комп'ютерів і сумісні з класичною інфраструктурою. Її головна перевага полягає в тому, що перехід до постквантових рішень не вимагає створення спеціальних оптичних мереж, а лише оновлення криптографічних бібліотек і протоколів.

13 серпня 2024 року Національний інститут стандартів і технологій США (NIST) затвердив три перші федеральні стандарти FIPS:

FIPS 203 (ML-KEM) – алгоритм обміну ключами на основі граткової криптосистеми CRYSTALS-Kyber, що поєднує високу швидкодію та низьку латентність;

FIPS 204 (ML-DSA) – цифровий підпис CRYSTALS-Dilithium, який використовує математичні властивості граток для формування квантово-стійких підписів;

FIPS 205 (SLH-DSA) – алгоритм SPHINCS+, що ґрунтується на хеш-функціях і не залежить від складних математичних проблем.

У 2025 року NIST додатково обрав HQC (Hamming Quasi-Cyclic) як резервний алгоритм для обміну ключами (KEM), що базується на кодовій криптографії [7; 8].

Запровадження цих стандартів формує нормативну основу для глобального переходу на квантово-стійкі протоколи у державному, фінансовому та корпоративному секторах. На відміну від QKD, PQC може бути масштабовано через звичайні мережеві протоколи – TLS, VPN, SSH – без зміни фізичної інфраструктури. Саме тому NIST рекомендує гібридний підхід, який поєднує класичні (RSA, ECC) та постквантові алгоритми, забезпечуючи криптоагільність і плавну міграцію в перехідний період [3].

Крім того, у сфері криптографії розвиваються квантові генератори випадкових чисел (QRNG), які використовують непередбачуваність квантових процесів для формування ключів з істинною ентропією. Також досліджуються квантові сенсори, здатні фіксувати втручання в канали зв'язку на рівні окремих фотонів. У перспективі передбачається їх інтеграція з системами SIEM та SOC для створення гібридних інтелектуальних платформ моніторингу безпеки [9; 10].

Попри величезний потенціал, впровадження квантових технологій залишається складним завданням через високу вартість обладнання, потребу в оптичній інфраструктурі, обмежену стабільність кубітів і вимоги до контролю шуму. Тому сучасні системи захисту перебувають у стані криптографічного переходу, коли класичні та постквантові методи співіснують у гібридному форматі.

Висновок.

Квантові технології становлять водночас виклик і можливість для розвитку систем інформаційної безпеки. Алгоритм Шора став передумовою перегляду класичних криптографічних стандартів, тоді як розвиток квантової криптографії, постквантових алгоритмів та генераторів випадкових чисел формує нову парадигму цифрового захисту. Прийняття NIST стандартів FIPS 203–205 і HQC у 2024–2025 роках заклало основу для глобальної стратегії переходу до квантово-

стійких протоколів, що є ключовим напрямом забезпечення кібербезпеки у найближчому десятилітті.

Перелік посилань:

1. Shor, P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer [Електронний ресурс] // arXiv:quant-ph/9508027. – Режим доступу: https://arxiv.org/abs/quant-ph/9508027 (дата звернення: 12.10.2025).

2. Fortinet. Shor's and Grover's Algorithms [Електронний ресурс]. – Режим доступу: https://www.fortinet.com/resources/cyberglossary/shors-grovers-algorithms (дата звернення: 12.10.2025).

3. National Institute of Standards and Technology (NIST). Post-Quantum Cryptography: FAQs [Електронний ресурс]. – Режим доступу: https://csrc.nist.gov/projects/post-quantum-cryptography/faqs (дата звернення: 12.10.2025).

4. Bennett, C. H., Brassard, G. Quantum Cryptography: Public Key Distribution and Coin Tossing [Електронний ресурс] // arXiv:2003.06557. – Режим доступу: https://arxiv.org/abs/2003.06557 (дата звернення: 12.10.2025).

5. European Commission. European Quantum Communication Infrastructure (EuroQCI) [Електронний ресурс]. – Режим доступу: https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci (дата звернення: 12.10.2025).

6. ID Quantique. Nation-wide Quantum-Safe Key Distribution Network in South Korea [Електронний ресурс]. – Режим доступу: https://www.idquantique.com/quantum-safe-security/nation-wide-quantum-safe-key-distribution-network-in-south-korea/ (дата звернення: 12.10.2025).

7. National Institute of Standards and Technology (NIST). Announcing Approval of Three Federal Information Processing Standards (FIPS) for Post-Quantum Cryptography, 13.08.2024 [Електронний ресурс]. – Режим доступу: https://csrc.nist.gov/news/2024/postquantum-cryptography-fips-approved (дата звернення: 12.10.2025).

8. National Institute of Standards and Technology (NIST). NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption, 11.03.2025 [Електронний ресурс]. – Режим доступу: https://www.nist.gov/news-events/news/2025/03/nist-selects-hqc-fifth-algorithm-post-quantum-encryption (дата звернення: 12.10.2025).

9. Herrero-Collantes, M., Garcia-Escartin, J. C. Quantum Random Number Generators // Reviews of Modern Physics. – 2017. – Vol. 89. – Article 015004. – DOI: 10.1103/RevModPhys.89.015004.

10. Degen, C. L., Reinhard, F., Cappellaro, P. Quantum Sensing // Reviews of Modern Physics. – 2017. – Vol. 89. – Article 035002. – DOI: 10.1103/RevModPhys.89.035002.

Денисов Я.Д.
студент групи 125-22-4,
НТУ «Дніпровська політехніка»,
Дніпро, Україна

Мєшков В.І.
старший викладач каф. БІТ,
НТУ «Дніпровська політехніка»,
Дніпро, Україна

КІБЕРГІГІЄНА ЯК ІНСТРУМЕНТ МІНІМІЗАЦІЇ РИЗИКІВ ЛЮДСЬКОГО ФАКТОРУ В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ПІДПРИЄМСТВА

У роботі досліджено роль кібергігієни як одного з ключових інструментів мінімізації ризиків, пов'язаних із людським фактором у сфері інформаційної безпеки підприємства. Проаналізовано сучасні тенденції використання навчальних платформ і симуляцій соціальної інженерії, розглянуто приклади інтерактивних підходів до підвищення цифрової обізнаності працівників. Обґрунтовано необхідність інтеграції кібергігієни у систему управління інформаційною безпекою підприємства для підвищення його кіберстійкості.

Ключові слова: кібергігієна, цифрова обізнаність, людський фактор, соціальна інженерія, кібербезпека, інформаційна безпека.

У сучасному цифровому середовищі, де інформаційні технології стали базовим елементом бізнес-процесів, питання кібербезпеки набуває особливого значення. Незважаючи на вдосконалення технічних систем захисту, головною причиною більшості інцидентів залишається людський фактор. За даними Verizon Data Breach Investigations Report (2025) [1, с. 39], близько 17% підтверджених витоків інформації у базі даних VERIS були пов'язані з використанням методів соціальної інженерії. За інформацією цього ж джерела, співробітники, що отримали тренування з кібергігієни, в чотири рази частіше за непідготовлених користувачів доповідають про підозрілі надходження. Однак відсоток натискання на шкідливі листи майже не відрізняється незалежно від отримання тренування [1, с. 48-49]. Це свідчить, що маніпулювання поведінкою людини є одним із найпоширеніших векторів атак, а формування навичок кібергігієни – критичним елементом системи інформаційної безпеки, що досі не досяг стійкого запровадження у багатьох організаціях по всьому світу.

Кібергігієна охоплює сукупність знань, навичок і поведінкових звичок, спрямованих на зниження ризиків, пов'язаних з помилками користувачів, несанкціонованими діями чи неуважністю персоналу. Вона є не лише частиною культури інформаційної безпеки, а й дієвим інструментом управління ризиками, спричиненими людським фактором. Людина, яка володіє базовими навичками цифрової безпеки, здатна розпізнати фішингову атаку, створити надійний пароль, уникнути переходу за підозрілими посиланнями та обережно працювати з конфіденційними даними.

Кіберзлочинці усвідомлюють, що використати недосвідченість або необачність людини значно простіше, ніж обійти технічні системи захисту. Тому дедалі більшого поширення набувають атаки, засновані на соціальній інженерії:

фішинг, крадіжка особистості, підбір паролів методами OSINT або атаки типу «генерального директора». Для мінімізації цих ризиків кібергігієна виконує роль профілактичного інструменту, що формує у працівників підприємства критичне мислення та обережність у цифровому середовищі.

Ефективна кібергігієна передбачає не лише ознайомлення з базовими правилами безпеки, а й відпрацювання поведінкових сценаріїв. Одним із практичних методів є інтерактивні симуляції атак, які дозволяють працівникам навчатися на власних помилках у контрольованому середовищі. Прикладом таких рішень є платформи Nimblr [2] та Boxphish [3], що імітують поширені типи атак соціальної інженерії, зокрема фішингові листи або повідомлення у месенджерах. Коли користувач натискає на підроблене посилання чи відкриває вкладення, система не завдає шкоди, а натомість надає миттєвий зворотний зв'язок із поясненням, як слід було діяти. Це дозволяє закріпити правильну поведінкову реакцію і підвищити обізнаність на практичному рівні.

Подібні методики застосовуються у корпоративних середовищах різного масштабу шляхом інтеграції у внутрішню IT-інфраструктуру. Вони забезпечують відстеження прогресу користувачів і дозволяють адаптувати навчальний матеріал до специфіки діяльності окремих підрозділів. За результатами аналізу даних симуляцій можливо визначити найвразливіші категорії працівників і коригувати навчальні пріоритети. Таким чином, кібергігієна стає елементом системи управління ризиками, а не лише освітньою ініціативою.

Окрему увагу слід приділити концепції автономних навчальних модулів, що функціонують поза межами робочої інформаційної системи. Такий підхід, запропонований у практиках Infosec [4], зменшує ризик втоми від симуляцій у реальному робочому середовищі, забезпечує безпечне навчання та легку адаптацію під нові типи загроз. У результаті працівники набувають досвіду взаємодії з типовими сценаріями атак, що підвищує загальну кіберстійкість підприємства.

Важливо підкреслити, що ефективність навчання напряму залежить від системності його впровадження. Кібергігієна має бути не одноразовою кампанією, а постійним процесом у межах політики інформаційної безпеки підприємства, і є невід'ємною складовою сучасної системи управління інформаційною безпекою. Її впровадження дозволяє не лише підвищити рівень цифрової грамотності працівників, а й суттєво знизити вразливості, спричинені людським фактором.

Перелік посилань:

1. Verizon. 2025 Data Breach Investigations Report [Електронний ресурс]. – Режим доступу: https://www.verizon.com/business/resources/Tfdb/reports/2025-dbir-data-breach-investigations-report.pdf (дата звернення: 09.10.2025).

2. Nimblr. Офіційний вебсайт [Електронний ресурс]. – Режим доступу: https://nimblrsecurity.com/ (дата звернення: 09.10.2025).

3. Boxphish. Офіційний вебсайт [Електронний ресурс]. – Режим доступу: https://www.boxphish.com/ (дата звернення: 09.10.2025).

4. Infosec. Офіційний вебсайт [Електронний ресурс]. – Режим доступу: https://www.infosecinstitute.com/ (дата звернення: 09.10.2025).

Кириченко О.А.
студент групи 125-22-2,
НТУ «Дніпровська політехніка»,
Дніпро, Україна

Мєшков В.І.
старший викладач каф. БІТ,
НТУ «Дніпровська політехніка»,
Дніпро, Україна

МЕТОДИ ВИЯВЛЕННЯ ТА ПРОТИДІЇ АТАКАМ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ В СИСТЕМАХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЙ

У роботі розглянуто соціальну інженерію як одну з провідних загроз інформаційній безпеці сучасних організацій. Визначено основні методи її реалізації, проаналізовано тенденції розвитку та наведено приклад фішингової атаки з використанням елементів соціальної маніпуляції. Визначено ефективні заходи протидії на технічному, організаційному та поведінковому рівнях, проведено оцінку їх взаємодії в межах концепції Zero Trust.

Ключові слова: соціальна інженерія, кібербезпека, фішинг, людський фактор, інформаційна безпека, Zero Trust.

Інформаційна безпека сучасних організацій формується на основі технічних, адміністративних та поведінкових компонентів. Проте досвід останніх років свідчить, що вирішальним чинником залишається людський фактор. Незалежно від рівня технічного захисту, більшість порушень інформаційної безпеки відбувається внаслідок маніпулювання довірою або необізнаністю співробітників. За даними звіту Verizon Data Breach Investigations Report [2], понад 70 % кібератак мають соціально-інженерне походження, що підтверджує актуальність розроблення дієвих методів їх виявлення та нейтралізації.

Соціальна інженерія – це цілеспрямований психологічний вплив на людину з метою отримання конфіденційних даних або доступу до інформаційних систем. На відміну від технічних атак, вона орієнтована не на програмні вразливості, а на когнітивні та поведінкові особливості користувачів. До найпоширеніших методів належать фішинг, цільовий фішинг (spear phishing), шахрайство з використанням підробленої особи керівника (CEO fraud), приманка (baiting) та тайлгейтинг, тобто несанкціоноване фізичне проникнення до захищеної зони. Такі атаки супроводжуються психологічним тиском, створенням відчуття терміновості або фальшивої авторитетності.

Сучасна соціальна інженерія еволюціонує разом із розвитком технологій. Застосування штучного інтелекту та алгоритмів автоматизованого створення текстів забезпечує зловмисникам можливість формувати повідомлення, які максимально імітують мовний стиль керівників або колег [3]. Технології

deepfake дозволяють підроблювати голосові та відео повідомлення, що значно ускладнює процес розпізнавання обману. Збір попередньої інформації про потенційну жертву здійснюється через відкриті джерела (OSINT), соціальні мережі та публічні звіти, що підвищує рівень достовірності фішингових кампаній.

Показовим прикладом є цілеспрямована фішингова атака на фінансовий відділ компанії. Зловмисник створює домен, схожий на офіційний, та надсилає електронний лист нібито від керівника із проханням здійснити терміновий платіж постачальнику. Психологічний тиск, брак часу та звичка довіряти посадовим інструкціям спонукають співробітника виконати запит без перевірки достовірності відправника. Такі інциденти можуть призвести до значних фінансових втрат та компрометації репутації організації.

Ефективна протидія подібним атакам можлива лише за умови реалізації багаторівневого підходу. На технічному рівні дієвими є механізми багатофакторної автентифікації, перевірки достовірності електронної пошти (SPF, DKIM, DMARC), впровадження систем поведінкового аналізу користувачів (UEBA) та централізованого моніторингу подій безпеки за допомогою SIEM-рішень. Організаційний рівень передбачає впровадження процедур подвійного підтвердження фінансових операцій, внутрішніх політик реагування на інциденти відповідно до ISO/IEC 27035 та систем управління інформаційною безпекою за стандартом ISO/IEC 27001 [3]. Поведінковий рівень базується на регулярному навчанні персоналу, симуляціях фішингових атак і розвитку корпоративної культури безпеки.

На практиці комплексна система протидії передбачає послідовну взаємодію всіх рівнів. У наведеному прикладі атаки фільтри SPF/DKIM/DMARC блокують лист із підробленого домену, SIEM-система фіксує аномальну активність користувача, а політика подвійного підтвердження платежів унеможливлює несанкціонований переказ коштів. Навчений співробітник, своєю чергою, ідентифікує підозріле повідомлення та інформує службу безпеки, що дозволяє зупинити атаку ще на ранньому етапі. Така інтеграція технічних, організаційних і поведінкових заходів демонструє високу ефективність комплексного підходу до управління ризиками.

Оцінка результативності існуючих методів свідчить, що ізольоване застосування окремих засобів не гарантує повного захисту. Технічні інструменти не враховують людський чинник, а навчання без належної політики та контролю не забезпечує системності. Відповідно, ключовим напрямом розвитку є поєднання технологічних рішень, чітких регламентів і підвищення обізнаності користувачів.

Дослідження Canadian Centre for Cyber Security [4] підтверджують, що регулярне навчання персоналу та проведення фішингових тестів зменшують кількість успішних атак удвічі. Подальше підвищення ефективності можливе шляхом упровадження принципів Zero Trust, за яких кожна дія користувача або процесу підлягає перевірці незалежно від внутрішнього статусу довіри. Це

формує нову модель безпеки, у якій не існує «довірених зон», а автентифікація і моніторинг відбуваються безперервно.

Узагальнюючи результати дослідження, можна зробити висновок, що соціальна інженерія поєднує психологічні методи впливу та кіберзлочинні технології, і тому становить загрозу навіть для організацій із високим рівнем технічного захисту. Ефективна протидія передбачає впровадження комплексних систем, які інтегрують технічні засоби, організаційні процедури та навчання персоналу. Використання аналітичних платформ, алгоритмів штучного інтелекту, поведінкового аналізу користувачів і автоматизованих систем оцінки ризиків створює передумови для формування гнучких і адаптивних систем кіберзахисту, здатних ефективно протидіяти динамічним загрозам інформаційній безпеці.

Перелік посилань:

1. National Institute of Standards and Technology (NIST). Social Engineering. URL: https://csrc.nist.gov (дата звернення: 07.10.2025).

2. Verizon. 2024 Data Breach Investigations Report. URL: https://www.verizon.com/business/resources/reports/dbir/ (дата звернення: 07.10.2025).

3. European Union Agency for Cybersecurity (ENISA). Threat Landscape Reports. URL: https://www.enisa.europa.eu (дата звернення: 07.10.2025).

4. Canadian Centre for Cyber Security. Civil Infrastructure Guidance. URL: https://www.cyber.gc.ca (дата звернення: 07.10.2025).

Рудик О.Ф.
студентка групи 125-22-2,
НТУ «Дніпровська політехніка»,
Дніпро, Україна

Мєшков В.І.
старший викладач каф. БІТ,
НТУ «Дніпровська політехніка»,
Дніпро, Україна

МЕТОДИ ВИЯВЛЕННЯ ТА ПРОТИДІЇ ФІШИНГОВИМ АТАКАМ У КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Фішинг є одним із найпоширеніших та найнебезпечніших видів кібератак, який продовжує залишатися серйозною загрозою для корпоративних інформаційних систем. Метою цієї роботи є дослідження сучасних методів виявлення й протидії фішинговим атакам у корпоративному середовищі, а також визначення ролі технологічних та поведінкових факторів у формуванні комплексної системи захисту.

Ключові слова: фішинг, кібербезпека, корпоративний захист, штучний інтелект, захист даних.

У сучасну цифрову епоху фішинг залишається основним інструментом кіберзлочинців, спрямованим на викрадення конфіденційної інформації, облікових даних та фінансових ресурсів. За даними аналітичних звітів за 2024 рік, понад 70% компаній у світі стикалися з фішинговими атаками, що спричинило мільярдні збитки та численні порушення роботи бізнес-процесів [1]. Висока ефективність цього виду атак зумовлена не лише технічними вразливостями, а насамперед людським фактором – довірою, необережністю або поспіхом користувачів.

Фішингові кампанії можуть мати різні форми: масові розсилки з фальшивими повідомленнями, цільові атаки на конкретних працівників (spear phishing), фішинг через SMS (smishing), дзвінки (vishing) або соціальні мережі. У багатьох випадках такі атаки імітують повідомлення від відомих компаній або внутрішніх служб підтримки, що створює ілюзію легітимності та підвищує ймовірність успішного обману.

Для ефективної протидії фішингу сучасні підходи поділяються на традиційні та нетрадиційні методи (рис. 1).

Традиційні методи охоплюють технічні засоби виявлення та блокування фішингових повідомлень. Серед них – контентний аналіз листів, евристичні правила, машинне та глибинне навчання, методи аналізу даних, а також системи на основі нечіткої логіки та гібридного навчання [2]. Ці підходи дозволяють автоматично визначати підозрілі ознаки: дивні домени, змінені URL, невідповідність стилю тексту або структури повідомлення.

Останні досягнення у сфері машинного навчання (ML) та штучного інтелекту (AI) значно підвищили точність виявлення фішингових атак. Алгоритми навчаються розпізнавати сотні характеристик – від мовних патернів до технічних атрибутів вебсторінок. Зокрема, методи глибинного навчання здатні виявляти навіть незначні відмінності між легітимними та підробленими сайтами, що дозволяє блокувати нові, ще не відомі види фішингових сторінок. Проте

навіть найкращі алгоритми залишаються неефективними без участі людини – користувача, який має вчасно розпізнати спробу обману.

Рис 1. Графічне представлення методів виявлення фішингових атак

Нетрадиційні методи протидії орієнтовані на людський фактор і організаційну культуру безпеки. Вони включають освітні програми, тренінги з кібергігієни, симуляції фішингових атак, створення внутрішніх політик перевірки транзакцій і комунікацій, а також використання «білих» і «чорних» списків сайтів та доменів [3]. До таких методів також належать візуальні перевірки схожості фішингових сайтів з оригінальними, моніторинг корпоративного бренду, а також застосування OSINT-платформ (AlienVault, VirusTotal) для оцінки репутації доменів, IP-адрес і цифрових сертифікатів.

Важливим аспектом є підвищення рівня обізнаності співробітників. Навчання персоналу правильній реакції на фішингові повідомлення є найефективнішим способом запобігання інцидентам. Практика проведення регулярних тренінгів і тестових кампаній, де працівники отримують навчальні «псевдофішингові» листи, дозволяє зміцнити навички розпізнавання загроз і підвищити стійкість до маніпуляцій. Відповідно до рекомендацій NIST SP 800-50, розвиток інформаційної культури та критичного мислення серед працівників має бути невід’ємною частиною корпоративної стратегії кіберзахисту.

Окрему загрозу становить використання штучного інтелекту з боку зловмисників: генерація фішингових текстів через великі мовні моделі, підробка голосу чи відео (deepfake), автоматизоване створення фальшивих сторінок. Це змушує компанії впроваджувати адаптивні системи безпеки, здатні навчатися в режимі реального часу та виявляти нові типи фішингових схем.

Перелік посилань:

1. Кібербезпека в інформаційному суспільстві: інформаційно-аналітичний дайджест / відп. ред. О. Довгань; упоряд. О. Довгань, Л. Литвинова, С. Дорогих. – Київ: Інститут інформації, безпеки і права НАПрН України, 2024. – № 5. – 316 с.

2. Alanezi, M. Phishing Detection Methods: A Review // Technium: Romanian Journal of Applied Sciences and Technology. – 2021. – Vol. 3, No. 9. – P. 19–35. – DOI: 10.47577/technium.v3i9.4973.

3. ECS Infotech. Anti-Phishing Solutions: How to Safeguard Your Business from Cyber Threats [Електронний ресурс]. – Режим доступу: https://www.ecsinfotech.com/anti-phishing-solutions-how-to-safeguard-business-from-cyber-threats/ (дата звернення: 10.10.2025).

Нечипоренко Є.В.
студент групи БСДМ-61, ННІКБЗІ
ДУІКТ,
Київ, Україна

МОЖЛИВОСТІ UAM SYTECA ДЛЯ ВИЯВЛЕННЯ ІНЦИДЕНТІВ ВНУТРІШНЬОЇ БЕЗПЕКИ

В роботі досліджено ключові можливості платформи UAM Syteca як інструменту для проактивного виявлення інцидентів внутрішньої безпеки, спричинених інсайдерськими загрозами. UAM Syteca здійснює безперервний моніторинг поведінки користувачів і систем, застосовуючи передові методи поведінкової аналітики (UEBA) та керування привілейованим доступом (PAM). Це дозволяє ефективно виявляти аномалії, нетипові дії та потенційно ризиковані патерни, що свідчать про компрометацію облікових записів чи зловмисні наміри співробітників. Завдяки скорингу ризиків та гнучким інструментам візуалізації, Syteca значно прискорює час реагування та підвищує точність ідентифікації загроз до того, як вони призведуть до критичних наслідків.

Ключові слова: PAM, UAM, UEBA, інцидент, інсайдер, Syteca, загроза, внутрішня безпека.

На сьогоднішній день важливо не лише захищатися від зовнішніх атак, але й виявляти інциденти, пов'язані з внутрішньою безпекою. Внутрішні загрози виникають як внаслідок навмисних дій співробітників, так і через їхню необережність або несанкціонований доступ до чутливої інформації. Тому дедалі більше значення набувають рішення класу UAM (User Activity Monitoring) — це клас рішень, призначених для безперервного контролю дій користувачів на робочих станціях та серверах [1]. Основними цілями таких систем є:

— фіксація та аналіз дій користувачів (клавіатурний ввід, переглянуті файли, запуск програм тощо);

— виявлення підозрілої поведінки на основі шаблонів чи аномалій;

— забезпечення доказової бази для внутрішніх розслідувань;

— попередження витоку даних (Data Loss Prevention).

Завдяки UAM організації отримують повну прозорість у тому, як саме користувачі взаємодіють із критичними системами та даними, що дозволяє оперативно реагувати на інциденти.. Одним із таких потужних інструментів є Syteca, яка забезпечує глибокий аналіз поведінки користувачів у корпоративному середовищі. Ця система дозволяє виявляти потенційно небезпечну активність у реальному часі та створювати детальні звіти для подальшого розслідування інцидентів.

Комбінуючи різні типи клієнтів Syteca, захищається та підвищується видимість кожної частини конкретної IT-інфраструктури. Для великих розгортань команда Syteca забезпечує високу доступність і аварійне відновлення для покращення стабільності системи для задоволення вимог сегментації та ізоляції даних [2].

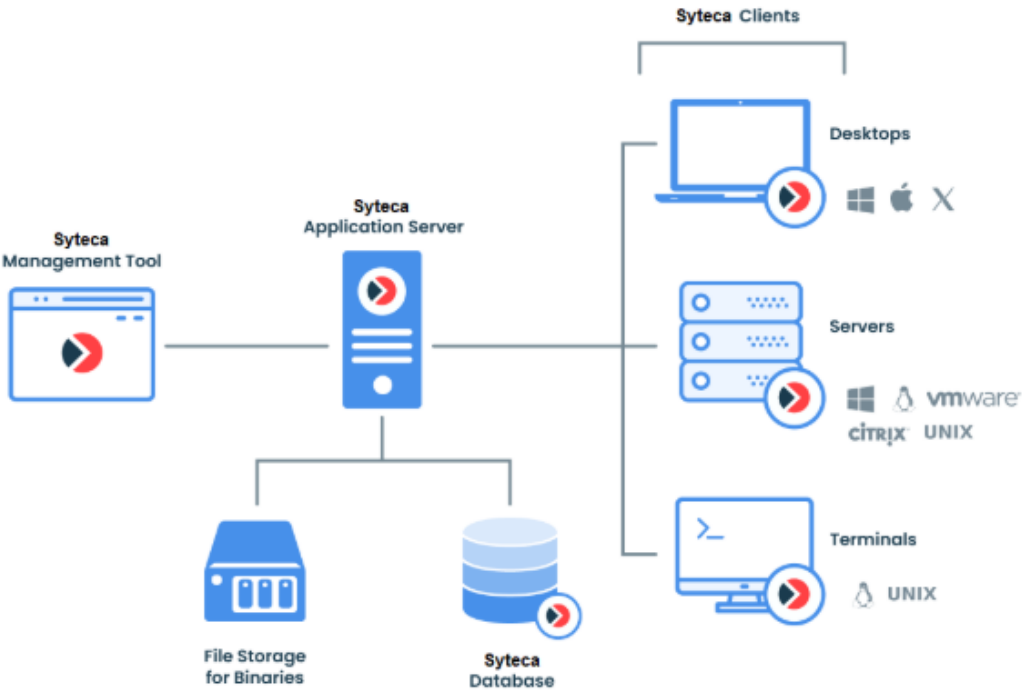

Рис. 1. Базова схема розгортання [2]

Завдяки такому розгортанню (рис. 1) досягається максимальна видимість та контроль будь-якої діяльності, що виконується в інфраструктурі, встановивши клієнт відповідного типу на кожну кінцеву точку.

В основі ефективності Syteca лежить комплексний підхід, що поєднує моніторинг, аналітику та контроль дій користувачів. Розглянемо ключові можливості платформи [1, 3].

1. Низькорівневе логування подій.

Агент системи фіксує широкий спектр подій, що включає: запуск і завершення програм; відкриття, редагування та копіювання файлів; доступ до зовнішніх носіїв (USB, CD/DVD); мережеву активність (веб-сайти, IP-з'єднання); натискання клавіш (keylogging); буфер обміну (clipboard activity).

Ці дані формують хронологічний журнал активності, доступний для перегляду у вигляді таблиць або фільтрованих списків.

2. Відеозапис сесій користувача.

Одна з ключових особливостей Syteca — створення відео-скрінкасту робочої сесії користувача. Запис включає: робочий стіл, активні вікна та взаємодію з інтерфейсом; одночасне відображення таймлайнів натискань клавіш та подій; можливість прискореного перегляду та переходу до підозрілих фрагментів.

Це дає змогу відтворити повну картину подій при розслідуванні інцидентів.

3. Поведенковий аналіз (User Behavior Analytics, UBA).

Syteca будує поведінкові профілі користувачів на основі: типових робочих годин; використовуваних програм; стандартних дій з файлами; обсягу даних, що передаються у мережу чи на носії.

Відхилення від звичного профілю автоматично позначаються як потенційно ризиковані.

4. Індикатори компрометації (Indicators of Compromise, IoC).

Система виявляє ознаки потенційної загрози, а саме: запуск інструментів адміністрування поза робочим контекстом; доступ до критичних директорій; масове копіювання файлів; спроби обходу політик безпеки.

Інциденти зберігаються в спеціальному журналі й супроводжуються тегами ризику.

5. Політики реагування та автоматичні тригери.

Syteca підтримує створення правил, які реагують на виявлену активність і застосовує певні дії згідно налаштованих політик: сповіщення (email, Telegram, Slack тощо); блокування сесії користувача; ізоляція ПК від мережі; запуск скриптів для локального реагування.

Це забезпечує як пасивний нагляд, так і активну протидію загрозам у реальному часі.

6. Формування звітів та експорт даних.

Для звітування та подальшого аналізу доступні шаблони звітів (інциденти, активність користувачів, порушення політик). Можливість експортувати дані у PDF, XLSX, CSV та відеоформати. Підтримує збереження даних для цифрової експертизи (форензики) [1, 3].

Система UAM Syteca є ефективним інструментом для виявлення інцидентів, пов’язаних із внутрішніми загрозами. Її функціональні можливості дозволяють не лише здійснювати повний моніторинг дій користувачів, але й оперативно реагувати на загрози, попереджуючи витоки даних та зловживання привілеями.

Перелік посилань:

1. Що таке Syteca?. Syteca | BAKOTECH. URL: https://syteca.bakotech.com/ua (дата звернення: 14.10.2025).

2. System Components. Syteca Knowledge Base of End-User Documentation. URL: https://docs.syteca.com/view/system-structure-and-architecture (дата звернення: 14.10.2025).

3. Liudmyla Pryimenko. Insider Threat Protection Guide: 10 Best Practices to Follow | Syteca. Syteca. URL: https://www.syteca.com/en/blog/guide-to-insider-threat-protection (дата звернення: 14.10.2025).

Шулімова Д.Д.
асистент кафедри СТКБ, ННІКБЗІ ДУІКТ,
Київ, Україна

АДАПТИВНІ ДЕРЕВА РІШЕНЬ ЯК НАДІЙНИЙ ТА ІНТЕРПРЕТОВАНИЙ ПІДХІД ДЛЯ ЕФЕКТИВНОГО ВИЯВЛЕННЯ АНОМАЛІЙ У СКЛАДНИХ НАБОРАХ ДАНИХ.

У сфері машинного навчання виявлення аномалій (Anomaly Detection) є одним із ключових завдань, яке має велике практичне значення в різних галузях — від кібербезпеки та фінансового моніторингу до промислової аналітики та охорони здоров'я. Суть цього підходу полягає у виявленні нестандартних або відхилених від звичних закономірностей об'єктів, подій чи поведінкових патернів, що можуть свідчити про потенційні загрози, збої або шахрайські дії.

Особливу складність становить застосування методів виявлення аномалій у великих та динамічних наборах даних, таких як мережевий трафік, фінансові транзакції чи показники промислових сенсорів, де обсяг інформації постійно зростає, а характеристики середовища змінюються в реальному часі. У таких умовах традиційні статистичні та евристичні методи часто демонструють обмежену ефективність, стикаючись із проблемами низької інтерпретованості, чутливості до викидів (outliers) та зниженням точності при зміні розподілу даних.

Ключові слова: машинне навчання, виявлення аномалій, Anomaly Detection, дерева рішень, Isolation Forest, інтерпретованість, пояснюваність, аномалії, outliers, ансамблеві методи.

Однією з головних проблем у виявленні аномалій є обробка великих і динамічних наборів даних та робота з шумними або рідкісними спостереженнями, які можуть спотворювати результати традиційних методів. Для подолання цих труднощів особливого значення набувають методи, засновані на деревах рішень. На відміну від традиційних статистичних або метричних алгоритмів, які часто припускають певний розподіл даних, дерева рішень роблять поступове розділення простору ознак, що дозволяє виділяти аномальні об'єкти без необхідності змінювати всю модель. Це надає алгоритму стійкість до екстремальних значень, адже поодинокі аномалії можна відокремити мінімальною кількістю поділів, не впливаючи на роботу моделі загалом. Крім того, дерева рішень легко працюють із різними типами даних — числовими та категоріальними — без необхідності їх додаткової підготовки або масштабування. Така властивість значно спрощує роботу з великими потоками даних, де швидкість обробки є критичною.

Особливої уваги заслуговує модель Isolation Forest, яка є одним із найефективніших алгоритмів для виявлення аномалій на базі дерев. Основна ідея цього методу полягає в тому, що аномальні об'єкти, які зустрічаються рідко і знаходяться в віддалених частинах простору ознак, можна відокремити швидше, ніж звичайні дані, оскільки для їхньої ізоляції потрібно менше поділів. Висока ефективність Isolation Forest забезпечується його швидкістю роботи, яка зростає пропорційно до розміру даних, і можливістю застосування у режимі реального часу. Використання ансамблю дерев робить модель більш надійною та стійкою до шуму в даних, а також дозволяє їй добре працювати на різних підмножинах ознак. На відміну від багатьох традиційних методів, що потребують нормалізації даних, Isolation Forest працює без таких припущень, що робить його

універсальним інструментом для різних завдань — від виявлення шахрайських фінансових операцій до моніторингу мережевої активності.

Ще однією важливою перевагою дерев рішень є їхня інтерпретованість, тобто зрозумілість того, як приймається рішення. Кожна гілка дерева формує правило типу «IF–THEN», що дозволяє при позначенні об’єкта як аномалії бачити, які саме ознаки та значення призвели до такого висновку. Така прозорість допомагає експертам швидше перевіряти результати моделі та приймати рішення у критичних ситуаціях. Завдяки цьому дерева рішень і моделі на їхній основі не лише ефективно виявляють аномалії, але й надають пояснення, які полегшують використання алгоритмів машинного навчання в реальних аналітичних і контрольних процесах.

Таким чином, застосування дерев рішень та моделей на їхній основі дозволяє вирішувати основні проблеми традиційних методів виявлення аномалій — забезпечувати стійкість до шуму, швидко обробляти великі потоки даних і давати зрозумілі пояснення результатів. Це робить їх особливо цінними для практичного застосування в різних високоризикових галузях, де точність і прозорість рішень є критичними.

Перелік посилань:

1. Liu F. T., Ting K. M., Zhou Z.-H. Isolation-based anomaly detection // ACM Transactions on Knowledge Discovery from Data (TKDD). 2012. Vol. 6, No. 1. Article 1. DOI: 10.1145/2133360.2133363.

2. Chandola V., Banerjee A., Kumar V. Anomaly detection: A survey // ACM Computing Surveys (CSUR). 2009. Vol. 41, No. 3. Article 15. DOI: 10.1145/1541880.1541882.

3. Li Z., Zhu Y., van Leeuwen M. A Survey on Explainable Anomaly Detection. arXiv preprint arXiv:2210.06959. 2023. [Електронний ресурс] – Режим доступу: https://arxiv.org/abs/2210.06959.

Марченко Віталій Вікторович
Доцент кафедри систем та технологій кібербезпеки, ННІКБЗІ ДУІКТ, Київ, Україна
Чайківський Віталій Володимирович
студент групи БСДМ-51, ННІКБЗІ ДУІКТ, Київ, Україна

ЯК ВІДКРИТІ ДАНІ СТАЮТЬ ЗБРОЄЮ: OSINT ТА АТАКИ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

З розвитком підходів до ініціації кібератак особливу загрозу становлять атаки соціальної інженерії, тобто ті, які спрямовані на людину. Зловмисники дедалі частіше намагаються обдурити працівників або користувачів, використовуючи психологічні маніпуляції. Розвиток відкритих інформаційних ресурсів в інтернеті дав нападникам досить дієвий інструмент підготовки атак – OSINT. Метою цієї тези є сформувати проблематику взаємозв'язку соціальної інженерії та OSINT, розкрити сутність цих понять і показати, як відкриті дані допомагають зловмисникам обирати вектор атаки.

Ключові слова: соціальна інженерія, OSINT, відкриті дані, кібербезпека.

Соціальна інженерія – спроба обманом змусити когось розкрити інформацію (наприклад, пароль), яка може бути використана для атаки на системи або мережі [1]. Іншими словами, зловмисник намагається «зламати» людину, а не компонент інформаційної інфраструктури. Для досягнення мети зловмисники встановлюють контакт із жертвою та шляхом обману завойовують її довіру. Нападники зазвичай досліджують майбутню жертву, аби знайти точки впливу і зібрати відомості, які допоможуть їм отримати потрібні відомості від особи. Після цього вони переходять до активної фази – маніпуляції. Наприклад, розігрують певний сценарій (легенду), видають себе за іншу особу чи організацію або створюють ситуацію терміновості.

До найпоширеніших методів соціальної інженерії належать: «phishing» (масове розсилання підроблених повідомлень від нібито відомих сервісів для викрадення паролів), «spear phishing» (цільові фішингові атаки на конкретних осіб, наприклад керівників – так звані «whaling»), «vishing» (телефонне шахрайство), «smishing» (шахрайські SMS), а також фізичні методи як «impersonation» (особисте видавання себе за іншу особу для проникнення, наприклад, на об'єкт) чи «tailgating» (проникнення слідом за уповноваженою особою). Усі ці підходи об'єднує використання довіри та неуважності людей. Людський фактор традиційно вважається «найслабшою ланкою» кіберзахисту, тому атаки, початковим вектором яких є методи соціальної інженерії, мають високий рівень успішності без застосування прикладних технічних методів.

OSINT (Open Source Intelligence) – визначаються як інформація, отримана шляхом збору, оцінки та аналізу загальнодоступної інформації з метою отримання відповіді на конкретне питання розвідки [2]. На відміну від закритих даних, відкриті джерела це будь-які загальнодоступні відомості, доступ до яких не обмежений власником. OSINT спочатку виник як інструмент військової та урядової розвідки, але нині широко використовується й у сфері кібербезпеки, журналістики, бізнес-аналітики та правоохоронними органами. Завдяки інтернету та соціальним медіа можливості OSINT значно розширилися, бо

сьогодні величезні масиви даних про людей, організації та події є у відкритому доступі. Типові джерела OSINT представлені на рисунку нижче.

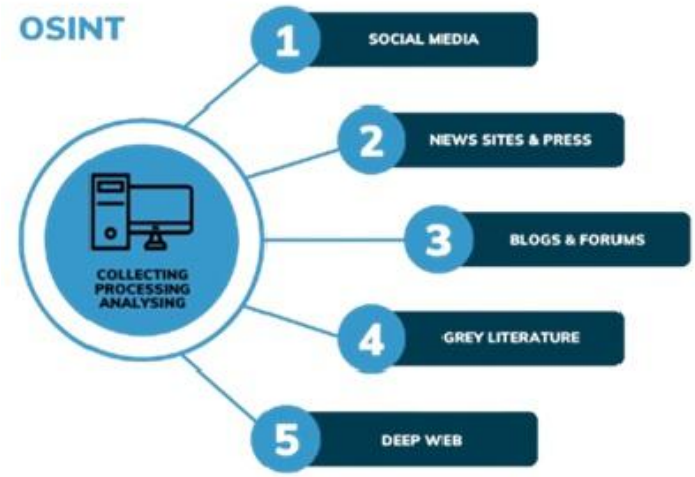

Рис. 1 – Типові OSINT-джерела [3]

• Соціальні мережі: профілі в Facebook, X (Twitter), LinkedIn, Instagram тощо; пости, фотографії, списки друзів і вподобань містять багато персональної інформації.

• Пошукові системи: Google, Bing і спеціальні техніки пошуку (наприклад, Google Dorking) для виявлення прихованих сторінок або файлів.

• Публічні реєстри та бази даних: реєстри компаній, судові рішення, витяги з урядових порталів.

• Новинні сайти й блоги: публікації в медіа можуть розкривати деталі про діяльність організації або окремих осіб.

• Форуми та об’яви: обговорення на Reddit, спеціалізованих форумах, дошках оголошень можуть містити корисну інформацію.

• IT-інфраструктура у відкритому доступі: сервіси типу Shodan чи Censys сканують інтернет на предмет відкритих портів, незахищених серверів, пристроїв IoT і показують, що видно будь-кому з мережі.

Особливу увагу нападники звертають на соціальні мережі та онлайн-профілі працівників організацій. Зокрема, через LinkedIn можна спробувати з’ясувати організаційну структуру організації та приблизне коло ключових співробітників, які мають доступ до чутливих даних. Зловмисники шукають у соціальних мережах особисті подробиці (дати народження, імена дітей, домашніх улюбленців), оскільки ці дані нерідко використовуються людьми як паролі або відповіді на секретні питання. Таким чином, відкриті профілі в соціальних мережах здатні видати нападникам підказки для підбору пароля або теми, на які можна спокусити жертву.

Важливо підкреслити, що збір інформації через OSINT є легальним, якщо дані відкриті. Однак, попри легітимність методів, зібрані відомості можуть бути використані у злочинних цілях. Саме тому OSINT-техніки стали «двосічним

мечем»: вони корисні для аналітиків та правоохоронців, але ними ж активно користуються й кіберзлочинці для підготовки атак.

Отже, з урахуванням викладеного вище, можна зробити висновок, що соціальна інженерія та OSINT утворюють досить небезпечне поєднання, яке загрожує як окремим користувачам, так і великим організаціям. Атаки, які ґрунтуються на методах соціальної інженерії використовують природну довірливість і помилки людей, а відкриті джерела інформації дають змогу зловмисникам підготувати ці атаки з високою точністю та результативністю. У тезі розкрито, що нападники активно використовують OSINT для вибору цілей, збору персональних даних і вивчення можливих шляхів проникнення. Знання, отримані з відкритих реєстрів і соціальних мереж, дозволяють створювати переконливі сценарії обману – від цілеспрямованих фішингових листів до «легенд» для телефонного шахрайства.

Найкращий підхід до захисту від таких комплексних загроз – комбінація технічних рішень та підвищення обізнаності працівників. Технічні засоби мають унеможливити несанкціонований доступ (міжмережеві екрани, системи виявлення вторгнень, системи для контролю привілеїв), а регулярне оновлення компонентів IT-інфраструктури й відстежування вразливостей здатне зменшити ризик, що зловмисник знайде потенційну «точку входу» за допомогою методів OSINT. Водночас безпека багато в чому залежить від обізнаності користувачів. Підготовлений та навчений працівник, який знає про методи соціальної інженерії та уважно ставиться до підозрілих дій, може зупинити атаку ще на її ініціації. Саме тому навчання персоналу та впровадження програм навчання з кібергігієни є важливим крокам у забезпеченні кіберстійкості організації. Підвищення обізнаності користувачів значно звужує поле для діяльності зловмисників, позбавляючи їх найпростішого вектора атаки – людської довірливості.

На завершення, соціальна інженерія та OSINT слід розглядати як дві грані однієї проблеми. З одного боку, вони становлять серйозну загрозу кібербезпеці, з іншого – вказують на напрями, де треба зміцнювати захист. Розуміння того, як легко інформація з відкритих джерел може бути обернена проти нас, спонукає до більш відповідального поводження з власними даними. А протистояти атакам, що націлені на психіку, можна лише випереджуючи їх – знаннями, пильністю і колективною культурою кібербезпеки.

Перелік посилань:

1. National Institute of Standards and Technology. Social Engineering – Glossary. URL: https://csrc.nist.gov/glossary/term/social_engineering (дата звернення: 29.09.2025).
2. SANS. What is Open-Source Intelligence. URL: https://www.sans.org/blog/what-is-open-source-intelligence (дата звернення 29.09.2025).
3. Safeguarding Science. OSINT analysis illustrating potential compromises of academic IT systems. URL: https://www.safeguarding-science.eu/wp-content/uploads/OSINT_open-source-intelligence-compromise-knowledge-security-systems-2023.pdf (дата звернення 29.09.2025).

Оліферчук В.В.
студент групи БСДМ-61, ННІКБЗІ ДУІКТ,
Київ, Україна

КОНТРОЛЬ ДОСТУПУ ЯК КЛЮЧОВИЙ ЕЛЕМЕНТ БЕЗПЕКИ ХМАРНИХ РЕСУРСІВ

Забезпечення безпеки хмарних ресурсів є критичною задачею для організацій, оскільки традиційний мережевий периметр втрачає значення. Контроль доступу стає ключовим елементом безпеки, переходячи від простого дозволу чи заборони до центрального механізму управління. Основою цього підходу є модель Zero Trust, де жоден користувач, пристрій або застосунок не вважається довіреним за замовчуванням. Такий підхід передбачає використання федерації ідентичності для уніфікації політик та впровадження адаптивних механізмів оцінки ризиків у реальному часі, що дозволяє динамічно коригувати рівень привілеїв залежно від контексту сесії.

Ключові слова: контроль доступу, Zero Trust, хмарні ресурси, адаптивний контроль, федерація ідентичності.

У хмарному середовищі, де ресурси розподілені та доступ здійснюється через публічний Інтернет, ідентичність стає новим «периметром» безпеки. Ефективний контроль доступу є ключовою складовою архітектури Zero Trust, яка передбачає автентифікацію та авторизацію кожного запиту незалежно від його джерела. Для реалізації цього принципу використовують механізми федерації ідентичності, що уніфікують управління привілеями через хмарні та локальні платформи та забезпечують застосування принципу найменших привілеїв. Це гарантує, що користувачі, застосунки та мікросервіси отримують доступ лише до необхідного мінімуму ресурсів, суттєво зменшуючи площу атаки та ризики потенційних витоків даних. Крім того, централізоване управління привілеями дозволяє швидко змінювати політики доступу при зміні ролей користувачів або при підключенні нових сервісів, що особливо важливо для організацій із великою кількістю хмарних і локальних ресурсів.

Сучасний контроль доступу виходить за рамки статичних правил і включає адаптивні механізми, які динамічно оцінюють ризики кожної сесії. Оцінка враховує такі фактори, як надійність ідентифікатора, географічне розташування, відомість IP-адреси, стан пристрою, а також аномалії поведінки користувача. Завдяки цьому система може не лише відмовити у доступі, а й миттєво коригувати права під час активної сесії. Наприклад, якщо користувач під час роботи намагається завантажити незвично великі обсяги даних або підключається з невідомої локації, адаптивна політика може автоматично знизити рівень привілеїв або вимагати повторну багатофакторну автентифікацію без повного припинення роботи. Такі динамічні рішення дозволяють зменшити ризики внутрішніх і зовнішніх загроз, одночасно підтримуючи безперервність бізнес-процесів.

Контроль доступу також виконує функцію аудиту та видимості. Технології безперервного моніторингу сесій дозволяють відслідковувати дії користувачів у хмарі, що необхідно для своєчасного виявлення зловживань і потенційних

інцидентів. Аудиторські записи системи контролю доступу служать основою для аналітики безпеки, дозволяючи визначати спроби витоку даних, використання несанкціонованих застосунків та інші відхилення від звичних патернів. Це також допомагає організаціям аналізувати поведінку користувачів і підвищувати ефективність внутрішніх політик безпеки, забезпечуючи одночасно прозорість і контроль.

Крім того, контроль доступу у хмарних середовищах інтегрується з іншими системами безпеки, такими як SIEM та DLP, що дозволяє отримувати централізовану аналітику загроз і швидко реагувати на потенційні атаки. Автоматизація процесів управління доступом знижує ризик людських помилок і підвищує ефективність безпеки без додаткового навантаження на IT-відділи. Таким чином, контроль доступу стає не лише бар'єром для загроз, а й комплексним інструментом, який поєднує превентивні, діагностичні та коригувальні функції, підтверджуючи свою ключову роль у захисті хмарних ресурсів.

Перелік посилань:

1. NIST. Zero Trust Architecture. NIST Special Publication 800-207. August 2020. [Електронний ресурс] – Режим доступу: https://doi.org/10.6028/NIST.SP.800-207.

2. Shetty S., Rao T. R. R., Pai P. A Survey on Identity and Access Management in Cloud Computing // Procedia Computer Science. 2015. Vol. 48. pp. 556–563. DOI: 10.1016/j.procs.2015.04.137.

3. Srinivasan K., Senthil Kumar S. K., Santhosh K. A comprehensive study on various cloud access control models // Journal of Cloud Computing. 2018. Vol. 7. Article 17. DOI: 10.1186/s13677-018-0120-1.

4. Wang W., He M., Wang F. Research on dynamic access control model in cloud computing environment // IEEE International Conference on Cloud Computing and Big Data (CCBD). 2016. pp. 410–415. DOI: 10.1109/CCBD.2016.091.

Борисенко Я.В.
студент групи БСДМ-63, ННІКБЗІ
ДУІКТ,
Київ, Україна

БЕЗПЕЧНІ API В ІНФОРМАЦІЙНИХ СИСТЕМАХ ОРГАНІЗАЦІЙ У КОНТЕКСТІ СУЧАСНИХ ЗАГРОЗ

У контексті архітектури мікросервісів та активної інтеграції, API стали ключовою точкою обміну даними та водночас основним вектором для кібератак. Ін'єкції, порушення контролю доступу на рівні об'єктів та надмірне розкриття даних, вимагають застосування багаторівневої стратегії захисту. Центральним елементом такої стратегії є використання API Gateway як єдиної точки контролю та виконання політик безпеки. Крім того, інтеграція принципів Zero Trust до API-інфраструктури забезпечує безперервну автентифікацію, авторизацію та валідацію кожного запиту, що дозволяє ефективно протидіяти як відомим, так і новим загрозам, гарантуючи цілісність і конфіденційність інформаційних систем.

Ключові слова: API; безпека; контроль доступу; API Gateway; Zero Trust; кіберзагрози.

Зі зростанням використання розподілених інформаційних систем та переходом до хмарних архітектур, API стали головним каналом взаємодії між сервісами та зовнішніми клієнтами. Водночас вони відкрили нову площину ризиків, адже кожен публічний або навіть внутрішній API може стати точкою входу для зловмисників. За даними OWASP, найбільш критичними залишаються вразливості, пов'язані з порушенням контролю доступу, неправильним управлінням автентифікацією, витоком конфіденційних даних, а також ін'єкціями у параметрах запитів. Ці загрози особливо небезпечні через свою логічну природу: вони часто не виявляються стандартними інструментами сканування та потребують глибокого аналізу поведінки API.

Для ефективного захисту необхідно змінити підхід до архітектури безпеки, зробивши її більш адаптивною та централізованою. API Gateway виступає ключовим елементом цього підходу. Він не лише забезпечує маршрутизацію запитів, а й виконує роль фільтра безпеки, який перевіряє схему запиту, структуру JSON або XML-повідомлень, а також застосовує механізми rate limiting, захищаючи сервіси від DDoS-атак або надмірної кількості запитів. Окрім цього, API Gateway спрощує впровадження єдиної системи логування та моніторингу, що дозволяє швидко виявляти підозрілу активність і реагувати на інциденти у реальному часі.

Важливою перевагою централізованого контролю є уніфікація автентифікації та авторизації. Замість реалізації цих механізмів у кожному мікросервісі, Gateway бере це на себе, використовуючи протоколи OAuth 2.0, OpenID Connect або JSON Web Token. Завдяки цьому зменшується ризик помилок у реалізації, підвищується узгодженість політик безпеки, а адміністрування стає простішим. Така централізація дозволяє організаціям забезпечувати єдиний контроль доступу, незалежно від кількості або типу API.

Однак навіть найкраще налаштований Gateway не гарантує повну безпеку без застосування принципів Zero Trust. У своїй основі цей підхід відмовляється

від концепції довіри за замовчуванням, вимагаючи постійної верифікації кожної взаємодії. У контексті API це означає, що кожен запит, незалежно від його джерела, має бути перевірений на відповідність політикам доступу. Система аналізує контекст — тип користувача або сервісу, історію взаємодій, геолокацію чи рівень ризику, — і лише після цього надає дозвіл. При цьому діє принцип найменших привілеїв: користувач або застосунок отримує рівно стільки прав, скільки потрібно для виконання конкретної операції.

Інтеграція Zero Trust із API Gateway дозволяє побудувати динамічну систему безпеки. Наприклад, при спробі виконання нетипового запиту або використанні підозрілого токена система може автоматично вимагати повторну автентифікацію або тимчасово обмежити доступ. Таке рішення ефективно протидіє викраденню токенів, підробці запитів та іншим складним атакам.

Крім того, важливим компонентом є моніторинг і аналітика. Застосування рішень класу API Security Platforms (наприклад, Akamai API Security, Salt Security, або Wallarm) дозволяє автоматично виявляти аномальну поведінку запитів, аналізувати логи й визначати потенційні загрози до того, як вони спричинять шкоду. Поєднання таких інструментів із API Gateway і Zero Trust формує повноцінну екосистему активного захисту, що не лише реагує на інциденти, а й передбачає їх.

Таким чином, захист API у сучасних інформаційних системах — це не окремий процес, а невід’ємна частина загальної архітектури безпеки. Комбінація API Gateway, політик автентифікації, принципів Zero Trust та систем поведінкового аналізу створює багаторівневий захист, здатний протистояти як технічним, так і логічним загрозам. Такий підхід забезпечує стабільність, надійність і безпеку цифрових сервісів, що є критично важливим для функціонування сучасних організацій.

Перелік посилань:

1. Rao I., Chen G. Security analysis of Microservices Architecture with API gateway // International Conference on Communications, Computing and Networking Technologies (ICCCNT). 2017. pp. 1–5. DOI: 10.1109/ICCCNT.2017.8204753.

2. NIST. Zero Trust Architecture. NIST Special Publication 800-207. August 2020. [Електронний ресурс] – Режим доступу: https://doi.org/10.6028/NIST.SP.800-207.

3. OWASP. OWASP API Security Top 10. OWASP Foundation. (Актуальне видання). [Електронний ресурс] – Режим доступу: https://owasp.org/www-project-api-security/.

Олександр КОРШИКОВ
студент групи УБДМ-51, ННІЗІ ДУІКТ, Київ, Україна

Застосування штучного інтелекту для підвищення ефективності виявлення та запобігання кіберзагрозам в мережах державних установ України

У статті проаналізовано масштаби проблеми кіберзагроз як у сучасному світі, так і в українському контексті та вплив розвитку ШІ як на кількість кібератак, так і на ефективність протидії їм. Розглянуто ключові переваги та можливі недоліки, з яким можна стикнутись під час залучення ШІ до захисту інформаційних систем, мереж і баз даних. Наведено приклади успішного впровадження штучного інтелекту в процеси кіберзахисту вже сьогодні та рішення які можливо адаптувати та використовувати для захисту систем державних установ України.

У сучасному світі відбувається стрімкий розвиток технологій, зокрема хмарних рішень та штучного інтелекту(ШІ). Одночасно з цим спостерігається значне зростання кількості та складності кібератак, які завдають чималої шкоди державам у всьому світі, різним типам організацій та суспільству. Втрати в грошовому еквіваленті від шкоди заподіяної кібератаками вже прирівнюють до шкоди заподіяної стихійними лихами. Деякі видання такі як Cybersecurity Ventures прогнозують, що на боротьбу з кіберзлочинністю в 2025 році буде витрачено до 10 трильйонів доларів США[1, с. 3]. В червні цього ж року низка таких видань як Forbes, TIME повідомляли про масовий витік інформації, внаслідок якого у відкритому доступі опинилися близько 16 мільярдів облікових записів сервісів Apple, Google, Facebook, Telegram, GitHub[2, 3 с. 3]. З початком гібридної війни в Україні з 2014 року кількість кібератак на урядові, фінансові, телекомунікаційні та енергетичні системи зі сторони російських хакерських угрупувань збільшилась в рази. Зокрема, у 2015 році відбулася кібератака на енергосистему України, організована російськими хакерами з використанням трояна BlackEnergy, внаслідок якої було вимкнено близько 30 підстанцій і понад 230 тисяч мешканців залишилися без електрики[4, с. 3]. З 24 лютого 2022 року, поряд з повномасштабним вторгненням РФ, кількість кібератак тільки збільшувалась. Кіберзлочинці йдуть у ногу з часом і активно застосовують штучний інтелект (ШІ) для здійснення кібератак. Це змушує фахівців із кібербезпеки використовувати аналогічні технології для захисту інформаційно-комунікаційних систем, мереж, баз даних тощо. Питання вже не стоїть — застосовувати чи ні; відповідь однозначна: застосовувати.

Застосування ШІ може значно посилити захисні механізми мереж державних організацій, завдяки швидкості та точності виявлення загроз ШІ які набагато перевищують можливості традиційних методів. Традиційні системи кібербезпеки часто спираються на статичні правила та сигнатури, які швидко втрачають актуальність. Натомість ШІ, базуючись на методах машинного навчання, здатний швидко адаптуватись та аналізувати величезні обсяги даних у реальному часі. Наприклад, SIEM(Security Information and Event Management) платформа Splunk[6, с. 3], яка пропонує централізоване рішення для збору,

аналізу та моніторингу даних використовує ШІ для виявлення відхилення у поведінці користувачів, хостів і мереж, щоб знаходити приховані загрози та допомагає аналітикам працювати ефективніше, виявляти зловживання, неавторизовані або потенційно шкідливі дії, особливо коли є великий обсяг інцидентів.

Ще однією ключовою перевагою є автоматизація реагування. ШІ може самостійно виявляти загрози, блокувати підозрілі IP-адреси чи ізолювати заражені вузли, мінімізуючи вплив людського фактора. Прикладом такої системи є Darktrace[7, с. 3]. Darktrace застосовує комбінацію поведінкового аналізу, машинного навчання та генеративного ШІ, щоб **виявляти і зупиняти невідомі атаки без сигнатур** (Advanced Persistent Threats, insider threats, zero-day), також може формувати короткі звіти, рекомендації та сценарії реагування. Багато організацій інтегрують Darktrace з SIEM-системами на кшталт Splunk. Ці технології дозволяють суттєво скоротити час реагування і, наприклад, їх можна застосовувати для моніторингу критичної інфраструктури, що є важливим інструментом для протидії російським кіберагресіям. Крім того, впровадження ШІ забезпечує економічну ефективність. Замість розширення штату аналітиків можна запровадити автоматизовану систему, що зменшує навантаження на фахівців SOC(Security Operations Center) та CERT-UA (Computer Emergency Response Team of Ukraine).

Водночас впровадження ШІ супроводжується певними недоліками. Одним із основних є висока вартість розробки та експлуатації. Невеликі державні установи, такі як обласні адміністрації чи комунальні структури, не завжди можуть дозволити собі сучасні рішення без централізованої підтримки на державному рівні. Іншою проблемою є недостатня підготовка персоналу. У багатьох державних органах бракує кваліфікованих фахівців, здатних налаштовувати та підтримувати ШІ-системи. Крім того, виникають юридичні та етичні перепони. Аналіз мережевого трафіку за допомогою ШІ може порушувати права громадян і вимоги законодавства, зокрема Закону України "Про захист персональних даних"[11, с. 3] та GDPR (General Data Protection Regulation)[10, с. 3] у разі міжнародної взаємодії. Наприклад, система моніторингу державної установи ризикує ненавмисно збирати приватні дані службовців або конфіденційну та чутливу інформацію фізичних і юридичних осіб які так або інакше взаємодіють з цією державною установою. Також систематичне впровадження ШІ в робочі процеси на великих підприємствах привело до скорочення кадрів і багато працівників через це втратили свої робочі місця. Багато студентів відмовляються від навчання за спеціальностями, у яких найближчим часом штучний інтелект може повністю замінити людський фактор.

В Україні на щастя поки що кількість охочих навчатися суттєво не зменшилася. Отже, варто розглянути готові рішення на основі штучного інтелекту в кібербезпеці, які успішно застосовуються за кордоном та можуть бути адаптовані для використання в Україні вже зараз. Наприклад Bot Manager

від Akamai[5, с. 3] та Cloudflare Bot Management, які використовують **виявлення, класифікацію та блокування шкідливих ботів** у вебтрафіку. Forti Mail Email Security від Fortinet, Proofpoint Core Email Protection та Mimecast Advanced Email Security, які використовують для виявлення **спам та фішинг** листів, що надходять на електронну пошту. Falcon[9, с. 3] від CrowdStrike, Sentinel One Singularity та Microsoft Defender XDR зосереджена на захисті кінцевих пристроїв (endpoints), виявленні загроз, реагуванні на інциденти, аналізі загроз. Подібних рішень уже досить багато, але й коштують вони чимало коштів. Поряд із зарубіжними рішеннями, які державні організації можуть використовувати завдяки партнерським програмам, в Україні Міністерством цифрової трансформації запущено першу державну онлайн-платформу, на базі якої інвестуються українські проєкти розвитку штучного інтелекту в різних сферах у тому числі в кібербезпеці.

Впровадження штучного інтелекту в кібербезпеку державних організацій та установ України є перспективним, але складним процесом який потребує значних фінансових, кадрових, технічних, організаційних та стратегічних навантажень. Висока вартість, відсутність або дефіцит кваліфікованих фахівців, вразливості ШІ, бюрократичні перепони та залежність від іноземних технологій створюють значні перешкоди. Для подолання цих перешкод Україні необхідно інвестувати в освіту, розвивати власні ШІ-системи, співпрацювати з міжнародними партнерами та вдосконалювати законодавчу базу, що дозволить підвищити кіберстійкість державних установ та зміцнити позиції України в сфері кібербезпеки.

Список літератури:

1. https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/
2. https://www.forbes.com/sites/daveywinder/2025/06/20/16-billion-apple-facebook-google-passwords-leaked---change-yours-now/
3. https://time.com/7296254/passwords-leaked-data-breach/
4. https://uk.wikipedia.org «Російсько-українська кібервійна»
5. akamai.com, workers.cloudflare.com
6. splunk.com
7. darktrace.com
8. fortinet.com, mimecast.com, proofpoint.com
9. crowdstrike.com, sentinelone.com
10. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679&qid=1760358225830
11. https://zakon.rada.gov.ua/laws/show/2297-17#Text

Кривець Данило Олександрович
студент групи БСДМ-61, ННІКЗБІ ДУІКТ, Київ, Україна

СУЧАСНІ ПРОБЛЕМИ ТА ВИКЛИКИ У ЗАБЕЗПЕЧЕННІ БЕЗПЕКИ ВЕБЗАСТОСУНКІВ

Безпека вебзастосунків є критичним чинником у сучасному цифровому середовищі, де швидкість розробки поєднується з постійними загрозами. Виклики, описані в OWASP Top 10, вимагають переходу до проактивних практик, серед яких важливу роль відіграє інтеграція безпеки на ранніх етапах (shift left) та використання статичного аналізу коду (SAST). Інноваційні рішення, зокрема Snyk Code, поєднують автоматизацію, штучний інтелект та безшовну інтеграцію у життєвий цикл розробки, що дозволяє забезпечити захист даних, швидші релізи та підвищення довіри користувачів.

Ключові слова: кібербезпека, вебзастосунки, OWASP Top 10, SAST, shift left, Snyk Code, штучний інтелект.

У 2025 році проблематика безпеки вебзастосунків набула ще більшої актуальності. Прискорений розвиток штучного інтелекту, що стимулює експоненційне зростання кількості нового коду, та широке використання API створюють умови для формування складних цифрових екосистем. Водночас організації стикаються з надзвичайно швидкими циклами розробки, розширенням площини атак і обмеженими ресурсами безпекових команд, які змушені захищати дедалі комплексніші інфраструктури.

Ключова проблема полягає в тому, що кожен новий елемент у системі — фрагмент коду, зовнішня бібліотека чи інтегрований сервіс — потенційно може містити приховані вразливості. Вони часто неочевидні: відсутність валідації введення, використання застарілої залежності або некоректна конфігурація. На перший погляд дрібні помилки здатні перетворюватися на катастрофічні збої безпеки, коли співпадають несприятливі фактори [1].

Хоча більшість розробників знайомі з OWASP Top 10 — переліком найбільш поширених та критичних уразливостей вебзастосунків — просте знання цього списку недостатнє. Як зазначають експерти, засвоєння Top 10 можна порівняти з вивченням правил шахів: воно необхідне, але без розуміння стратегії перемоги цього знання бракує (OWASP, 2023). Справжня складність виникає у повсякденній розробці, коли тиск дедлайнів суперечить вимогам до ретельного тестування безпеки.

Інтенсивність сучасної розробки призводить до того, що щодня у продуктивне середовище потрапляють сотні й тисячі рядків нового коду. До цього додаються десятки сторонніх бібліотек і численні зовнішні API. Кожен новий commit чи інтеграція стає ще однією потенційною слабкою ланкою в «броні» застосунку. Виявлення цих проблем після релізу не лише дорого коштує, а й підриває довіру користувачів та бізнес-партнерів [1].

Актуальність цих проблем підтверджується оновленим списком OWASP Top 10 за версією Snyk Code, що визначає найбільш критичні загрози для вебзастосунків у 2025 році [2]:

- A01: Broken Access Control – порушення контролю доступу дозволяє зловмисникам обходити обмеження й отримувати доступ до конфіденційних даних.

- A02: Cryptographic Failures – вразливості через слабкі алгоритми, неправильне керування ключами або відсутність належного шифрування.
- A03: Injection (SQL, Command, etc.) – атаки, що використовують неперевірені вхідні дані для виконання шкідливих команд або запитів.
- A04: Insecure Design – системні вразливості, спричинені відсутністю безпечних принципів проєктування.
- A05: Security Misconfiguration – помилки у конфігурації систем чи бібліотек, що відкривають додаткові вектори атак.
- A06: Vulnerable and Outdated Components – використання застарілих бібліотек або компонентів із відомими вразливостями.
- A07: Identification and Authentication Failures – слабка автентифікація та некоректне керування сесіями, що дозволяє викрадати облікові дані.
- A08: Software and Data Integrity Failures – відсутність перевірки цілісності даних та процесів, зокрема в CI/CD-пайплайнах.
- A09: Security Logging and Monitoring Failures – недостатнє логування та моніторинг, що ускладнює виявлення атак у реальному часі.
- A10: Server-Side Request Forgery (SSRF) – можливість обманути сервер і змусити його виконувати шкідливі запити до внутрішніх ресурсів.

Щоб мінімізувати ці ризики, компанії застосовують кращі практики інформаційної безпеки, серед яких ключову роль відіграє зазначений вище принцип «shift left». Це означає інтеграцію безпеки у ранні етапи життєвого циклу розробки замість традиційної моделі «перевірки перед релізом». Особливо ефективним інструментом є статичний аналіз коду (SAST), який дозволяє автоматично виявляти критичні уразливості ще під час написання коду. Такий підхід дає змогу виправляти проблеми швидко і дешево, не чекаючи виходу продукту.

Важливими складовими кращих практик також є постійне тестування та пріоритезація виправлень. Інтеграція SAST у CI/CD-конвеєр створює механізм безперервного контролю: кожен новий фрагмент коду проходить автоматичну перевірку, а виявлені уразливості отримують пріоритетність залежно від їх критичності (CVSS). Це дозволяє командам швидко зосереджуватися на найбільш небезпечних проблемах. Додаткове застосування принципу найменших привілеїв (POLP) та регулярний моніторинг формують комплексний захист, який охоплює всі етапи розробки й експлуатації [3].

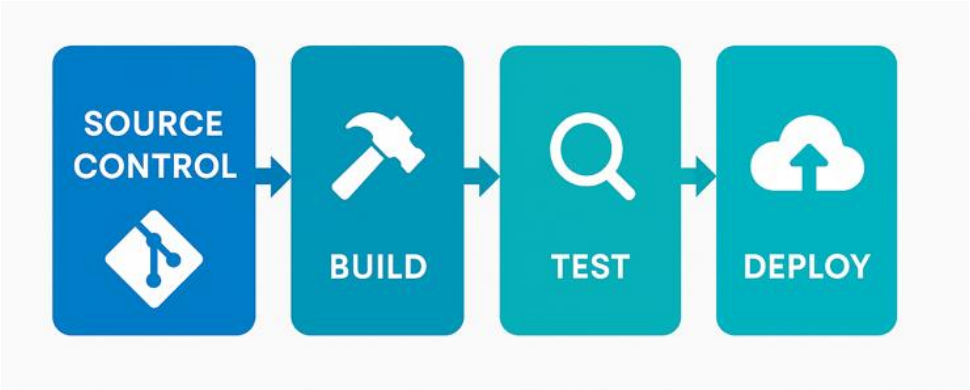

Рис. 1 – життєвий цикл веб-додатка (спрощений)

У цьому контексті особливої уваги заслуговує Snyk Code, що поєднує SAST із технологіями штучного інтелекту. Завдяки гібридному аналізу потоків даних інструмент вирізняється низьким рівнем хибнопозитивних спрацювань, що дозволяє розробникам зосередитися на реальних проблемах. Крім того, Snyk Code забезпечує інтерактивні підказки та приклади виправлення, що підвищує швидкість та якість роботи команд без відриву від їх основних процесів.

Таким чином, сучасні виклики безпеки вимагають від організацій нового підходу: поєднання перевірених практик, таких як shift left і SAST, з інноваційними рішеннями на базі AI. Використання платформ на кшталт Snyk Code допомагає не лише зменшити кількість уразливостей, а й трансформувати саму культуру розробки — від реагування на інциденти до проактивного запобігання. Результатом стають більш захищені вебзастосунки, швидші релізи та підвищена довіра користувачів, яка є основою цифрової економіки.

Перелік посилань:

1. Jamie Gale, Application Security: Challenges, Tools & Best Practices // Dec 18, 2024. URL: https://www.crowdstrike.com/en-us/cybersecurity-101/application-security.

2. Snuk Code, OWASP Compliance and Secure Web Applications White Papers // Feb 15, 2025. URL: https://snyk.io/lp/what-you-need-to-know-about-owasp/.

3. Web Application Security Threats in 2025: 10 Critical Risks Every Organization Must Address // July 23, 2025. URL: https://www.stackhawk.com/blog/10-web-application-security-threats-and-how-to-mitigate-them/#h-emerging-web-application-security-risks-in-2025.

Шандровський Ярослав Ігорович
студент групи БСДМ-61, ННІКЗБІ ДУІКТ, Київ,
Україна

РОЗВИТОК ПІДХОДІВ ДО МЕРЕЖЕВОЇ БЕЗПЕКИ: ВІД VPN ДО ZERO TRUST

Кібербезпека сьогодні є одним із ключових факторів стабільності та розвитку суспільства. В умовах цифрової трансформації саме дані виступають головним активом, а доступ до них — критичним елементом безпеки. Традиційні моделі контролю доступу, зокрема VPN, вже не відповідають вимогам сучасності, адже не враховують реальні потреби користувачів і створюють ризики надмірних прав. Акцентується увага на необхідності переходу до концепції Zero Trust, яка базується на принципі мінімально необхідних прав і забезпечує прозорість, гнучкість та підвищений рівень захисту інформаційних ресурсів.

Ключові слова: контроль доступу, кібербезпека, VPN, Zero Trust, віддалена робота, мінімальні права, політика безпеки.

Сучасний ринок інформаційних технологій і кібербезпеки пропонує широкий спектр інструментів для протидії актуальним загрозам. Однак саме це й створює складність для компаній: замість цілісної системи вони часто змушені комбінувати різнорідні засоби захисту, що не завжди добре інтегруються між собою. У результаті зростає не лише складність управління безпекою, але й ризик виникнення прогалин у захисті.

Для кінцевих користувачів ця ситуація обертається дилемою: обирати між безпекою та зручністю. Нерідко співробітники віддають перевагу зручності, що призводить до порушення політик безпеки й підвищує ризики витоку даних. Це свідчить про те, що сучасні підходи до організації доступу є застарілими й не відповідають вимогам цифрової трансформації та віддаленого формату роботи.

Корінь проблеми криється в крихкій моделі контролю доступу, яка сформувалася ще у 1990-х роках і практично не зазнала суттєвих змін. Навіть для найбільш критичних ресурсів компанії продовжують використовувати базові засоби контролю, серед яких [1]:

- Статичні імена користувачів і паролі;
- Приватні, захищені мережі, прив’язані до фізичних локацій (офісів);
- Жорстко керовані пристрої (часто у поєднанні з VPN для віддаленого доступу до цих мереж).

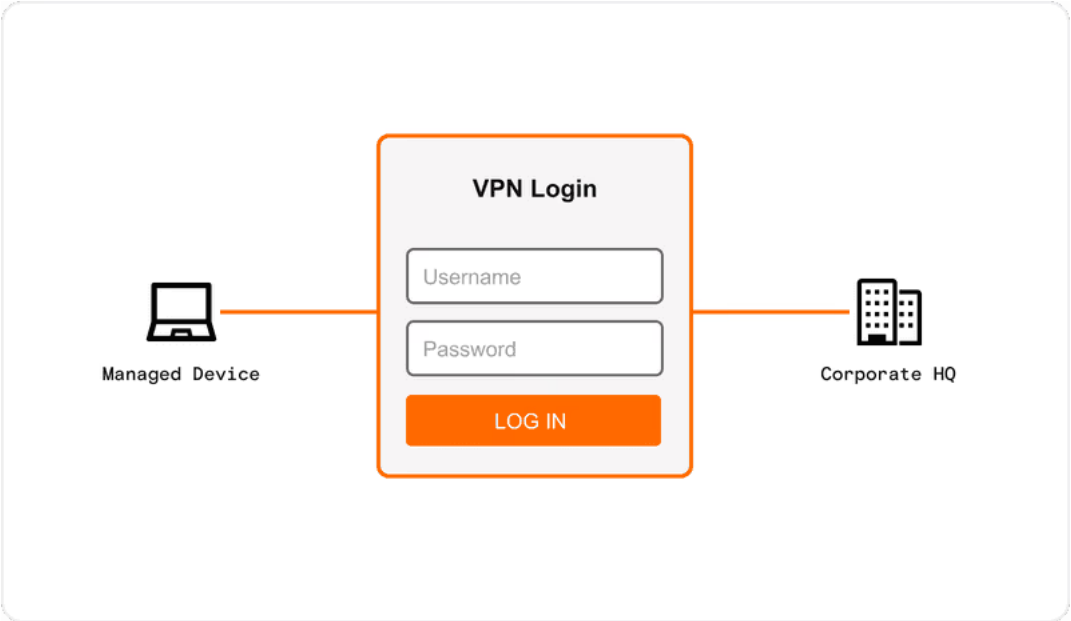

Рис. 1 – класична модель доступу

Однак такі методи вже не відповідають сучасним викликам. В умовах розподілених команд і зростаючої кількості хмарних сервісів жорстка прив'язка доступу до фізичного офісу чи конкретного пристрою не дозволяє забезпечити гнучкість і масштабованість. Більше того, статичні паролі вразливі до фішингових атак і компрометацій, а VPN забезпечує доступ до мережі в цілому, а не до окремих ресурсів, що створює надмірні права доступу.

Таким чином, перехід до сучасних моделей контролю доступу є нагальною потребою. Без відмови від архаїчних механізмів управління і впровадження принципу мінімально необхідних прав (least privilege) організації ризикують залишитися незахищеними перед зростаючим спектром кіберзагроз. Це робить контроль доступу ключовим елементом кібербезпеки наступного десятиліття.

Однак, просте заміщення одного інструмента іншим не може вважатися ефективним вирішенням проблеми контролю доступу. Концепція Zero Trust передбачає глибоку перебудову всієї системи організаційних і технічних заходів, а також формування єдиної політики безпеки, що ґрунтується на реальних потребах користувачів. Важливим викликом у цьому процесі стає необхідність збору, аналізу та інтерпретації інформації про те, хто саме і до яких ресурсів звертається. Лише на основі таких даних можна сформувати збалансовану систему доступу, яка одночасно гарантує і безпеку, і продуктивність.

Таким чином, основний алгоритм впровадження підходу Zero Trust у контексті управління доступом можна описати так [2]:

- Ідентифікація всіх наявних активних серверів та сервісів в мережі;
- Розуміння, хто фактично звертається та й до чого (проти того, хто теоретично може);
- Розробка політики безпеки на основі реальних паттернів використання
- Впровадження доступ з найменшими правами.

Разом із тим, інструменти та практики, що застосовуються для реалізації цього підходу, можуть створювати певні труднощі для користувачів. Використання громіздких VPN уповільнює роботу мережі, постійні зміни паролів викликають роздратування, ручне управління списками дозволених IP-адрес виявляється надто крихким і складним, а рішення з керування пристроями часто є надмірно інвазивними для особистих гаджетів. Усе це призводить до того, що користувачі шукають способи обходу встановлених заходів безпеки, що, у свою чергу, створює додаткове навантаження на команди IT і безпеки.

У результаті компанії залишаються вразливими, навіть коли формально впроваджують сучасні рішення. Саме тому Zero Trust розглядається як перспективна модель майбутнього: вона поєднує принцип мінімально необхідних прав із гнучким підходом до користувачів, орієнтуючись не на довіру до середовища чи пристрою, а на конкретну перевірку кожного запиту доступу. Це дозволяє поступово усунути ключові слабкі місця класичних систем контролю доступу.

Таким чином, проблема сучасного мережевого доступу полягає не лише у технічних обмеженнях традиційних інструментів, а й у відсутності прозорості у використанні ресурсів та гнучкості в управлінні доступом. Модель Zero Trust є логічною відповіддю на ці виклики: вона змінює саму парадигму контролю, орієнтуючись на дані про реальні потреби користувачів і мінімізуючи ризики надмірних прав. Проте її впровадження вимагає комплексної роботи — від збору даних і побудови політик до подолання бар’єрів зручності для користувачів. Саме поєднання цих елементів визначає майбутнє ефективної кібербезпеки в наступному десятилітті [3].

Перелік посилань:

1. Tony Huie, Solving the usability problem to unlock Zero Trust adoption // Apr 14, 2022. URL: https://www.twingate.com/blog/series-b-announcement.

2. Bren Sapience, Solving the Zero Trust Usage Puzzle with Twingate Insight Reports // Mar 25, 2025. URL: https://www.twingate.com/blog/insight-reports.

3. Blend uses Opal and Twingate to implement a holistic Zero Trust Strategy // July 20, 2025. URL: https://www.twingate.com/customers/blend.

Сиротенко Д. Г.
студент групи БСДМ-63, ННІКБЗІ ДУІКТ,
Київ, Україна

ВИКОРИСТАННЯ МАШИННОГО НАВЧАННЯ ДЛЯ РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ

Машинне навчання у сфері кібербезпеки – це сучасний підхід, що дозволяє системам автоматично аналізувати великі обсяги даних і виявляти приховані закономірності без прямого програмування. У контексті розслідування кіберінцидентів воно забезпечує швидке виявлення підозрілої активності, аналіз логів, мережевого трафіку та поведінкових моделей користувачів, що допомагає вчасно реагувати на загрози. Алгоритми класифікації, кластеризації та глибокого навчання дозволяють автоматизувати процеси виявлення та оцінки інцидентів, зменшуючи вплив людського фактора. Таким чином, машинне навчання стає ключовим інструментом для підвищення ефективності розслідувань, оптимізації роботи центрів безпеки (SOC) та створення адаптивних систем захисту, здатних протидіяти складним кіберзагрозам у реальному часі.

Ключові слова: машинне навчання, кіберінцидент, штучний інтелект, аналіз даних, SOC, виявлення загроз, розслідування, кібербезпека.

У сучасному світі, де більшість бізнес-процесів, комунікацій та управлінських рішень здійснюється за допомогою цифрових технологій, зростає кількість і складність кіберзагроз. Розслідування кіберінцидентів вимагає глибокого аналізу величезних обсягів даних, журналів подій, мережевого трафіку та поведінкових моделей користувачів. Традиційні методи аналітики часто є недостатньо гнучкими та не встигають за динамікою атак. Саме тому у практику кіберзахисту активно впроваджуються технології машинного навчання (ML), які здатні автоматизувати виявлення, класифікацію та аналіз кіберінцидентів.

Машинне навчання - це підхід до аналізу даних, при якому комп’ютерні системи отримують знання не через жорстко задані алгоритми, а на основі виявлення закономірностей у наявних даних. У контексті кібербезпеки ML дає змогу створювати моделі, що автоматично розпізнають ознаки шкідливої активності, аналізують поведінку користувачів і систем, а також допомагають виявляти інциденти, які залишилися поза увагою традиційних засобів захисту.

Одним із ключових напрямів застосування машинного навчання є автоматизація розслідувань у SOC (Security Operations Center). Алгоритми класифікації дозволяють визначати тип інциденту - наприклад, фішинг, DDoS-атака, зловмисне ПЗ чи несанкціонований доступ. За допомогою методів кластеризації події групуються за схожими характеристиками, що дає змогу аналітикам фокусуватися на найважливіших і найбільш небезпечних загрозах. Використання нейронних мереж у поєднанні з технологіями глибокого навчання дає можливість виявляти навіть ті атаки, що маскуються під звичайну активність користувачів.

Особливо важливим напрямом є виявлення аномальної поведінки у корпоративних мережах. Системи, засновані на ML, аналізують історичні дані про типову роботу користувачів і пристроїв, після чого автоматично фіксують відхилення - наприклад, незвичний час доступу, підозрілу передачу великих

обсягів даних або спроби входу з невідомих IP-адрес. Це дозволяє запобігати інсайдерським загрозам, коли компрометація відбувається через внутрішніх співробітників.

Машинне навчання також ефективно використовується на етапі післяінцидентного аналізу. Алгоритми допомагають відновити ланцюжок подій, які призвели до атаки, визначити первинну точку проникнення, методи розповсюдження шкідливого коду та оцінити масштаби впливу. Завдяки автоматизації таких процесів скорочується час розслідування, підвищується точність висновків і мінімізується ризик людської помилки.

Проте впровадження ML у розслідування кіберінцидентів супроводжується низкою викликів. Найважливіший з них - якість і обсяг даних, необхідних для навчання моделей. Недостатня кількість репрезентативних прикладів або наявність некоректних даних можуть призвести до помилкових спрацьовувань. Крім того, зловмисники вже починають застосовувати методи штучного інтелекту для обходу систем виявлення, що створює нову гонку між оборонними і атакуючими технологіями.

Таким чином, застосування машинного навчання в розслідуванні кіберінцидентів стає одним із ключових напрямів розвитку сучасної кібербезпеки. Інтелектуальні системи допомагають автоматизувати рутинні процеси, зменшити навантаження на аналітиків SOC, підвищити швидкість реагування та точність діагностики інцидентів. У перспективі поєднання ML із методами штучного інтелекту дозволить створити автономні системи кіберзахисту, здатні самостійно виявляти, аналізувати й нейтралізовувати атаки у реальному часі.

Перелік посилань:

1. Unlocking the Potential of AI/ML in Cybersecurity: Challenges, Opportunities, and Progress Indicators. Stellar Cyber. URL: https://stellarcyber.ai/uk/unlocking-the-potential-of-ai-ml-in-cybersecurity-challenges-opportunities-and-progress-indicators/.

2. Бабенко О.Ю., Степаненко Ю.В. Використання штучного інтелекту в системах забезпечення кібербезпеки / *Cybersecurity: Education, Science, Technique* – 2024. – №2(22). URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/774.

3. The Role of AI and Machine Learning in Cybersecurity in 2025. Lazarus Alliance. URL: https://lazarusalliance.com/uk/the-role-of-ai-and-machine-learning-in-cybersecurity-in-2025/.

4. Романишин В.Я., Бідюк Н.М. Моделі та методи машинного навчання для забезпечення кібербезпеки / *Вісник Національного університету «Львівська політехніка»* – Серія: Комп'ютерні науки та інформаційні технології. – 2025. – №2504. – С. 73–80. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2025/may/38956/k250473-70-80.pdf.

Балацький А.В.
студент групи БСДМ-51, ННІКБЗІ ДУІКТ,
Київ, Україна

КІБЕРЗАХИСТ КОРПОРАТИВНИХ ІТ-СИСТЕМ

Кібербезпека корпоративних інформаційних систем – це комплекс методів, процесів та технологій, спрямованих на захист інформаційних активів організації. До таких активів належить програмне забезпечення, мережеві ресурси, бази даних та критично важлива інформація, що обробляється і зберігається у корпоративних системах. У сучасному світі інформація є ключовим ресурсом, і саме її захист визначає стабільність роботи організацій та безпеку бізнес-процесів.

Ключові слова: корпоративні інформаційні системи, фішинг, кібербезпека, конфіденційні дані, контроль доступу, шифрування, IDS/IPS, політики інформаційної безпеки, стандарти ISO/IEC 27001, управління ризиками, SIEM.

Найслабшим елементом у забезпеченні безпеки корпоративних систем залишаються люди, оскільки їхні помилки або зловмисні дії можуть призвести до витоку або компрометації даних. Будь-яка організація – державна чи комерційна, фінансова чи медична – накопичує та обробляє значні обсяги інформації про клієнтів, користувачів та співробітників. Кожна інформаційна система, що взаємодіє з електронними обчислювальними машинами та мережею, відіграє критично важливу роль у забезпеченні ефективної роботи компанії та захисту суспільства від кіберзагроз.

У межах корпоративної інформаційної системи кібербезпека включає управління доступом, контроль за цілісністю та конфіденційністю даних, моніторинг подій безпеки, впровадження стандартів та політик інформаційної безпеки. Це дозволяє своєчасно виявляти потенційні загрози, зменшувати ризики та забезпечувати безперервність бізнес-процесів.

Основні загрози корпоративних ІС

Загрози можна класифікувати на три основні групи:

- зовнішні загрози – атаки з боку хакерів або організованих кіберзлочинних груп. Приклади: фішинг, ransomware, DDoS-атаки [1];
- внутрішні загрози – дії співробітників або партнерів, що мають доступ до системи, але порушують політики безпеки (insider threat);
- технічні загрози – вразливості програмного та апаратного забезпечення, неправильні налаштування мережі та систем.

Сучасні атаки часто комбінуються, наприклад, фішинг для проникнення з наступним встановленням шкідливого програмного забезпечення [2].

Методи захисту корпоративних ІС

Контроль доступу обмежує доступ користувачів до ресурсів відповідно до їхніх ролей. Найпоширеніші моделі: **RBAC (Role-Based Access Control)** та **ABAC (Attribute-Based Access Control)**.

Формально доступ можна описати функцією:

$$A(u,r) = \begin{cases} 1, & \text{якщо користувач } u \text{ має роль } r \\ 0, & \text{інакше} \end{cases}$$

де $A(u,r)$– дозвіл доступу користувача u до ресурсу з роллю r [3].

Захист даних у корпоративних ІС забезпечується алгоритмами шифрування: **AES** для симетричного та **RSA** для асиметричного шифрування.

$$C = E_k(M)$$

де C– шифротекст, E_k– алгоритм шифрування з ключем k, M– відкритий текст.

Шифрування даних у базах та при передачі між сервером і клієнтом гарантує конфіденційність і цілісність інформації.

IDS/IPS дозволяють виявляти підозрілу активність у мережі та реагувати на потенційні загрози. Типова архітектура включає сенсори, аналізатори та консоль управління (Рис. 1).

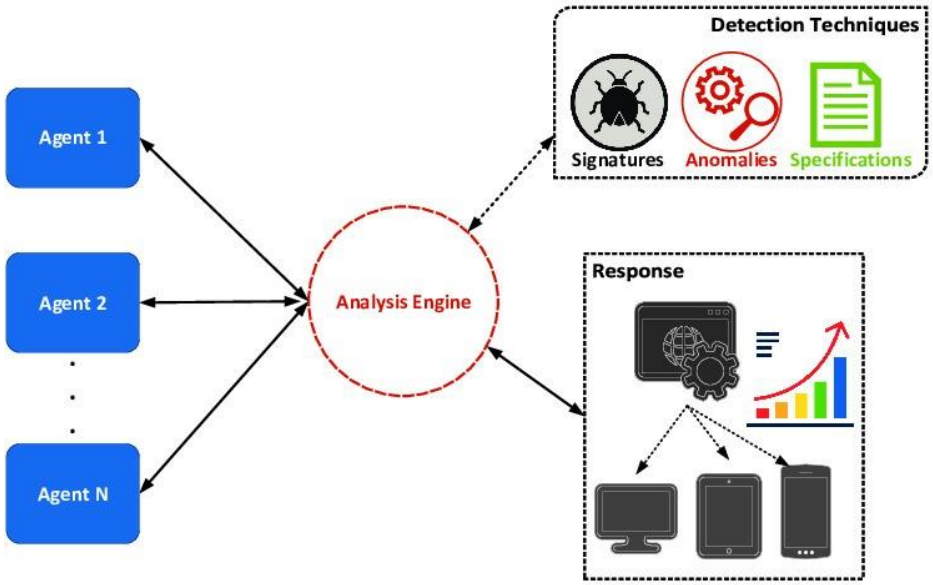

Рис. 1 – Архітектура IDS/IPS

Agents (1…N) — це сенсори або моніторингові вузли, які збирають трафік або системні події з різних джерел (наприклад, мережеві пакети, журнали, поведінкові дані).

Analysis Engine — центральний аналітичний модуль, який обробляє отримані дані, застосовує методи виявлення атак і приймає рішення.

Detection Techniques — три основні підходи

Signatures — сигнатурний аналіз, пошук відомих шаблонів атак;

Anomalies — виявлення відхилень від нормальної поведінки;

Specifications — перевірка відповідності дій специфікаціям або політикам.

Response — реакція системи (сповіщення адміністратора, блокування трафіку, створення звітів, тощо).

Інтеграція IDS/IPS із системами **SIEM** забезпечує кореляцію подій та автоматичне формування сигналів безпеки.

Формальні політики стандартизують управління доступом, оновлення ПЗ, резервне копіювання та реагування на інциденти.

Наприклад, **Password Policy** встановлює мінімальні вимоги до складності паролів, включаючи довжину, наявність великих і малих літер, цифр та спеціальних символів, а також регламентує періодичність їх зміни. Це дозволяє підвищити стійкість облікових записів до несанкціонованого доступу та зменшити ризик злому через прості або повторно використовувані паролі.

Стандарти та нормативи

Стандарти та нормативи є фундаментальними інструментами забезпечення кібербезпеки корпоративних інформаційних систем, оскільки вони визначають чіткі вимоги та рекомендації щодо захисту інформаційних ресурсів. Використання міжнародних стандартів дозволяє організаціям впроваджувати перевірені практики управління безпекою, мінімізувати ризики та забезпечити відповідність законодавчим і галузевим вимогам.

ISO/IEC 27001, наприклад, пропонує комплексний підхід до побудови системи управління інформаційною безпекою. Цей стандарт визначає процеси оцінки ризиків, встановлення політик, процедур та контролів, що забезпечують захист конфіденційності, цілісності та доступності інформації. Впровадження ISO/IEC 27001 дозволяє організаціям не лише формалізувати підходи до безпеки, але й регулярно оцінювати ефективність заходів та вдосконалювати їх.

NIST Cybersecurity Framework надає рекомендації щодо управління кіберризиками і допомагає організаціям впорядкувати процеси захисту, адаптуючи їх під конкретні загрози та вимоги бізнесу. Він включає п’ять основних функцій: ідентифікація активів, захист, виявлення, реагування та відновлення після інцидентів, що забезпечує всебічний підхід до безпеки.

CIS Controls є практичним набором заходів з контролю, які дозволяють ефективно захищати корпоративні системи від відомих атак. Ці заходи структуровані за пріоритетністю та спрямовані на усунення найбільш поширених вразливостей, що дозволяє організаціям швидко підвищити рівень захисту.

Впровадження таких стандартів і нормативів дозволяє систематизувати процеси кібербезпеки, забезпечити їх прозорість і контрольованість, а також створити основу для регулярного аудиту і вдосконалення заходів захисту, що суттєво підвищує загальний рівень безпеки корпоративної інформаційної системи [4].

Висновки

Кібербезпека корпоративних інформаційних систем є ключовим елементом стабільної роботи сучасних організацій. Комплексне застосування технічних і організаційних заходів, таких як контроль доступу, шифрування, IDS/IPS та стандарти ISO/IEC 27001, забезпечує стійкість до зовнішніх і внутрішніх загроз. Впровадження політик безпеки та постійний моніторинг

дозволяють зменшити ризики кіберінцидентів і забезпечити безперервність бізнес-процесів.

Перелік посилань:

1. National Institute of Standards and Technology (NIST). *Cybersecurity Framework (CSF) 2.0*. 2024. URL: https://www.nist.gov/cyberframework
2. European Union Agency for Cybersecurity (ENISA). Threat Landscape 2024. URL: https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape
3. IBM. Role-Based Access Control (RBAC) — Concepts and Relationships. 2024. URL: https://www.ibm.com/docs/en/coss/3.18.3?topic=administration-rbac-model
4. ISO/IEC 27001:2022 Information Security Management Systems – Requirements 2022. URL: https://ain.ua/2022/12/06/nova-versiya-standartu-iso-iec-270012022-chym-it-kompaniyam-korysnyj-czej-standart-ta-yak-jogo-vprovadyty/

Шкляр Я.Р.
студент групи БСДМ-62, ННІКБЗІ
ДУІКТ,
Київ, Україна

ESET PROTECT ЯК ІННОВАЦІЙНИЙ ПІДХІД ДО АВТОМАТИЗОВАНОГО УПРАВЛІННЯ ПОЛІТИКАМИ БЕЗПЕКИ

У роботі проаналізовано ESET PROTECT як централізоване рішення, що пропонує нові механізми автоматизації. Особливу увагу приділено тому, як платформа забезпечує єдине управління кінцевими точками, повний огляд стану безпеки та можливість автоматичного впровадження політик безпеки, моніторингу та коригування політик у відповідь на зміни в середовищі та нові загрози. Використання автоматизованого підходу в ESET PROTECT дозволяє зменшити вплив людського фактора, прискорити реакцію на інциденти та підтримувати відповідність стандартам безпеки. Впровадження ESET PROTECT є важливим для організацій, які прагнуть досягти високого рівня кіберстійкості через інтелектуальне та проактивне управління безпекою.

Ключові слова: ESET, автоматизація, політики безпеки, кінцеві точки, інциденти.

ESET Inspect — Всеохоплююча система виявлення кінцевих точок і реагування, яка включає в себе такі функції, як виявлення інцидентів, керування інцидентами та реагування на них, збір даних, виявлення індикаторів компрометації, виявлення аномальної активності, виявлення поведінки і порушення політик [1].

ESET використовує політики інформаційної безпеки для забезпечення відповідності всім аспектам стандарту ISO 27001, зокрема в питаннях управління безпекою інформації, а також контролю за безпекою й практиками. Політики переглядаються щорічно та оновлюються після суттєвих змін, що гарантує їхню актуальність [2].

ESET щорічно переглядає цю політику й внутрішні процедури перевірки безпеки, щоб забезпечити їхню узгодженість із цією політикою. Недотримання політик щодо інформаційної безпеки призводить до дисциплінарних стягнень для співробітників ESET або до передбачених контрактом штрафів аж до розірвання контракту для постачальників [2].

Архітектура ESET Protect заснована на централізованій консолі управління, яка дозволяє адміністраторам розгортати рішення ESET, керувати завданнями, застосовувати політики безпеки, відстежувати стан системи та швидко реагувати на проблеми й загрози на віддалених комп’ютерах.

ESET Protect може бути встановлений на серверах під управлінням Windows або Linux, а також розгорнутий як віртуальний пристрій, що забезпечує гнучкість у виборі інфраструктури.

Завдяки гнучким можливостям рішень ESET, організації мають змогу створювати динамічні групи для автоматизованого моніторингу, налаштовувати політики захисту, ізоляції та реагування, а також проводити детальний аналіз інцидентів за допомогою журналів та інтерактивних таймлайнів.

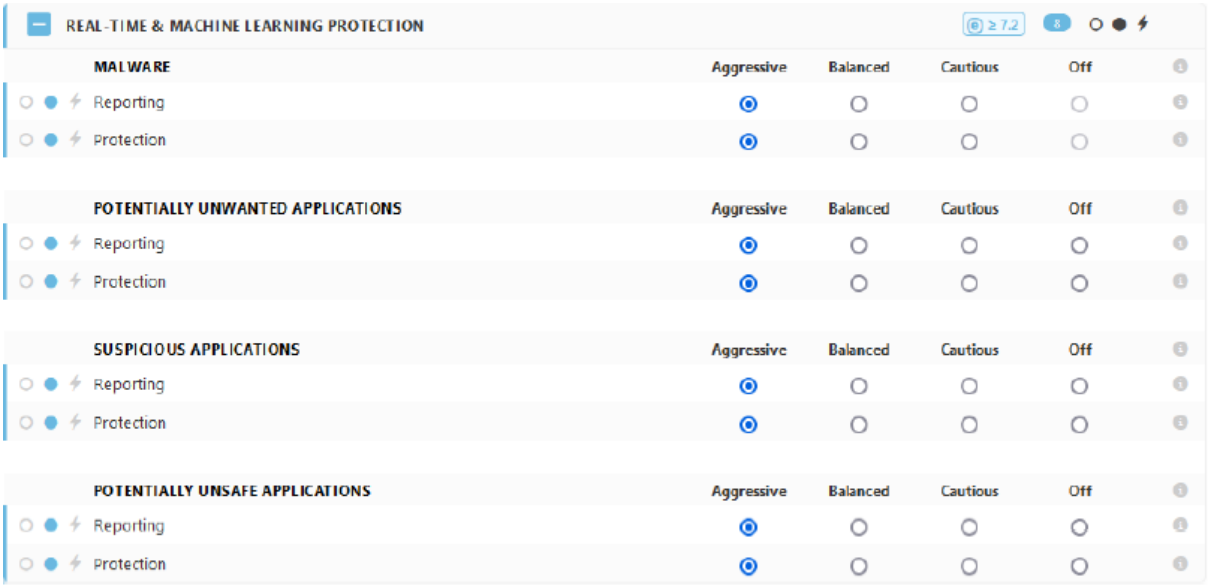

Рис. 1. Налаштування політики

Щоб запобігти несанкціонованим змінам параметрів захисту, в політиках безпеки ESET Protect, ESET Management Agent та ESET Inspect Connector необхідно встановити пароль. Цей пароль захистить від можливості:

— модифікувати критичні налаштування продукту;

— видаляти програмне забезпечення;

— відключати параметри безпеки чи агента управління.

Встановлення пароля гарантує, що лише уповноважені особи зможуть вносити зміни в параметри безпеки, тим самим підвищуючи загальний рівень захисту інфраструктури.

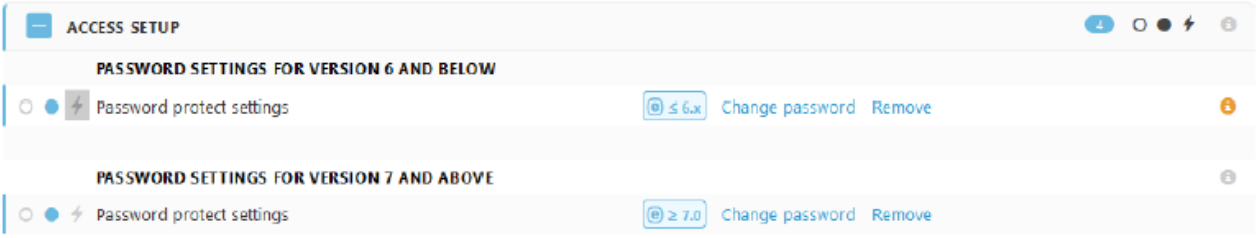

Рис. 2. Захист паролем

Налаштування автоматизації політик безпеки в ESET PROTECT здійснюється за допомогою управління завданнями (Tasks). Ви можете створювати та налаштовувати завдання для автоматичного застосування політик до груп комп'ютерів, наприклад, для розгортання, налаштування, оновлення та виконання регулярних перевірок [3].

Можливості автоматизації включають:

Створення та планування завдань: у веб-консолі ESET PROTECT створюєте нове завдання і в його налаштуваннях вибрати тип політики, яку необхідно застосувати. Далі запланувати виконання цього завдання на певний час або за тригером.

Групове застосування: завдання можна застосувати до конкретних статичних або динамічних груп комп'ютерів, що дозволяє централізовано керувати політиками для всіх пристроїв у групі.

Розгортання агента ESET Management Agent: автоматична установка агента на нові пристрої.

Оновлення компонентів: регулярне оновлення антивірусних модулів і програмного забезпечення.

Налаштування політик: автоматична установка або зміна параметрів безпеки, таких як налаштування брандмауера або антивірусного захисту.

Запуск перевірок: налаштування регулярних повних або вибіркових перевірок на віруси [3].

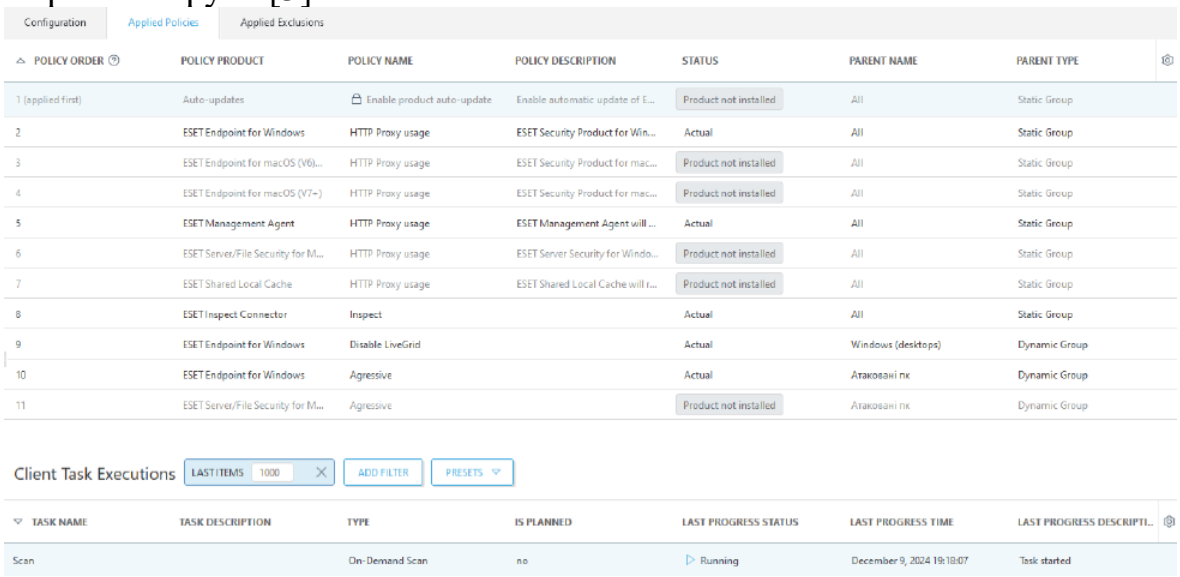

Рис. 3. Застосовані політики та заплановані завдання

Рішення ESET Protect демонструє свою ефективність у централізованому управлінні безпекою, надаючи адміністраторам можливість віддалено керувати політиками захисту та аналізувати інциденти [3].

Перелік посилань:

1. ESET Inspect | ESET PROTECT. ESET Online Help. URL: https://help.eset.com/protect_cloud/uk-UA/eset_inspect.html (дата звернення: 15.10.2025).

2. Безпека для ESET PROTECT. ESET Online Help. URL: https://help.eset.com/protect_cloud/uk-UA/cloud_security.html (дата звернення: 15.10.2025).

3. Автоматизація ESET PROTECT. ESET Online Help. URL: https://help.eset.com/protect_cloud//uk-UA/admin_how_to_automate.html (дата звернення: 15.10.2025)

Талан Анна Владиславівна
Студентка групи БСДМ-52, ННІКБЗІ, Київ, Україна

БЕЗПЕКА ХМАРНИХ ТЕХНОЛОГІЙ: ВИКЛИКИ ТА РЕЗИЛЬЄНТНІСТЬ

Що ми розуміємо під безпекою хмарних технологій? Це комплекс заходів, методів та технологій, спрямованих на забезпечення конфіденційності, цілісності та доступності даних, що зберігаються або обробляються у хмарному середовищі. Хмарні сервіси сьогодні використовуються як приватними компаніями, так і державними структурами, адже вони дають змогу гнучко масштабувати ресурси та оптимізувати витрати. Проте разом із перевагами виникають і ризики – несанкціонований доступ, витік даних, збої в роботі сервісів. Саме тому питання кібербезпеки в хмарних системах стає одним із ключових напрямів захисту інформації у сучасному цифровому світі.

Ключові слова: хмарні технології, кібербезпека, моделі розгортання, контроль доступу, шифрування даних, багаторівневий захист, управління ризиками, безпека даних, моніторинг інцидентів.

Завдяки своїй масштабованості, гнучкій інфраструктурі та економії коштів хмарні обчислення стають дедалі популярнішими як у корпоративному, так і в державному секторі. Однак поширення хмарних послуг пов'язане зі зростанням кіберзагроз, пов'язаних із втратою конфіденційності, цілісності та доступності даних. [1]

Модель спільної відповідальності передбачає розподіл відповідальності між постачальником та клієнтом. [2] Нерозуміння цього принципу призводить до прогалин у безпеці.

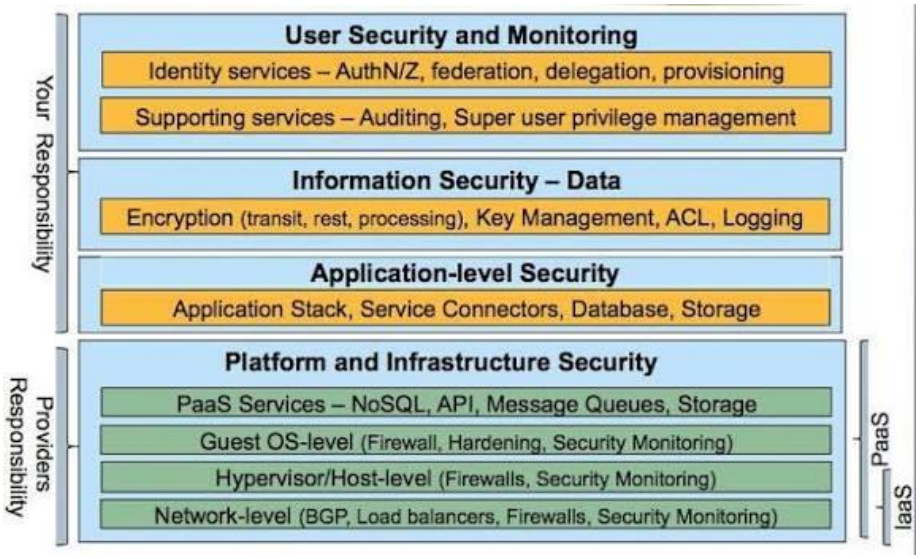

Рис. 1 – Архітектура безпеки хмарної інфраструктури

До основних загроз належать порушення конфіденційності, цілісності та доступності даних внаслідок помилок конфігурації, вразливості API та порушення безпеки облікових записів. [3]

Захист хмарних систем включає шифрування даних у стані спокою та під час передачі, управління ключами, правила мінімальних прав та централізоване моніторингування подій безпеки. Впровадження централізованого моніторингу подій безпеки та застосування систем SIEM (Security Information and Event Management) і SOAR (Security Orchestration, Automation, and Response) дозволяє швидко виявляти аномалії та реагувати на інциденти. [4]

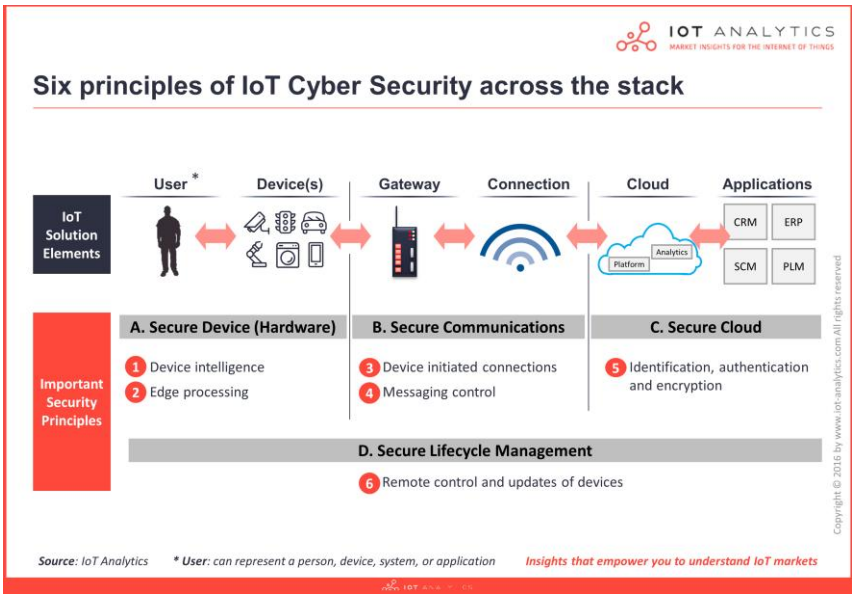

Рис. 2 – Архітектура безпеки IoT: рівні пристроїв, передачі, хмари, додатків

У контексті військової агресії проти України особлива увага приділяється суверенітету даних, оскільки деякі хмарні ресурси можуть бути фізично розташовані за межами країни. [5] Слід враховувати правові ризики, регуляторні аспекти та підвищену потребу в стійкості та надмірності даних.

Безпека хмари вимагає системного підходу, що включає технічні, організаційні та правові заходи. Ефективна модель безпеки хмари включає прозору взаємодію з постачальником, безпечну архітектуру, механізми контролю доступу та постійний моніторинг загроз. [6]

Перелік посилань:

1. 50 Endpoint Security Stats You Should Know. Expert Insights. URL: https://expertinsights.com/insights/50-endpoint-security-stats-you-should-know/.
2. Verma A., Kaushal S. Cloud Computing Security Issues and Challenges: A Survey. ResearchGate. URL: https://www.researchgate.net/publication/220790184_Cloud_Computing_Security_Issues_and_Challenges_A_Survey
3. Akinade A. O. Cloud Security Challenges and Solutions: A Review of Current Best Practices. ResearchGate. URL: https://www.researchgate.net/publication/387558426_Cloud_Security_Challenges_and_Solutions_A_Review_of_Current_Best_Practices.
4. Systematic Literature Review on Cloud Computing Security. SSRN. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4775074.

5. Koverznev V. Legal Regulation of the Cloud Services Market of Ukraine. European Journal of Sustainable Development. URL: https://ecsdev.org/ojs/index.php/ejsd/article/download/1499/1472/2902.

6. National Institute of Standards and Technology (NIST). Cloud Computing Security Reference Architecture. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-292.pdf.

Ботвінніков М.А.
студент групи 125-22-4,
НТУ «Дніпровська політехніка»,
Дніпро, Україна

Мєшков В.І.
старший викладач каф. БІТ,
НТУ «Дніпровська політехніка»,
Дніпро, Україна

Дослідження біометричних методів автентифікації та оцінка ризиків їх впровадження у сучасних інформаційних системах

У добу цифрової трансформації автентифікація користувачів стає критичним елементом інформаційної безпеки. Традиційні паролі й токени все частіше поступаються місцем біометричним технологіям, які використовують унікальні фізіологічні (обличчя, райдужка, відбитки пальців) або поведінкові характеристики (мова, підпис, динаміка натискання клавіш). Біометрія підвищує зручність та ефективність ідентифікації, однак її впровадження пов'язане з низкою ризиків – технічних, правових і етичних, особливо у критичних інфраструктурах.

Ключові слова: біометрична автентифікація, інформаційна безпека, спуфінг-атаки, нейронні мережі, deepfake, критична інфраструктура, захист даних.

У сучасну цифрову епоху автентифікація користувачів посідає ключове місце в системах інформаційної безпеки. Зростання обсягів даних і поширення віддалених сервісів призвели до того, що традиційні методи перевірки особи, засновані на паролях і токенах, стають дедалі вразливішими. Біометричні технології, які використовують унікальні фізіологічні або поведінкові характеристики людини, поступово формують нову парадигму цифрової ідентифікації. Їхня перевага полягає у високій зручності та швидкості доступу, проте впровадження таких систем супроводжується значними ризиками, пов'язаними з точністю, приватністю та можливістю підробки біометричних даних.

Сучасні біометричні системи поділяються за типом ознак, які використовуються для розпізнавання. До фізіологічних належать методи, засновані на аналізі відбитків пальців, обличчя, райдужки ока або геометрії вен, тоді як поведінкові методи орієнтовані на аналіз індивідуальних шаблонів руху, голосу, темпу натискання клавіш або особистого підпису. Відомими прикладами реалізації є технології Face ID від Apple, Windows Hello від Microsoft та Samsung Iris Recognition, а також стандартизовані рішення на основі FIDO2/WebAuthn, у яких біометричні параметри поєднуються з криптографічними ключами, не залишаючи шаблони у відкритому вигляді на сервері. Це дозволяє підвищити рівень безпеки та уникнути централізованих витоків даних.

Як зазначають Швець і Фесенко [1], ефективність біометричної автентифікації залежить від балансу між рівнем безпеки і зручністю користувача. Водночас Журавльов і Польшакова [2] доводять, що вразливість більшості систем зумовлена відсутністю механізмів перевірки «живості», що відкриває можливості для спуфінг-атак, коли зловмисники використовують фотографії,

відеозаписи або тривимірні маски для обману алгоритмів розпізнавання. Технологічним рішенням цієї проблеми є системи liveness detection, які аналізують мікрорухи очей, реакцію зіниці на освітлення, спектральне відбиття шкіри або параметри глибини сцени.

У дослідженні Korchenko та співавт. [3] описано модульну нейронну мережу, призначену для біометричної автентифікації персоналу критичної інфраструктури. Її архітектура поєднує дані про обличчя та райдужну оболонку ока, що забезпечує нижчий рівень помилок розпізнавання та підвищену стійкість до спуфінг-атак, а також дозволяє працювати за умов недостатнього освітлення або часткового закриття обличчя. Проте навіть такі удосконалені рішення залишаються вразливими до нових викликів, зокрема до атак із використанням технологій deepfake. У роботі Не та співавт. [4] зазначено, що системи, які базуються на статичних модальностях – таких як обличчя або голос – є особливо чутливими до підробок, створених генеративними моделями. Автори пропонують багаторівневу модель захисту, що поєднує аналіз динамічних характеристик, міміки, рухів очей і синхронізації аудіо-відео сигналів із підвищенням обізнаності користувачів щодо потенційних загроз.

Оцінювання надійності біометричних систем здійснюється на основі кількісних метрик, зокрема показників FAR (False Acceptance Rate), FRR (False Rejection Rate), EER (Equal Error Rate) та PAD (Presentation Attack Detection) Index, які відображають імовірність помилкового прийняття зловмисника, відмови легітимному користувачеві, баланс між ними та ефективність виявлення атак. Відповідно до стандартів NIST SP 800-63B та ISO/IEC 2382-37, безпечною вважається система, у якій FAR не перевищує 0,001 %, реалізована перевірка живості, а біометричні шаблони зберігаються у зашифрованому вигляді та не можуть бути відновлені у первинну форму. Для забезпечення більшої стійкості до атак у критичних інфраструктурах рекомендується поєднувати біометрію з криптографічними токенами або одноразовими кодами, створюючи багатофакторні моделі автентифікації.

Крім технічних показників, важливою складовою оцінки ризику є правові та етичні аспекти використання біометрії. Біометричні шаблони належать до категорії чутливих персональних даних, тому їх обробка повинна відповідати вимогам Закону України «Про захист персональних даних» і Загального регламенту ЄС про захист даних (GDPR).

Це передбачає інформовану згоду користувачів, прозорість процедур збору та зберігання даних, а також неможливість використання біометричної інформації з метою дискримінації або масового нагляду.

Висновок.

Біометрична автентифікація посідає вагоме місце у розвитку сучасних інформаційних систем. Найперспективнішими напрямами є поєднання фізіологічних і поведінкових ознак, упровадження систем перевірки живості, використання криптографічного захисту шаблонів, регулярний аудит безпеки та правове регулювання процесів обробки даних.

Лише баланс між технологічною ефективністю, етичністю та правовою відповідністю може забезпечити довіру користувачів і безпечне використання біометричних технологій у корпоративному й державному секторах.

Перелік посилань:

1. Швець, В. А., Фесенко, А. О. Basic biometric characteristics, modern systems & technologies of biometric authentication // Ukrainian Scientific Journal of Information Security. – 2024. – DOI: 10.18372/2225-5036.19.4882.

2. Журавльов, Д., Польшакова, О. Виявлення спуфінг-атак на системи біометричної ідентифікації за обличчям // Адаптивні системи автоматичного управління. – Київ: КПІ ім. Ігоря Сікорського, 2023. – DOI: 10.20535/1560-8956.42.2023.279095.

3. Korchenko, O., Tereikovskyi, I., Ziubina, R. та ін. Modular Neural Network Model for Biometric Authentication of Personnel in Critical Infrastructure Facilities Based on Facial Images // Applied Sciences. – 2025. – Vol. 15, No. 5. – Article 2553. – DOI: 10.3390/app15052553.

4. He, S., Lei, Y., Zhang, Z., Sun, Y., Li, S., Zhang, C., Ye, J. Identity Deepfake Threats to Biometric Authentication Systems: Public and Expert Perspectives [Електронний ресурс] // arXiv preprint. – 2025. – arXiv:2506.06825. – Режим доступу: https://arxiv.org/abs/2506.06825 (дата звернення: 12.10.2025).

Калалб Дмитро Олександрович
Студент Державного торгівельно-економічного університету
Науковий керівник - Терейковський Ігор
Київ, Україна

РОЗРОБКА КОМПЛЕКСУ ЗАХОДІВ ЩОДО ЗАХИСТУ ВЕБЗАСТОСУНКІВ ВІД DDOS-АТАК НА ОСНОВІ ПЛАТФОРМИ IBM CIS

Що ми розуміємо під захистом вебзастосунків від DDoS-атак? DDoS-атаки (Distributed Denial of Service) — це цілеспрямовані дії, метою яких є перевантаження вебресурсу шляхом надсилання великої кількості запитів із різних джерел. Такі атаки призводять до зниження продуктивності серверів, тимчасової недоступності сервісів, фінансових втрат та зниження довіри користувачів.

Ключові слова: DDoS, IBM Cloud Internet Services, вебзастосунки, кіберзахист, хмарні технології.

Зростання кількості DDoS-атак у світі є одним із головних викликів для сучасної кібербезпеки. За даними Akamai (2024), кількість атак зросла на 65% порівняно з попереднім роком, а середня тривалість збільшилася до кількох годин[1].

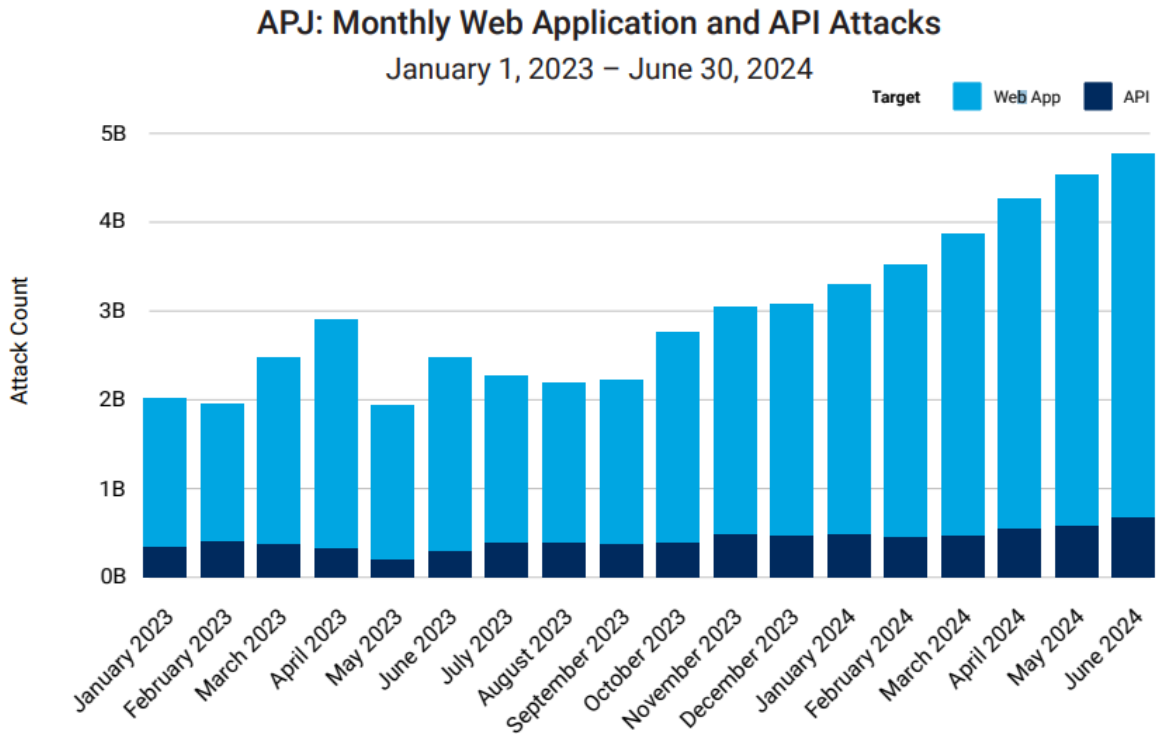

Рис. 1 - Графік зросту кількості атак від Akamai

Такі атаки часто носять мультивекторний характер — одночасно використовуються UDP-флуди, SYN-флуди, HTTP-флуди та DNS-amplification, що значно ускладнює їх виявлення стандартними засобами.

DDoS-атаки спрямовані на виведення з ладу вебресурсів шляхом перевантаження серверів великим обсягом запитів. Для бізнесу це означає втрату доступності послуг, фінансові збитки, падіння довіри користувачів та репутаційні ризики. Особливо небезпечними є атаки на прикладному рівні (Layer 7), які імітують легітимні дії користувачів, тому потребують глибокого аналізу поведінки трафіку[2].

Проблема протидії DDoS-атакам актуальна й для України. Під час повномасштабної війни зафіксовано численні атаки на державні портали, банки та операторів зв’язку. Це підтверджує необхідність впровадження надійних хмарних рішень, здатних забезпечити фільтрацію трафіку на глобальному рівні.

Платформа IBM Cloud Internet Services (CIS) є одним із таких рішень. Вона поєднує можливості CDN, Web Application Firewall (WAF), DDoS Protection, DNSSEC, Global Load Balancer та SSL/TLS-шифрування. Усі компоненти базуються на Anycast-архітектурі, що дозволяє рівномірно розподіляти навантаження між географічно рознесеними датацентрами IBM[3].

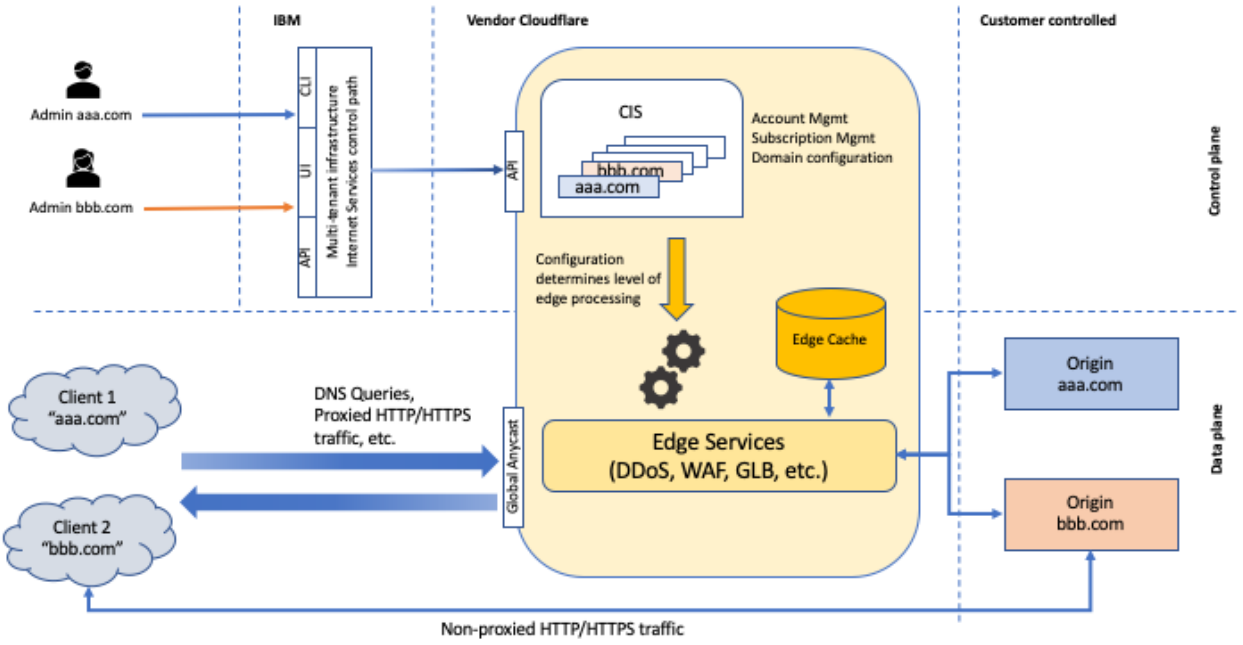

Рис. 2 - Архітектура рішення IBM Cloud Internet Services

Основою захисту є автоматичне виявлення аномального трафіку за допомогою аналітики на базі AI та машинного навчання. Система використовує поведінкові моделі для розпізнавання бот-активності, аналізує TLS-профілі, запроваджує політику Rate Limiting і в разі перевантаження автоматично перенаправляє шкідливий трафік на фільтраційні вузли.

До комплексу заходів, розробленого в межах дослідження, увійшли:

- Інтеграція IBM CIS у корпоративну інфраструктуру з використанням API-інтерфейсів і Terraform;
- Використання глобального балансування навантаження (GLB) для перенаправлення трафіку на доступні сервери;
- Налаштування Web Application Firewall за шаблонами OWASP Top 10;
- Застосування IP Firewall для блокування підозрілих діапазонів IP;
- Впровадження Rate Limiting і CAPTCHA для протидії ботам;
- Моніторинг через IBM Cloud Dashboard у режимі реального часу[3].

Практичне тестування комплексу проводилось за допомогою утиліти Apache JMeter з імітацією HTTP GET/POST-флуду.

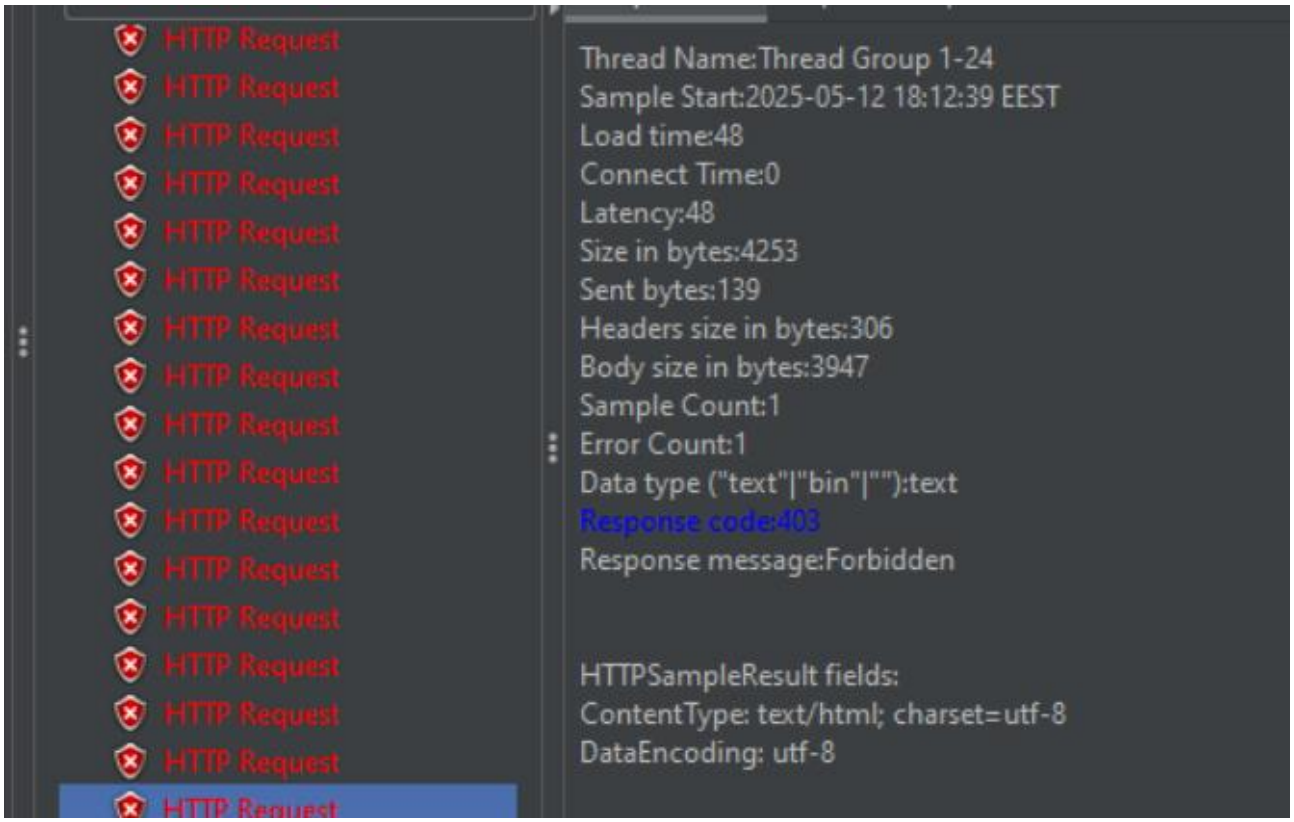

Рис. 3 - Результати тестування DDoS-захисту у середовищі IBM CIS (Apache JMeter)

Після активації WAF і DDoS Protection навантаження на сервер знизилось у середньому на 70–80%, а час відновлення доступності зменшився до 30 секунд після припинення атаки. Це підтверджує ефективність обраної архітектури IBM CIS для запобігання розподіленим атакам.

Використання IBM CIS також дозволяє інтегрувати систему з SIEM-рішеннями (наприклад, IBM QRadar)[3], що дає змогу автоматизувати процеси збору подій безпеки, виявлення інцидентів та генерації звітів. Такий підхід підвищує рівень готовності організації до реагування на загрози у рамках SOC.

Запропонований комплекс заходів на базі IBM CIS забезпечує багаторівневий захист вебзастосунків від DDoS-атак завдяки інтеграції інтелектуальних алгоритмів фільтрації, глобальному балансуванню навантаження та автоматизації моніторингу. Рішення може бути рекомендоване до впровадження в корпоративних мережах, хмарних середовищах та державних установах для підвищення рівня кіберстійкості вебресурсів.

Перелік посилань:

1. Akamai. *State of the Internet Security Report 2024.* Akamai Technologies. URL: https://www.akamai.com/site/en/documents/state-of-the-internet/2024/securing-apps-report.pdf
2. Cloudflare. *Understanding DDoS Attacks and Mitigation Mechanisms.* Cloudflare Inc. URL: https://www.cloudflare.com/learning/ddos
3. IBM Cloud Internet Services Documentation. IBM. URL: https://cloud.ibm.com/docs/cis

Поремський Ярослав Сергійович,
студент групи БСДМ-51, ННІКБЗІ ДУІКТ, Київ, Україна
Журавель Олександр Олегович
студент групи БСДМ-51, ННІКБЗІ ДУІКТ, Київ, Україна

РОЛЬ МЕТРИК ЕФЕКТИВНОСТІ В РОБОТІ SOC

Ефективність операційного центру безпеки (SOC) неможлива без чітких вимірювань, що відображають зрілість процесів і здатність протистояти кіберзагрозам. Такі показники, як час виявлення та реагування на інциденти, рівень хибних спрацювань чи частка ескалацій, формують основу оцінки роботи SOC. Вони дозволяють організації не лише контролювати власну стійкість, а й вибудовувати стратегії вдосконалення, забезпечуючи баланс між швидкістю, точністю та якістю захисту інформаційних активів.

Ключові слова: SOC, метрики ефективності, ескалація інцидентів, кібербезпека, оцінка продуктивності.

У світі, де кіберзагрози стають дедалі складнішими, функціонування SOC неможливе без постійного вимірювання власної результативності. Саме кількісні показники дозволяють не лише описати поточний стан справ, а й спрямувати зусилля команди на вдосконалення. Метрики стають інструментом зворотного зв'язку: вони демонструють, як швидко SOC реагує на події, наскільки точно системи розрізняють справжні атаки від шуму, і чи спроможні аналітики першої лінії самостійно нейтралізувати більшість інцидентів.

MTTD та MTTR: вимірювання швидкості SOC

Одними з ключових показників є **MTTD** (середній час виявлення) та **MTTR** (середній час реагування). Якщо SOC здатний виявити загрозу за хвилини, це значно обмежує можливості зловмисника для розвитку атаки. Якщо ж час реагування надто великий, організація ризикує зазнати суттєвих збитків навіть попри швидке виявлення. Ці два показники дозволяють оцінити не лише технології, а й якість взаємодії між людьми та процесами [1].

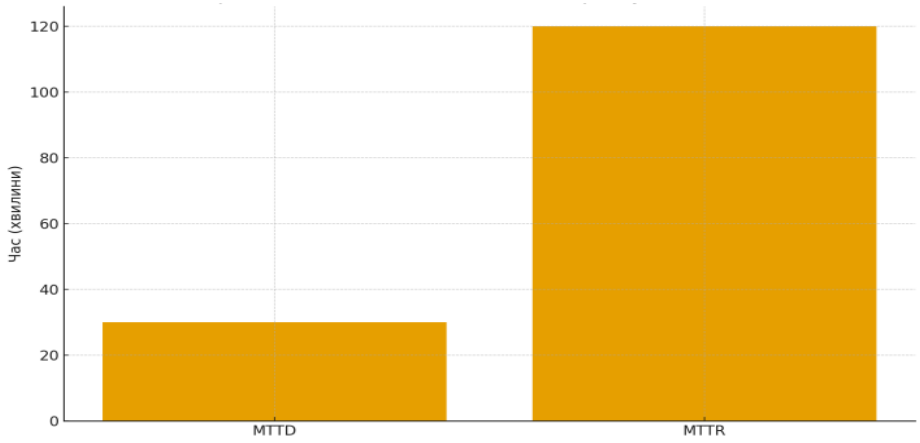

Рис. 1 – Середній час виявлення (MTTD) та реагування (MTTR)

У цьому умовному сценарії (рис. 1) SOC досягає середнього часу виявлення близько 30 хвилин, тоді як середній час реагування становить 2 години (120 хвилин). Така різниця означає, що хоча загрози виявляються доволі

швидко, їх повне усунення займає більше часу. Зменшення обох показників – особливо MTTR – є критично важливим для обмеження впливу інцидентів: що швидше команда нейтралізує загрозу після виявлення, то меншими будуть потенційні збитки та час простою систем. Постійний моніторинг MTTD і MTTR дозволяє оцінити ефективність впроваджених заходів (нових інструментів моніторингу, автоматизації, навчань команди тощо) та виявити "вузькі місця" у процесі реагування.

Рівень хибних спрацювань: баланс точності й навантаження

Не менш важливим є **False Positive Rate (FPR)** – показник кількості оповіщень, що виявилися помилковими. Якщо цей рівень занадто високий, команда SOC витрачає час на перевірку інцидентів, яких насправді не існує. Це призводить до явища «alert fatigue», коли аналітики втрачають увагу до справжніх атак. З іншого боку, надмірне зниження FPR без належного налаштування може призвести до пропуску реальних загроз. Тому завдання SOC полягає у досягненні здорового балансу між чутливістю й точністю [1].

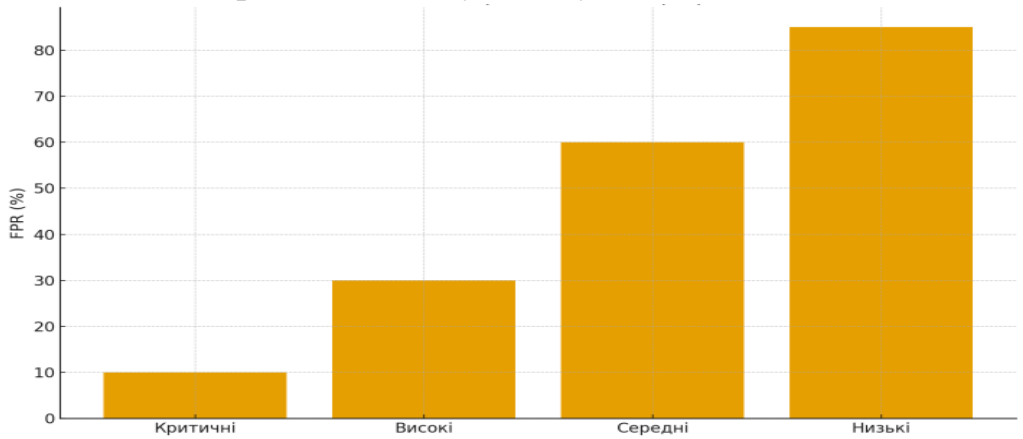

Рис. 2 – Рівень хибних спрацювань (False Positive Rate) за пріоритетом

Високий рівень FPR (рис. 2) свідчить про велику кількість помилкових тривог, що призводить до «втоми від оповіщень» і відволікає аналітиків від справжніх загроз. Для критичних інцидентів FPR має бути мінімальним (менше 25%), а для менш важливих – вищим (до 50-75%). Налаштування правил виявлення для зменшення FPR покращує ефективність SOC і дозволяє команді зосередитися на реальних загрозах, підвищуючи її продуктивність і довіру до систем моніторингу.

Коефіцієнт ескалацій: віддзеркалення зрілості команди

Ще однією показовою метрикою є **Incident Escalation Rate** – частка випадків, які аналітики передають на вищий рівень. Занадто високий показник може сигналізувати про складність інцидентів або недостатню підготовку першої лінії, натомість надто низький коефіцієнт може означати, що команда уникає ескалацій навіть тоді, коли вони необхідні. Оптимальний рівень показує, що SOC ефективно розподіляє навантаження: більшість загроз вирішуються одразу, але критичні випадки своєчасно передаються фахівцям вищого рівня.

Високий коефіцієнт ескалацій для критичних інцидентів (50%) логічний, оскільки серйозні атаки часто вимагають втручання експертів. Для інцидентів

високого рівня пріоритету ескалація відбувається в 20% випадків, середнього – в 10%, а низького – лише 5%. Це свідчить, що менш серйозні загрози вирішуються на першій лінії. Високий коефіцієнт ескалацій для певних інцидентів може вказувати на прогалини в знаннях чи інструментах команди першої лінії. Зниження кількості непотрібних ескалацій допомагає підвищити ефективність SOC, зменшивши час на розв'язання проблем [2].

Виклики у зборі та використанні метрик

Хоча метрики є потужним інструментом управління SOC, їх правильне запровадження та інтерпретація можуть бути непростими. По-перше, потрібно мати налагоджений збір даних: автоматичне логування часів виявлення, реагування, закриття інцидентів тощо. Без якісних даних показники MTTD чи MTTR можуть виявитися неточними. По-друге, важливо чітко визначити, що саме вважати "інцидентом", "помилковим спрацюванням" тощо – узгоджені дефініції гарантують, що метрики відображають реальний стан справ. Інша проблема – **інтерпретація метрик** у правильному контексті. Наприклад, високий MTTR в одній організації може бути обумовлений складністю атак, з якими вона стикається, а не повільністю команди [2]. Тому метрики слід порівнювати не тільки з усередненими "галузевими" значеннями, а й з власними історичними показниками (трендами) та цілями, які відповідають ризик-профілю і ресурсам конкретної компанії. Ще один виклик – не перетворити відстежування метрик на самоціль. Якщо метрики не пов'язані з реальними цілями безпеки й бізнесу, вони перетворюються на "фоновий шум" і можуть ввести в оману. Наприклад, прагнучи знизити FPR, команда може несвідомо почати ігнорувати частину сповіщень (ризик збільшення false negatives) – такий "обман метрикою" матиме протилежний ефект на безпеку. Таким чином, керівники SOC повинні уважно добирати, які показники відслідковувати, і пояснювати команді їх значення. Метрики мають слугувати інструментом для прийняття рішень, а не просто цифрами в звіті.

Перелік посилань:

1. Fortinet. Essential Metrics to Track for Successful Security Operations. — Fortinet CyberGlossary. URL: https://www.fortinet.com/resources/cyberglossary/secops-metrics#:~:text=KPIs%20like%20mean%20time%20to,threat%20identification%20across%20the%20environment (дата звернення: 05.10.2025).

2. Tamnoon. SOC Metrics: Types, Best Practices, and How to Use Them Effectively. URL: https://tamnoon.io/blog/soc-metrics-types/#:~:text=But%20without%20clear%2C%20meaningful%20metrics%2C,a%20SOC%2C%20noise%20is%20expensive (дата звернення: 05.10.2025).

Кравченко Ярослав Ігорович,
БСДМ-63
Державний університет
інформаційно-комунікаційних технологій,
м. Київ

ТЕХНОЛОГІЯ ЗАХИСТУ ВЕБ ДОДАТКІВ ВІД DDOS-АТАК НА ОСНОВІ AWS WAF

Визначено мету і основні завдання щодо захисту веб додатків від DDoS-атак. Розглянуто зміст технології захисту веб додатків від DDoS-атак на основі AWS WAF.

Сучасні веб-сайти – це складні багатокомпонентні додатки, які обслуговують різноманітних користувачів та пристроїв – браузери від різних розробників, мобільні додатки та інші онлайн-сервіси, що взаємодіють через HTTP-запити та API. На відміну від десятирічної давності, сучасні веб-додатки покладаються на передові технології, такі як AJAX, API та BFF (Backend-for-Frontend), для забезпечення безперебійного взаємодії [1].

Однак, ця архітектурна складність має й зворотний бік: більшу вразливість до кіберзагроз, включаючи DDoS-атаки. Веб-сайти мають бути захищені на кількох рівнях моделі OSI, включаючи мережевий (L3), транспортний (L4) та прикладний (L7) рівні [1].

В останні роки «розумні» атаки на рівні додатків стають дедалі поширенішими. На відміну від традиційних DDoS-атак, вони спрямовані не лише на протоколи HTTP/HTTPs, а й на те, як серверні компоненти взаємодіють з клієнтськими модулями та іншими системами, такими як бази даних (СУБД) або шини даних. Зловмисники використовують слабкі місця в цих взаємодіях, щоб порушувати роботу таким чином, що стандартні засоби захисту можуть не виявити їх [1].

AWS WAF – це брандмауер веб-застосунків, який дозволяє фахівцям контролювати та керувати веб-запитами, що пересилаються до захищених ресурсів AWS. За допомогою AWS WAF ми можемо захистити такі ресурси, як дистрибутиви Amazon CloudFront, REST API Amazon API Gateway, балансувальники навантаження додатків та API AWS AppSync GraphQL. Ми можемо використовувати AWS WAF для перевірки веб-запитів на відповідність заданим умовам, таким як IP-адреса, з якої надходять запити, значення певного компонента запиту або швидкість надсилання запитів. AWS WAF може керувати запитами на відповідність різними способами, включаючи їх підрахунок, блокування або дозвіл, а також надсилання завдань, таких як головоломки CAPTCHA, користувачеві клієнта або браузеру [2].

Місце рішення AWS WAF в загальній архітектурі AWS та основний функціонал показано на рисунку 1:

AWS WAF – розгортає веб-список контролю доступу AWS WAF, групи правил керованих правил AWS, користувацькі правила та набори IP-адрес.

Здійснює виклики API AWS WAF для блокування поширених атак та захисту веб-застосунків.

Amazon Data Firehose – доставляє журнали AWS WAF до корзин Amazon S3.

Амазон S3 – зберігає журнали AWS WAF, CloudFront та ALB.

AWS Lambda – розгортає кілька лямбда-функцій для підтримки користувацьких правил.

Amazon EventBridge – створює правила подій для виклику Lambda.

Amazon Athena – створює запити Athena та робочі групи для підтримки парсера журналів Athena.

AWS Glue – створює бази даних і таблиці для підтримки парсера журналів Athena.

Amazon SNS – надсилає сповіщення електронною поштою Amazon Simple Notification Service (Amazon SNS) для підтримки збереження IP-адрес у списках дозволених та заборонених.

AWS Systems Manager – забезпечує моніторинг ресурсів на рівні додатка та візуалізацію операцій з ресурсами та даних про витрати.

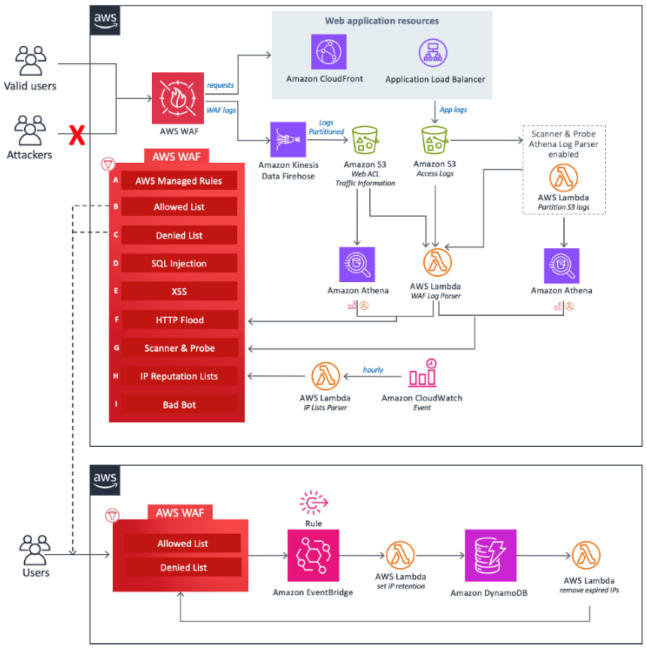

Рис. 1. Місце рішення AWS WAF в загальній архітектурі AWS та основний функціонал [3]

Захист веб додатків від DDoS-атак за допомогою AWS WAF – це багаторівневий процес, який поєднує автоматичні засоби захисту та власні правила для фільтрації шкідливого трафіку. Розглянемо основні дії для реалізації ефективного захисту.

Крок 1: Створення архітектури та інтеграція AWS WAF.

Перш за все, важливо правильно побудувати архітектуру. AWS WAF працює разом з іншими сервісами AWS, тому ключовим є розміщення додатків за ресурсами, що підтримують WAF.

Необхідно використовувати AWS Edge сервіси: необхідно розмістити

корпоративний додаток за Amazon CloudFront (для глобального контенту) або Application Load Balancer (ALB) (для регіонального). Це створює перший рубіж оборони та дозволяє WAF аналізувати трафік ще до того, як він досягне сервера.

Необхідно створити Web ACL (Access Control List): Web ACL – це контейнер для правил, які застосовуються до трафіку. Ми створюємо один Web ACL і пов'язуємо його з відповідним ресурсом (CloudFront або ALB).

Крок 2: Налаштування Керованих Правил (AWS Managed Rules).

Це найпростіший і найшвидший спосіб отримати базовий захист. AWS надає готові набори правил, розроблені для захисту від поширених загроз.

Amazon IP reputation list: необхідно увімкнути групу правил *AmazonIpReputationList*. Вона автоматично блокує запити з IP-адрес, які відомі як джерела ботів або іншої шкідливої активності.

Core rule set (CRS): необхідно додати групу правил *AWSManagedRulesCommonRuleSet*. Вона захищає від широкого спектра вразливостей, таких як SQL-ін'єкції та міжсайтовий скриптинг (XSS), які часто є частиною DDoS-атак на рівні додатку.

Anonymous IP list: необхідно розглянути можливість увімкнення *AWSManagedRulesAnonymousIpList* для блокування трафіку з анонімних проксі, VPN та Tor, які часто використовуються для атак.

Bot Control: необхідно увімкнути групу правил для контролю ботів, щоб ідентифікувати та блокувати шкідливий автоматизований трафік.

Крок 3: Створення Власних Правил (Custom Rules).

Для більш специфічного захисту, адаптованого до конкретного додатку, необхідно створити власні правила. Правила на основі частоти запитів (Rate-Based Rules) – це найважливіший інструмент протидії HTTP-флуду (найпоширеніший тип DDoS-атак на рівні додатку).

Необхідно створити загальне правило: необхідно налаштувати правило, яке блокує будь-яку IP-адресу, що надсилає надмірну кількість запитів. Наприклад, заблокувати IP, якщо кількість запитів перевищує 1000 за 5 хвилин.

Необхідно створити специфічні правила: необхідно визначити «важкі» для корпоративного сервера запити (наприклад, сторінка входу, пошук, API-ендпоїнти) і встановіть для них більш жорсткі ліміти. Наприклад, не більше 100 запитів за 5 хвилин на сторінку /login.

Необхідно застосовувати географічне блокування (Geographic Match Rules). Якщо бізнес орієнтований на певні країни, можна заблокувати трафік з регіонів, звідки ми не очікуємо легітимних користувачів. Це може значно зменшити поверхню атаки.

Необхідно здійснювати блокування за IP-адресами (IP Set Match Rules). Під час атаки ми можемо аналізувати лог-файли, ідентифікувати IP-адреси зловмисників і додавати їх до списку блокування (IP set) вручну або автоматично.

Правила на основі сигнатур (String and Regex Match Rules). Необхідно створити правила, які перевіряють частини запиту (наприклад, User-Agent, URI, query string) на наявність певних патернів, характерних для атаки, і блокують їх.

Крок 4: Моніторинг, Логування та Автоматизація.

Захист – це безперервний процес, а не одноразове налаштування. Необхідно ввімкнути логування. Обов'язково активуйте логування для корпоративного Web ACL. Логи можна надсилати в Amazon S3 через Kinesis Data Firehose для подальшого аналізу.

Необхідно налаштувати сповіщення. Використовується Amazon CloudWatch для моніторингу метрик WAF (наприклад, кількість заблокованих запитів). Необхідно налаштувати сповіщення (Alarms), які повідомлятимуть про аномальні сплески трафіку.

Здійснюється автоматизація реагування. Для цього використовується AWS Lambda для автоматизації реагування на загрози. Наприклад, можна створити функцію, яка автоматично аналізує логи, виявляє IP-адреси атакуючих і додає їх до списку блокування в WAF.

Крок 5: Інтеграція з AWS Shield Advanced.

Для критично важливих додатків рекомендується використовувати AWS Shield Advanced. AWS Shield Standard надається безкоштовно і захищає від поширених DDoS-атак на мережевому та транспортному рівнях (L3/L4). AWS Shield Advanced – це платний сервіс, що пропонує:

розширений захист від атак на рівні додатку (L7);

цілодобовий доступ до команди реагування на DDoS-атаки (DDoS Response Team);

захист від фінансових втрат, пов'язаних зі сплесками трафіку під час атаки;

автоматичне пом'якшення атак на рівні додатку.

Таким чином, поєднання AWS WAF з правильно налаштованими керованими та власними правилами, а також інтеграція з AWS Shield Advanced створює надійний та ешелонований захист від більшості видів DDoS-атак.

Література

1. How to Protect Websites and Web Applications from DDoS Attacks. StormWall. URL: https://stormwall.network/resources/blog/how-to-prevent-ddos-attacks-on-websites (дата звернення: 08.10.2025).
2. AWS WAF, AWS Firewall Manager, AWS Shield Advanced, and AWS Shield network security director. Developer Guide. URL: https://docs.aws.amazon.com/waf/latest/developerguide/waf-chapter.html (дата звернення: 08.10.2025).
3. Security Automations for AWS WAF Implementation Guide. URL: https://docs.aws.amazon.com/solutions/latest/security-automations-for-aws-waf/architecture-overview.html (дата звернення: 08.10.2025).

Ковальський Богдан Андрійович,
БСДМ-63
Державний університет
інформаційно-комунікаційних технологій,
м. Київ

Технологія керованого захисту хмарних корпоративних додатків від DDoS-атак на основі AWS Shield

Визначено мету і основні завдання щодо керованого захисту хмарних корпоративних додатків від DDoS-атак. Розглянуто зміст технології керованого захисту хмарних корпоративних додатків від DDoS-атак на основі AWS Shield.

Впровадження хмарних технологій прискорюється на кожному архітектурному рівні, особливо на гібридному, мультихмарному та периферійному, але стратегії безпеки не встигають за цим. 62% організацій розширили хмарні технології на периферії (такі як SASE), 57% розширили гібридну хмару, а 51% перейшли на багатохмарні, фрагментуючі середовища та переважні традиційні засоби захисту на основі периметра. Незважаючи на багаторічні інвестиції в інструменти та стратегії хмарної безпеки, рівень інцидентів зростає, що свідчить про невідповідність між сучасними хмарними середовищами та засобами захисту, призначеними для їх захисту [1].

Керований захист хмарних корпоративних додатків від DDoS-атак передбачає використання спеціалізованих послуг від хмарних постачальників або сторонніх розробників, які використовують багаторівневий захист, постійний моніторинг трафіку та автоматизоване пом'якшення наслідків для захисту корпоративних додатків від об'ємних, протокольних та прикладних атак. Ключові функції включають автоматичне реагування, очищення трафіку, брандмауери веб додатків (WAF), обмеження швидкості та екстрену підтримку для забезпечення безперервності бізнесу.

Великі хмарні постачальники, такі як AWS, Azure та Google Cloud, пропонують власні керовані сервіси захисту від DDoS-атак для захисту корпоративних додатків, розгорнутих на їхній інфраструктурі.

Сервіси захисту хмарних корпоративних додатків від DDoS-атак автоматично виявляють та блокують шкідливий трафік у режимі реального часу, часто протягом кількох секунд, щоб запобігти перебоям у роботі сервісу. Захист включає кілька стратегій захисту для обробки різних типів атак. Масштабні атаки, спрямовані на перевантаження пропускної здатності мережі, обробляються шляхом перенаправлення трафіку до центрів очищення, які фільтрують шкідливий трафік. Складні потоки, такі як HTTP-потоки, пом'якшуються за допомогою таких методів, як JavaScript challenges та обмеження швидкості, часто через WAF. Безперервний моніторинг трафіку допомагає швидко виявляти атаки. Деякі сервіси пропонують доступ до команди екстреного реагування для більш складних ситуацій. Функції обмеження швидкості та дроселювання контролюють кількість запитів, які клієнт може зробити протягом певного періоду часу, щоб запобігти зловживанням.

AWS Shield Standard та AWS Shield Advanced забезпечують захист від розподілених DDoS-атак для ресурсів AWS на мережевому та транспортному рівнях (рівень 3 та 4) і прикладному рівні (рівень 7) [2].

AWS Shield забезпечує захист від широкого спектру відомих векторів DDoS-атак та векторів атак «нульового дня». Виявлення та пом'якшення загроз AWS Shield розроблено для забезпечення захисту від загроз, навіть якщо вони явно не відомі сервісу на момент виявлення. Класи атак, які виявляє AWS Shield, включають [2]:

мережеві об’ємні атаки (рівень 3) – це підкатегорія векторів атак на рівні інфраструктури. Ці вектори намагаються перевантажити потужність цільової мережі або ресурсу, щоб відмовити в обслуговуванні легітимним користувачам;

атаки мережевого протоколу (рівень 4) – це підкатегорія векторів атак інфраструктурного рівня. Ці вектори зловживають протоколом, щоб відмовити в обслуговуванні цільового ресурсу. Поширеним прикладом атаки мережевого протоколу є перевантаження TCP SYN, яке може виснажити стан з’єднання на таких ресурсах, як сервери, балансувальники навантаження або брандмауери. Атака мережевого протоколу також може бути об’ємною. Наприклад, більша перевантаження TCP SYN може мати на меті перевантажити пропускну здатність мережі, одночасно виснажуючи стан цільового ресурсу або проміжних ресурсів;

атаки на рівні додатків (рівень 7) – ця категорія векторів атаки намагається відмовити в обслуговуванні легітимним користувачам шляхом перевантаження додатка запитами, які є дійсними для цілі, наприклад, перевантаженням веб-запитів.

Приклад архітектури для веб додатка, стійкої до DDoS-атак, наведено на рисунку 1.

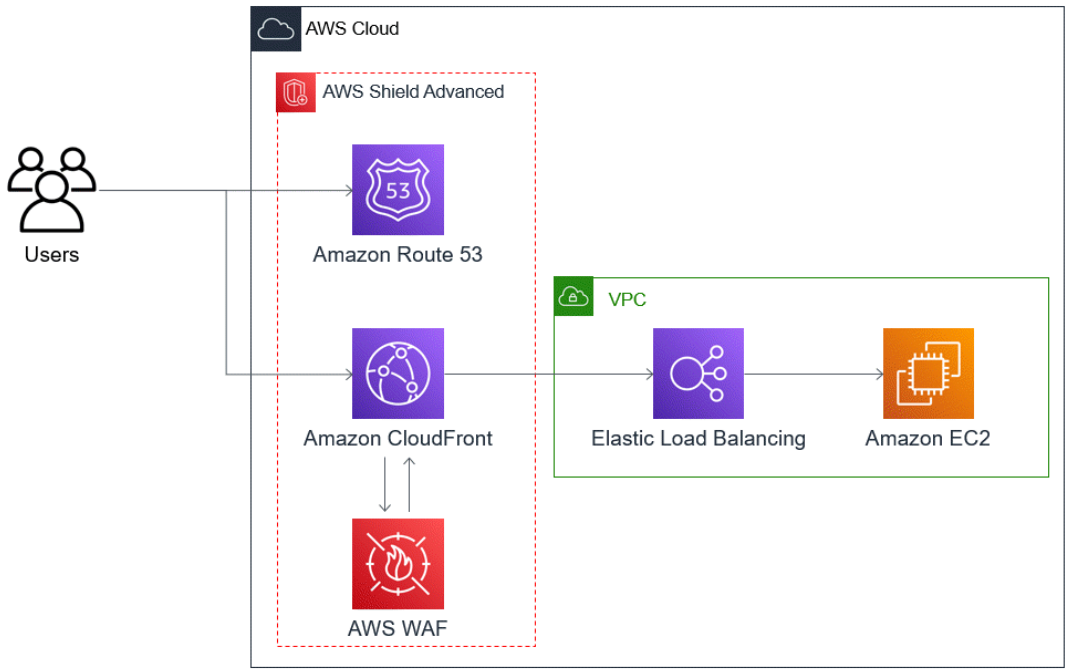

Рис. 1. Архітектура для веб додатка, яка стійка до DDoS-атак [2]

Зміст технології керованого захисту хмарних корпоративних додатків від DDoS-атак на основі AWS Shield [2] включає:

захист від DDoS-атак, що часто використовуються на рівні інфраструктури (рівень 3 та рівень 4), без затримки виявлення. Крім того, якщо ресурс часто є мішенню, AWS Shield Advanced застосовує заходи захисту на триваліші періоди часу. AWS Shield Advanced також використовує контекст додатка, отриманий з мережевих ACL (NACL), для блокування небажаного трафіку далі по черзі. Це ізолює збої ближче до їх джерела, мінімізуючи вплив на законних користувачів;

захист від перевантажень TCP SYN. Системи пом’якшення DDoS-атак, інтегровані з CloudFront, Route 53 та AWS Global Accelerator, забезпечують можливість проксі-сервера TCP SYN, яка перевіряє нові спроби підключення та обслуговує лише легітимних користувачів;

захист від атак на рівні додатків DNS, оскільки Route 53 відповідає за обслуговування авторитетних відповідей DNS;

захист від перевантаження запитами на рівні веб додатків. Правило на основі тарифу, яке налаштовується у своєму веб-списку контролю доступу AWS WAF, блокує вихідні IP-адреси, коли вони надсилають більше запитів, ніж дозволяє правило;

автоматичне пом'якшення DDoS-атак на рівні додатків для корпоративних дистрибутивів CloudFront, якщо вмикається ця опція. Завдяки автоматичному пом'якшенню DDoS-атак AWS Shield Advanced підтримує правило на основі частоти у пов'язаному з дистрибутивом веб-списку контролю доступу AWS WAF, яке обмежує обсяг запитів від відомих джерел DDoS. Крім того, коли AWS Shield Advanced виявляє подію, яка впливає на справність корпоративного додатка, він автоматично створює, тестує та керує правилами пом'якшення у веб-списку контролю доступу;

проактивна взаємодія з командою реагування Shield (SRT), якщо застосовується ця опція. Коли AWS Shield Advanced виявляє подію, яка впливає на працездатність корпоративного додатка, SRT реагує та проактивно взаємодіє з командами безпеки або операцій, використовуючи надану контактну інформацію. SRT аналізує закономірності у корпоративному трафіку та може оновлювати правила AWS WAF, щоб блокувати атаку.

Отже, керований захист хмарних корпоративних додатків від DDoS-атак забезпечує доступність критично важливих сервісів під час атаки, запобігає дороговартісним перебоям у наданні послуг, потенційним юридичним санкціям та втраті доходу.

Література

1. 2025 Cloud Security Report. Check Point. URL: https://www.checkpoint.com/resources/items/report-cloud-security-report-2025 (дата звернення: 13.10.2025).
2. AWS WAF, AWS Firewall Manager, AWS Shield Advanced, and AWS Shield network security director. Developer Guide. URL: https://docs.aws.amazon.com/waf/latest/developerguide/shield-chapter.html (дата звернення: 13.10.2025).

Чуб Г.С.
БСДМ-62
Державний університет
інформаційно-комунікаційних технологій,
м. Київ

ТЕХНОЛОГІЯ КЕРУВАННЯ БЕЗПЕКОЮ В ХМАРІ НА ОСНОВІ СЕРВІСУ AWS SECURITY HUB

Визначено мету і основні завдання щодо керування безпекою в хмарі. Розглянуто зміст технології керування безпекою в хмарі на основі сервісу AWS Security Hub.

Організації будь-якого розміру певним чином використовують хмарні обчислення, що дозволяє їм працювати ефективніше, не беручи на себе тягар повного управління додатками та інфраструктурою. Використання хмарних сервісів продовжує зростати, і за деякими оцінками, світові витрати перевищують 600 мільярдів доларів щорічно. І хоча ці інвестиції відкривають нові та продуктивні способи взаємодії бізнесу з клієнтами, постачальниками, співробітниками та партнерами, побоювання щодо безпеки цих хмарних середовищ є лякаючими. Опитування IT-персоналу та керівників продовжують показувати, що витрати та безпека є головними проблемами, з якими стикаються організації в управлінні використанням хмарних сервісів [1].

Управління хмарною безпекою – це взаємодоповнююча комбінація стратегій, інструментів та практик, метою якої є допомогти бізнесу ефективно та безпечно розміщувати

робочі навантаження та дані в хмарі. Це складне завдання щодо обмеження впливу загроз та вразливостей вимагає дій за кількома напрямками, зокрема [1]:

автентифікація та авторизація. Методи керування користувачами, такі як керування ідентифікацією та доступом, є важливими для забезпечення доступу до хмарних робочих навантажень та даних лише авторизованих користувачів та пристроїв;

безпека даних. Шифрування є вирішальним інструментом захисту цінних бізнес-даних від крадіжки, втрати та іншого несанкціонованого доступу;

відповідні хмарні архітектури. Робочі навантаження краще захищені від пошкоджень, коли вони виконуються на правильно налаштованих хмарних архітектурах;

моніторинг та звітність. Інструменти, які постійно відстежують діяльність та події й надають сповіщення безпеки в режимі реального часу, є важливими для підтримки безпеки хмари.

AWS Security Hub – це уніфіковане хмарне рішення для безпеки, яке визначає пріоритетність критичних проблем безпеки та допомагає фахівцям реагувати на них масштабно. AWS Security Hub виявляє проблеми безпеки, автоматично співвідносячи та збагачуючи сигнали безпеки з різних джерел, таких як управління станом, управління вразливостями (Amazon Inspector), конфіденційні дані (Amazon Macie) та виявлення загроз (Amazon GuardDuty). Це дозволяє командам безпеки визначати пріоритетність активних ризиків у своїх хмарних середовищах за допомогою автоматизованого аналізу та контекстуальної аналітики. Завдяки інтуїтивно зрозумілим візуалізаціям AWS Security Hub перетворює складні сигнали безпеки на практичну аналітику, що дозволяє вам швидко приймати обґрунтовані рішення щодо вашої безпеки. AWS Security Hub також включає автоматизовані робочі процеси реагування, які допоможуть фахівцям усувати ризики, підвищувати продуктивність команди та мінімізувати операційні збої [2].

AWS Security Hub забезпечує єдине місце, яке об’єднує, упорядковує та визначає пріоритети всіх сповіщень безпеки або висновків з кількох облікових записів, інструментів партнерів AWS та сервісів AWS, таких як Amazon GuardDuty, Amazon Inspector, Amazon Macie, AWS IAM Access Analyzer, AWS Firewall Manager та AWS Audit Manager. Основні функції рішення AWS Security Hub показано на рисунку 1.

Рис. 1. Основні функції рішення AWS Security Hub [3]

Схема агрегації джерел даних для рішення AWS Security Hub показана на рисунку 2.

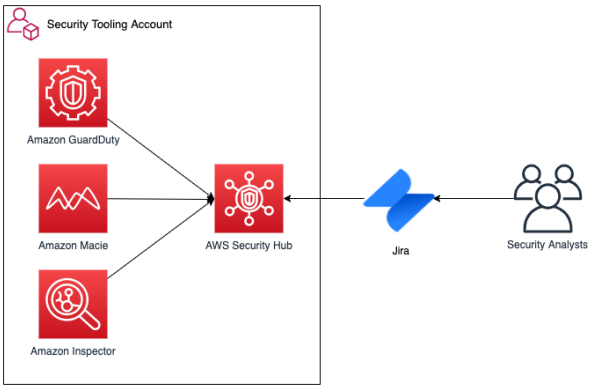

Рис. 2. Схема агрегації джерел даних для рішення AWS Security Hub [4]

AWS Security Hub – це сервіс для керування станом безпеки в хмарі (Cloud Security Posture Management – CSPM), який надає комплексне уявлення про стан безпеки корпоративних ресурсів в AWS. Впровадження цього інструменту дозволяє централізовано керувати попередженнями, автоматизувати перевірки на відповідність стандартам безпеки та своєчасно реагувати на загрози.

Розглянемо порядок ефективне керування безпекою в хмарі з AWS Security Hub. Основними етапами є:

Етап 1: Активація та централізоване налаштування.

Першим кроком є активація Security Hub у корпоративному AWS-акаунті. Для організацій з кількома акаунтами рекомендується використовувати інтеграцію з AWS Organizations. Це дозволяє:

призначити адміністратора: визначити один обліковий запис для централізованого керування Security Hub;

автоматично підключати нові акаунти: нові облікові записи в організації будуть автоматично додаватися до Security Hub;

агрегувати дані: збирати всі знахідки (findings) з різних регіонів та акаунтів в одному місці для єдиного огляду.

На цьому етапі також необхідно увімкнути AWS Config, оскільки Security Hub використовує його для моніторингу конфігурацій ресурсів та перевірки на відповідність правилам безпеки.

Етап 2: Налаштування стандартів безпеки та контролів.

Після активації сервісу необхідно налаштувати стандарти безпеки, які Security Hub буде використовувати для оцінки ваших ресурсів. Доступні такі стандарти:

AWS Foundational Security Best Practices (FSBP): набір основних практик безпеки від AWS;

CIS AWS Foundations Benchmark: рекомендації від Center for Internet Security;

Payment Card Industry Data Security Standard (PCI DSS): Стандарт для організацій, що працюють з платіжними картками;

NIST Special Publication 800-53: Стандарти від Національного інституту стандартів і технологій США.

Ми можемо вмикати або вимикати окремі контролі в межах кожного стандарту, щоб адаптувати їх до специфічних потреб організації та уникнути непотрібних сповіщень.

Етап 3: Інтеграція з іншими сервісами AWS та сторонніми рішеннями.

Перевігою Security Hub полягає в його здатності агрегувати дані з різних джерел. Важливо налаштувати інтеграцію з (рисунок 2):

Amazon GuardDuty: для виявлення загроз;

Amazon Inspector: для керування вразливостями;

Amazon Macie: для виявлення та захисту конфіденційних даних;

AWS Firewall Manager: для централізованого керування брандмауерами;

сторонніми інструментами: Security Hub підтримує інтеграцію з багатьма партнерами AWS, що дозволяє отримувати дані з інших засобів безпеки.

Ці інтеграції збагачують дані, що надходять до Security Hub, надаючи більш повний контекст для кожної знахідки.

Етап 4: Аналіз, пріоритезація та реагування на знахідки.

Після агрегації даних Security Hub надає єдину інформаційну панель (dashboard) для візуалізації стану безпеки. На цьому етапі ключовими є:

пріоритезація: зосередження уваги на знахідках з високим (CRITICAL, HIGH) рівнем серйозності;

використання Insights: створення власних або використання готових Insights для фільтрації та групування знахідок за певними критеріями (наприклад, ресурси з найбільшою кількістю вразливостей);

аналіз шляхів атак: використання візуалізації для розуміння того, як потенційний зловмисник може отримати доступ до корпоративних ресурсів.

Етап 5: Автоматизація реагування та усунення недоліків.

Для ефективного керування великою кількістю знахідок необхідно автоматизувати процеси реагування. Це можна зробити за допомогою:

правил автоматизації (Automation Rules): налаштовуються правила для автоматичної зміни статусу знахідок, рівня їхньої серйозності або для пригнічення несуттєвих сповіщень;

інтеграції з Amazon EventBridge: створюються правила, які будуть запускати певні дії у відповідь на конкретні знахідки. Наприклад, автоматично створювати завдання в Jira, надсилати сповіщення в Slack або запускати AWS Lambda функцію для усунення проблеми;

рішення «Automated Security Response on AWS»: використовуються готові рішення від AWS, яке надає набір автоматизованих сценаріїв (playbooks) для реагування на поширені проблеми безпеки.

Впровадження цих етапів дозволить побудувати надійну систему керування безпекою в хмарі, яка не тільки виявляє проблеми, але й допомагає ефективно та швидко на них реагувати.

Отже, AWS Security Hub – це хмарний інструмент безпеки, який допомагає компаніям контролювати та керувати безпекою AWS, збираючи дані з різних сервісів AWS та сторонніх інструментів – все в одній інформаційній панелі. Він пропонує аналітику безпеки в режимі реального часу та автоматизує перевірки безпеки. AWS Security Hub покращує безпеку хмарних технологій, забезпечуючи централізований моніторинг, виконуючи автоматизовані перевірки безпеки, допомагаючи компаніям дотримуватися стандартів безпеки та інтегруючись із такими сервісами, як Amazon GuardDuty, для виявлення загроз у режимі реального часу.

Література

1. Phil Sweeney, Stephen J. Bigelow. What is cloud security management? A strategic guide. TechTarget. Published: 04 Jun 2024. URL: https://www.techtarget.com/searchsecurity/feature/Guide-to-cloud-security-management-and-best-practices (дата звернення: 08.10.2025).

2. AWS Security Hub User Guide. https://docs.aws.amazon.com/securityhub/latest/userguide/what-are-securityhub-services.html URL: (дата звернення: 08.10.2025).

3. Jon Bonso. AWS Security Hub Cheat Sheet. Last updated on November 14, 2024. URL: https://tutorialsdojo.com/aws-security-hub/ (дата звернення: 08.10.2025).

4. Anuj Gupta and Anna McAbee. Journey to Adopt Cloud-Native Architecture Series #5 – Enhancing Threat Detection, Data Protection, and Incident Response. AWS Architecture Blog. URL: https://aws.amazon.com/blogs/architecture/journey-to-adopt-cloud-native-architecture-series-5-enhancing-threat-detection-data-protection-and-incident-response/ (дата звернення: 08.10.2025).

Гончаренко Радомир Сергійович,
БСДМ-62
Державний університет
інформаційно-комунікаційних технологій,
м. Київ

ТЕХНОЛОГІЯ УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ ХМАРНИХ КОРПОРАТИВНИХ РЕСУРСІВ НА ОСНОВІ AMAZON INSPECTOR

Визначено мету і основні завдання щодо управління вразливостями хмарних корпоративних ресурсів. Розглянуто зміст технології управління вразливостями хмарних корпоративних ресурсів на основі Amazon Inspector.

Перехід до хмарних технологій змінив характер кіберзагроз та потреби бізнесу в захисті інформаційних ресурсів. Швидка трансформація шляхом міграції в хмару, хоча й забезпечує гнучкість та масштабованість, також призвела до появи складних проблем безпеки.

Незважаючи на повсюдний перехід до хмари, лише 42% компаній усвідомлюють очікувану цінність цих ініціатив, частково через проблеми безпеки [1]. Ці загрози змусили підприємства переглянути або відкласти свої стратегії міграції до хмари, щоб уникнути перебоїв у роботі основних додатків. Потреби в захисті змінилися до такої міри, що вимагають комплексних заходів із забезпечення безпеки хмари. Загрози безпеці хмари, такі як неправильні конфігурації, витоки даних та несанкціонований доступ, повинні вирішуватися за допомогою сучасних рішень для захисту бізнес-операцій. Зміна ландшафту загроз та вимоги захисту динамічних хмарних середовищ вимагають більш проактивного, інтегрованого підходу до кібербезпеки, який адаптується до складнощів впровадження хмарних технологій.

Хмарні обчислення – це надання розміщених послуг, включаючи програмне забезпечення, апаратне забезпечення та сховище, через Інтернет. Переваги швидкого розгортання, гнучкості, низьких початкових витрат та масштабованості зробили хмарні обчислення практично універсальними серед організацій будь-якого розміру, часто як частину гібридної/багатохмарної архітектури інфраструктури [2].

Хмарна безпека стосується технологій, політик, засобів контролю та сервісів, які захищають хмарні дані, додатки та інфраструктуру від загроз. Безпека хмарних послуг – це відповідальність, яку розділяють постачальник хмарних послуг і клієнт. У моделі спільної відповідальності існують три основні категорії відповідальності: відповідальність, яка завжди належить постачальнику, відповідальність, яка завжди належить клієнту, та відповідальність, яка залежить від моделі обслуговування: інфраструктура як послуга (IaaS), платформа як послуга (PaaS) або програмне забезпечення як послуга (SaaS), таке як хмарна електронна пошта тощо.

Обов’язки щодо безпеки, які завжди є обов’язком постачальника, пов’язані із захистом самої інфраструктури, а також доступом до фізичних хостів і фізичної мережі, на якій працюють обчислювальні екземпляри, а також знаходяться сховище та інші ресурси, а також їх встановленням та налаштуванням. Обов’язки щодо безпеки, які завжди покладаються на клієнта, включають керування користувачами та їхніми правами доступу (керування ідентифікацією та доступом), захист хмарних облікових записів від несанкціонованого доступу, шифрування та захист хмарних даних, а також управління рівнем безпеки (відповідність) [2].

Згідно з результатами дослідження Wiz Research за 2025 рік [3], 54% хмарних середовищ стикаються з вразливостями через безсерверні функції та відкриті віртуальні машини, що містять критично важливі дані. Зловмисники наполегливо шукають вразливості, оскільки їх легше використовувати. Незважаючи на те, що вони поширені, організації все ще

не вживають належних заходів для захисту від цих вразливостей, або тому, що вони не знають про ризик, або просто не знають, як його зменшити.

Необхідно відмітити, що хмарні технології забезпечують бізнес надійним та безпечним середовищем для розміщення критично важливих даних і послуг. Але без чіткої стратегії безпеки та контролю доступу до хмари, який здійснюється користувачем, вразливості можуть перетворитися на руйнівну бізнес-загрозу.

Управління вразливостями в хмарних обчисленнях – це процес виявлення, визначення пріоритетів та усунення слабких місць безпеки в хмарній інфраструктурі, системах і додатках. Проактивно усуваючи вразливості хмари, ми можемо впровадити заходи контролю, які запобігатимуть використанню зловмисниками неправильних конфігурацій та інших проблем безпеки хмари. Хоча управління вразливостями хмарних технологій пропонує багато переваг, воно також має свій власний набір проблем. Деякі поширені проблеми наведено в таблиці 1.

Таблиця 1

Проблеми управління вразливостями хмарних технологій [4]

Виклик	Опис
Масштабованість	Зі зростанням корпоративного хмарного середовища керування та моніторинг вразливостей у всіх ресурсах може стати складним завданням.
Складність	Хмарні середовища можуть бути складними, з численними взаємопов'язаними сервісами та ресурсами. Розуміння тонкощів цих середовищ є важливим для ефективного управління вразливостями.
Керування виправленнями	Підтримка хмарних ресурсів у актуальному стані з використанням останніх патчів безпеки може бути трудомістким завданням, особливо в динамічному хмарному середовищі.
Відповідність	Забезпечення відповідності галузевим стандартам і нормам може бути складним завданням, оскільки хмарні середовища часто вимагають індивідуальних конфігурацій для задоволення конкретних вимог.
Попередження про втому	Через постійний потік сповіщень та оповіщень від інструментів сканування вразливостей, команди безпеки можуть відчувати втому від сповіщень, потенційно пропускаючи критичні проблеми безпеки.

Amazon Web Services – це найповніша та найширше впроваджена хмара у світі, яка дозволяє клієнтам величезні можливості для підвищення ефективності бізнес-процесів. Організації будь-якого типу, розміру та галузі використовують хмару для широкого спектру видів діяльності, таких як резервне копіювання даних, аварійне відновлення, електронна пошта, віртуальні робочі столи, розробка та тестування програмного забезпечення, аналітика великих даних та веб-додатки, орієнтовані на клієнтів тощо.

Amazon Inspector – це автоматизована служба управління вразливостями, розроблена для забезпечення безпеки корпоративних робочих навантажень AWS. Вона автоматично виявляє такі ресурси, як екземпляри Amazon EC2, образи контейнерів в Amazon ECR та функції Lambda, а потім постійно сканує їх на наявність програмних вразливостей та ненавмисного мережевого впливу. Коли виявляється потенційна проблема, Amazon Inspector генерує детальний звіт про виявлену вразливість або ризик. Ці дані можна легко керувати через консоль Amazon Inspector або API, що надає фахівцям інструменти для ефективного та проактивного вирішення ризиків безпеки [5]. Основні функції рішення Amazon Inspector показано на рисунку 1.

Розглянемо структурований алгоритм для ефективного управління вразливостями хмарних корпоративних ресурсів. Цей процес є циклічним і вимагає постійної уваги та вдосконалення.

Етап 1: Ідентифікація та інвентаризація. Мета: зрозуміти, які активи є у хмарному середовищі та які вразливості на них можуть існувати.

Етап 2: Пріоритезація ризиків. Мета: визначити, які вразливості становлять найбільшу загрозу для бізнесу, щоб зосередити зусилля на найважливішому.

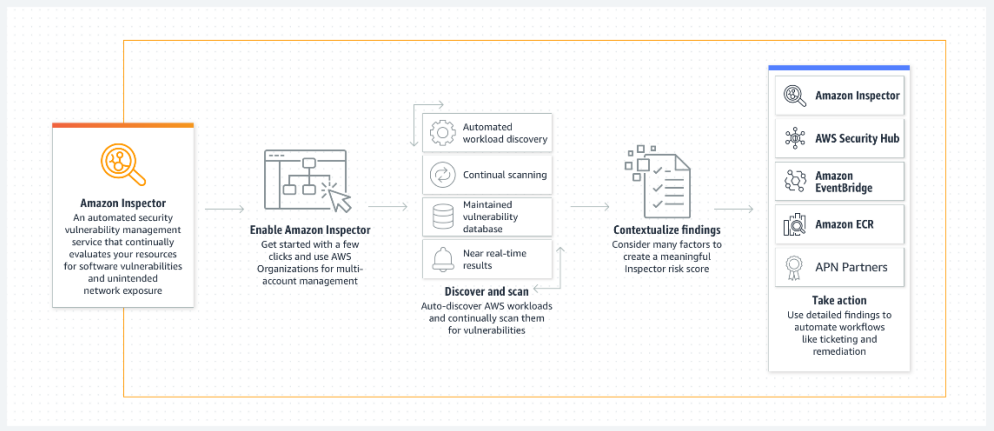

Рис. 1. Основні функції рішення Amazon Inspector [5]

Етап 3: Виправлення. Мета: ефективно усунути або мінімізувати виявлені та пріоритезовані вразливості.

Етап 4: Верифікація та звітність. Мета: переконатися, що вразливість дійсно усунута, та інформувати зацікавлені сторони про стан безпеки.

Етап 5: Постійне вдосконалення. Мета: аналізувати результати та покращувати процес управління вразливостями.

Отже, в умовах постійного зростання кіберзагроз та витоків даних, управління вразливостями хмари є життєво важливою практикою для захисту корпоративного хмарного середовища. Розуміючи поширені вразливості хмари, впроваджуючи ефективні стратегії пом'якшення наслідків та дотримуючись найкращих практик, можна значно знизити ризик інцидентів безпеки. Використання автоматизації та правильних інструментів може оптимізувати процес управління вразливостями, зробивши його керованим та економічно ефективним. Регулярне сканування вразливостей, оцінка ризиків та усунення наслідків мають вирішальне значення для підтримки цілісності та безпеки хмарних корпоративних ресурсів. Завдяки надійній програмі управління вразливостями хмарних корпоративних ресурсів ми можемо впевнено використовувати переваги хмарних технологій, зберігаючи при цьому безпеку корпоративних даних та активів.

Література

1. Most Common Cloud Security Threats. Darktrace. URL: https://www.darktrace.com/cyber-ai-glossary/the-most-common-cloud-security-threats (дата звернення: 08.10.2025)

2. Cloud Security is a Shared Responsibility. Check Point. URL: https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/ (дата звернення: 08.10.2025).

3. Top 11 Cloud Security Vulnerabilities and How to Fix Them. Wiz Experts Team, August 12, 2025. URL: https://www.wiz.io/academy/common-cloud-vulnerabilities (дата звернення: 08.10.2025).

4. Ron Reiter. Cloud Vulnerability Management Best Practices for 2025. November 26, 2024. Sentra. URL: https://www.sentra.io/learn/cloud-vulnerability-management (дата звернення: 08.10.2025).

5. Amazon Inspector: A Guide to AWS Vulnerability Management. Cloudchipr, November 26, 2024. URL: https://cloudchipr.com/blog/amazon-inspector (дата звернення: 08.10.2025).

Орлик Павло Анатолійович,
БСДМ-62
Державний університет
інформаційно-комунікаційних технологій,
м. Київ

ТЕХНОЛОГІЯ ІНТЕЛЕКТУАЛЬНОГО ВИЯВЛЕННЯ ЗАГРОЗ ХМАРНИМ КОРПОРАТИВНИМ РЕСУРСАМ НА ОСНОВІ AMAZON GUARDDUTY

Визначено мету і основні завдання щодо інтелектуального виявлення загроз хмарним корпоративним ресурсам. Розглянуто зміст технології інтелектуального виявлення загроз хмарним корпоративним ресурсам на основі Amazon GuardDuty.

Хмарні інфраструктури стали основою незліченної кількості підприємств та послуг. Очікується, що ринок хмарних обчислень досягне 2 291,59 мільярда доларів США до 2032 року. Однак, побоювання щодо безпеки хмарних технологій часто є основною перешкодою для їх впровадження. Без належного захисту хмарні корпоративні ресурси стають вразливими. Захист хмарних ресурсів та ідентифікаційних даних зараз важливіший, ніж будь-коли [1].

Загрози безпеці хмарних середовищ включають витоки даних, внутрішні загрози, викрадення облікових записів, незахищені API та атаки шкідливого програмного забезпечення. Ці загрози спрямовані на хмарні середовища, використовуючи неправильні конфігурації, слабкі засоби контролю доступу або людські помилки. Виявлення в хмарній безпеці передбачає використання передових інструментів, таких як штучний інтелект та машинне навчання, для моніторингу, ідентифікації та реагування в режимі реального часу на незвичайну поведінку або потенційні порушення безпеки.

Проблеми безпеки хмарних технологій включають:

інтеграція застарілих систем;

управління мультихмарними та гібридними середовищами;

забезпечення конфіденційності даних та дотримання нормативних вимог;

підтримка видимості та контролю над складними хмарними інфраструктурами.

Вирішення цих проблем вимагає проактивного та комплексного підходу до захисту хмарних середовищ.

Amazon GuardDuty – це служба виявлення загроз, яка постійно відстежує, аналізує та обробляє джерела даних і журнали AWS у вашому середовищі AWS. GuardDuty використовує канали інформації про загрози, такі як списки шкідливих IP-адрес і доменів, хеші файлів і моделі машинного навчання (ML), для виявлення підозрілої та потенційно шкідливої активності у корпоративному середовищі AWS. Рішення Amazon GuardDuty може допомогти виявити такі потенційні сценарії загроз [2]:

скомпрометовані та викрадені облікові дані AWS;

викрадання та знищення даних, що може призвести до події, спричиненої програмою-вимагачем. Незвичайні закономірності подій входу в підтримувані версії механізмів баз даних Amazon Aurora та Amazon RDS, що свідчать про аномальну поведінку;

несанкціонована діяльність з криптомайнінгу у корпоративних екземплярах Amazon Elastic Compute Cloud (Amazon EC2) та робочих навантаженнях контейнерів;

наявність шкідливого програмного забезпечення у корпоративних екземплярах Amazon EC2 та робочих навантаженнях контейнерів, а також нещодавно завантажені файли у корпоративних корзинах Amazon Simple Storage Service (Amazon S3);

події на рівні операційної системи, мережі та файлів, що вказують на несанкціоновану поведінку у корпоративних кластерах Amazon Elastic Kubernetes Service (Amazon EKS), завданнях Amazon Elastic Container Service (Amazon ECS) – AWS Fargate, а також екземплярах Amazon EC2 та робочих навантаженнях контейнерів.

Місце рішення Amazon GuardDuty в загальній архітектурі AWS показано на рисунку 1.

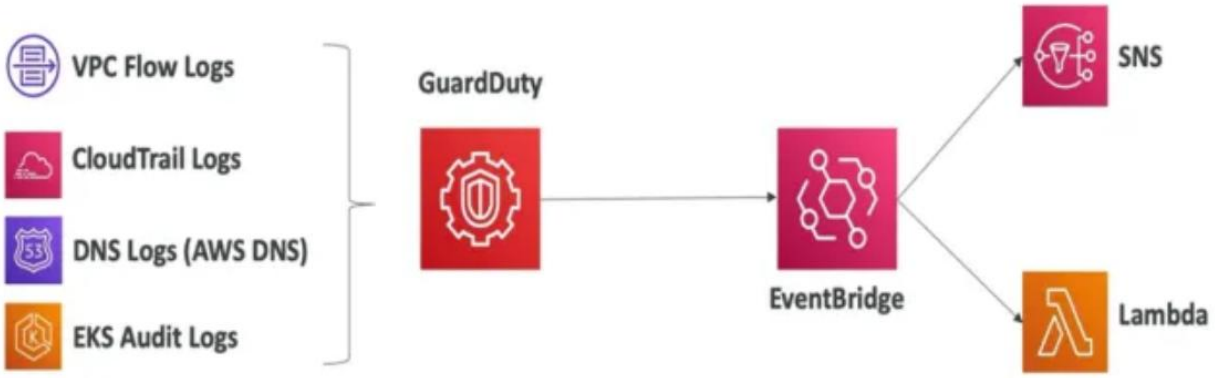

Рис. 1. Місце рішення Amazon GuardDuty в загальній архітектурі AWS [3]

Вхідні дані Amazon GuardDuty включають [3]:

журнали подій CloudTrail – незвичайні виклики API, несанкціоновані розгортання;

журнали подій керування CloudTrail – створення VPC, підмережі, створення сліду;

події даних Cloud Trail S3 – отримання об'єкта, перелік об'єктів, видалення об'єктів;

журнали потоку VPC – незвичайний внутрішній трафік, незвичайна IP-адреса;

журнали DNS – скомпрометовані екземпляри EC2, що надсилають закодовані дані за допомогою DNS;

журнали аудиту Kubernetes – підозріла активність та компрометація кластера EKS.

Розглянемо зміст технології інтелектуального виявлення загроз хмарним корпоративним ресурсам на основі Amazon GuardDuty на прикладі виявлення аномалій у поведінці користувачів та ресурсів. Процес можна розділити на три ключові етапи:

Етап 1. Збір та аналіз даних. Amazon GuardDuty не втручається у роботу корпоративних ресурсів і не впливає на їхню продуктивність. Замість цього він "тихо" аналізує величезні потоки даних з трьох основних джерел:

журнали AWS CloudTrail: фіксується кожен виклик API: хто, що, коли і звідки зробив. Це основне джерело для аналізу поведінки користувачів та ролей;

журнали VPC Flow Logs: це інформація про весь мережевий трафік, що входить і виходить з корпоративних віртуальних мереж (VPC). GuardDuty аналізує, хто з ким спілкується, які порти та протоколи використовуються. Це ключові дані для аналізу поведінки ресурсів, таких як EC2-інстанси;

DNS-логи: це записи про те, до яких доменних імен звертаються корпоративні ресурси. Аналіз цих журналів допомагає виявити комунікацію зі шкідливими серверами (наприклад, командними центрами ботнетів).

Етап 2. Створення базової лінії поведінки. Після активації GuardDuty починає процес навчання, формуючи модель нормальної, очікуваної активності для корпоративного середовища. Ця базова лінія є унікальною для кожного акаунту і включає в себе патерни поведінки як для користувачів, так і для ресурсів.

Щодо поведінки користувачів (IAM Users/Roles) моделі машинного навчання аналізують такі аспекти:

типові API-виклики: які сервіси та дії зазвичай виконує певний користувач чи роль? (Наприклад, розробник часто працює з Lambda та API Gateway, а роль для EC2 – з S3);

геолокація та IP-адреси: з яких країн, міст чи мереж зазвичай надходять запити;

час активності: в які дні тижня та години користувач зазвичай активний;

використовувані інструменти: чи використовує користувач AWS CLI, консоль, чи певний SDK?

Щодо поведінки ресурсів (EC2, контейнери тощо) моделі машинного навчання аналізують такі аспекти:

мережеві з'єднання: з якими IP-адресами та по яких портах зазвичай комунікує EC2-інстанс? Чи є стабільні патерни трафіку?

обсяг трафіку: скільки даних зазвичай відправляється чи отримується?

DNS-запити: до яких доменів ресурс звертається для оновлень, отримання даних тощо?

Етап 3. Виявлення аномалій та відхилень. Це найважливіший етап, де GuardDuty порівнює поточну активність із вивченою базовою лінією. Якщо фіксується значне відхилення, сервіс генерує знахідку (finding).

Ось конкретні приклади аномалій, які Amazon GuardDuty може виявити:

Приклади аномалій у поведінці користувачів:

незвичні API-виклики – IAM-користувач, який зазвичай працює лише з базами даних (RDS), раптом починає робити виклики для вимкнення логування в CloudTrail (StopLogging) або створення знімків баз даних. Це класична ознака скомпрометованого акаунту;

вхід з нетипової локації: адміністратор, який завжди підключається з України, раптом робить запит з IP-адреси, що належить до іншої країни, та ще й у неробочий час;

«неможлива подорож» (Impossible Travel): API-ключ був використаний спочатку в Києві, а через 5 хвилин – у Сінгапурі. Фізично це неможливо, що свідчить про викрадення облікових даних;

спроби приховати сліди: користувач намагається видалити логи або вимкнути механізми безпеки.

Приклади аномалій у поведінці ресурсів:

незвичний мережевий трафік: веб сервер, який зазвичай спілкується лише з користувачами по портах 80/443, раптом починає відправляти великі обсяги даних на невідому IP-адресу по нестандартному порту. Це може свідчити про витік даних;

комунікація з відомими шкідливими IP: EC2-інстанс встановлює з'єднання з IP-адресою, яка відома як командний центр (C&C) для майнінгу криптовалют;

сканування портів: один з корпоративних EC2-інстансів починає масово сканувати порти інших ресурсів у корпоративній VPC. Це може означати, що інстанс скомпрометовано і зловмисник проводить розвідку всередині мережі.

Таким чином, машинне навчання в GuardDuty – це не просто набір статичних правил, а динамічна система, що постійно адаптується. Вона вчиться, що є нормальним саме для конкретних ресурсів, і завдяки цьому може ефективно виявляти складні та раніше невідомі загрози, які неможливо знайти за допомогою традиційного сигнатурного аналізу.

Література

1. Niels Kroeze. 14 Cloud Security Risks, Threats and Challenges in 2025. URL: https://intercept.cloud/en-gb/blogs/14-cloud-security-risks-threats-challenges-2025 (дата звернення: 09.10.2025).

2. Amazon GuardDuty User Guide. URL: https://docs.aws.amazon.com/guardduty/latest/ug/what-is-guardduty.html (дата звернення: 09.10.2025).

3. Ranjinnijoshe. AWS GuardDuty Architecture. Medium, Sep 12, 2023. URL: https://medium.com/@ranjinnijoshe/%EF%B8%8Faws-guardduty-architecture-e01067d83fb2 (дата звернення: 09.10.2025).

Богданович Олексій Дмитрович,
БСДМ-63
Державний університет
інформаційно-комунікаційних технологій,
м. Київ

ТЕХНОЛОГІЯ ВИЯВЛЕННЯ ВТОРГНЕНЬ ДО ХМАРНИХ КОРПОРАТИВНИХ РЕСУРСІВ НА БАЗІ AMAZON DETECTIVE

Визначено мету і основні завдання щодо виявлення вторгнень до хмарних корпоративних ресурсів. Розглянуто зміст технології виявлення вторгнень до хмарних корпоративних ресурсів на базі Amazon Detective.

Згідно з опитуванням CrowdStrike кількість вторгнень у хмару зросла на 136 відс. у першій половині 2025 року. Найпримітніше, що 81 відс. цих вторгнень не були пов'язані з використанням шкідливого програмного забезпечення. Замість розгортання шкідливого програмного забезпечення, зловмисники все частіше покладаються на викрадені облікові дані для отримання доступу та роботи в легітимних системах. Цей зсув означає, що багато традиційних методів виявлення, створених для позначення шкідливого коду, повністю ігноруються [1].

Оскільки більшість вторгнень зараз повністю уникають шкідливого програмного забезпечення, акцент у безпеці має зміститися. Коли зловмисники діють з дійсними обліковими даними, ключовою точкою контролю стає ідентифікація, а не периметр мережі. Сьогодні існує очевидна потреба в безпеці, орієнтованій на дані, яка захищає самі дані та виявляє зловживання, а не покладається виключно на запобігання проникненню [1].

Оскільки інфраструктура додатків та робоче середовище стають складнішими в хмарі, командам безпеки може бути складно виявляти потенційні проблеми та всебічно досліджувати їхню діяльність. Amazon Detective розроблений для того, щоб допомогти пом'якшити ці проблеми за допомогою аналітики та візуалізації на основі машинного навчання [2].

Amazon Detective допомагає вирішувати кілька поширених проблем хмарної безпеки завдяки єдиному огляду активності та підтримці швидкого відстеження з'єднань для виявлення першопричин [2]:

виявлення криптомайнінгу – виявлення незвичайного вихідного трафіку та використання API, що свідчить про встановлення відповідного програмного забезпечення;

захист від DDoS-атак – виявлення джерел перевантаження трафіком та посилань на скомпрометовані ресурси;

відстеження зараження шкідливим програмним забезпеченням – поверхневі ознаки витоку даних та їхнього переміщення тощо.

Amazon Detective – служба безпеки, яка допомагає аналітикам розслідувати потенційні проблеми безпеки. Вона робить це, збираючи дані журналів з AWS CloudTrail, журналів потоків Amazon Virtual Private Cloud (VPC) та інших служб. Amazon Detective використовує машинне навчання, статистичний аналіз та теорію графів для створення пов'язаного набору даних, який називається графіком поведінки безпеки, який можна використовувати для проведення швидших та ефективніших розслідувань безпеки [3].

Основні функції Amazon Detective показано на рисунку 1.

На основі подій безпеки Amazon Detective використовує машинне навчання та візуалізацію для створення єдиного, інтерактивного представлення поведінки корпоративних ресурсів та взаємодії між ними з часом. Ми можемо дослідити цей графік поведінки, щоб проаналізувати різні дії, такі як невдалі спроби входу або підозрілі виклики API. Також можна побачити, як ці дії впливають на такі ресурси, як облікові записи AWS та екземпляри Amazon

EC2. Ми можемо налаштувати область дії та часову шкалу графіка поведінки для різних завдань [4]:

швидке розслідування будь-якої діяльності, яка виходить за рамки норми;
визначення закономірностей, які можуть свідчити про проблему безпеки;
усвідомлення всіх ресурсів, на які впливає знайдений процес.

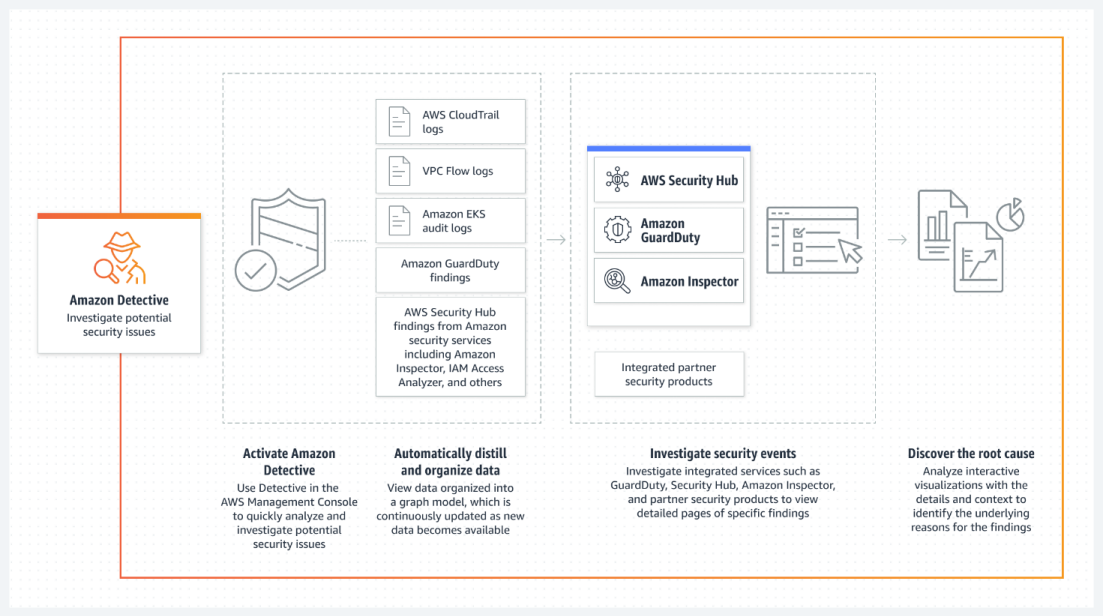

Рис. 1. Основні функції Amazon Detective [2]

Візуалізації, адаптовані для аналітиків, забезпечують базову точку зору та узагальнюють інформацію про обліковий запис. Ці результати можуть допомогти відповісти на такі питання, як «Чи є це незвичайним викликом API для цієї ролі?» або «Чи очікуваним є цей сплеск трафіку з цього екземпляра?»

Розслідування в Amazon Detective може розпочатися з окремого виявлення, групи виявлених порушень або об’єкта. Розглянемо етапи розслідування в Amazon Detective.

Етап 1. Сортування. Процес розслідування починається, коли ми отримуємо повідомлення про підозрюваний випадок шкідливої або високоризикової діяльності. Наприклад, нам доручають розглянути результати або сповіщення, виявлені такими сервісами, як Amazon GuardDuty та Amazon Inspector.

На етапі сортування ми визначаємо, чи вважаємо, що активність є справді позитивною (справжня зловмисна активність) чи хибнопозитивною (не зловмисна або високоризикова активність). Профілі Amazon Detective підтримують процес сортування, надаючи уявлення про активність залученої особи. Для справді позитивних випадків ми переходимо до наступного етапу.

Етап 2. Визначення обсягу. Під час етапу визначення обсягу діяльності аналітики визначають масштаби зловмисної або високоризикової діяльності та її основну причину. Огляд відповідає на такі типи питань: Які системи та користувачі були скомпрометовані? Звідки виникла атака? Як довго триває напад? Чи є інша пов’язана діяльність, яку потрібно виявити? Наприклад, якщо зловмисник витягує дані з вашої системи, як він їх отримав?

Візуалізації Amazon Detective можуть допомогти нам ідентифікувати інші сутності, які були залучені або постраждали.

Етап 3. Відповідь. Останній крок – реагування на атаку, щоб зупинити її, мінімізувати збитки та запобігти повторенню подібної атаки в майбутньому.

Схема процесу розслідування в Amazon Detective на загальному рівні показано на рисунку 2.

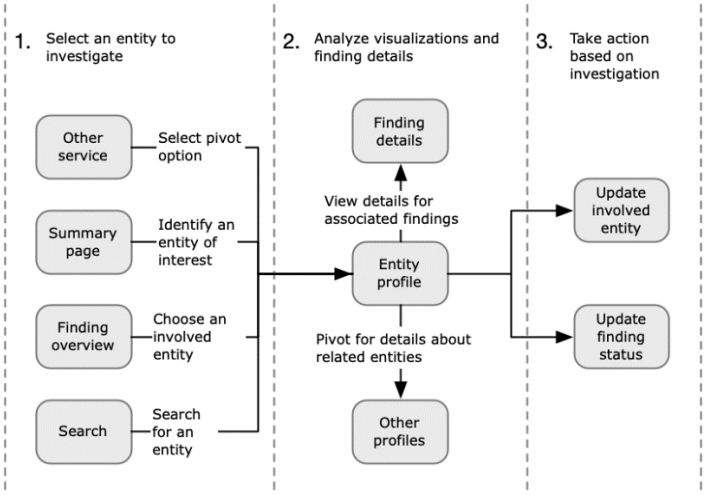

Рис. 2. Схема процесу розслідування в Amazon Detective на загальному рівні [4]

Рішення Amazon Detective пропонує інноваційний підхід до аналітики безпеки хмарних технологій та розслідування загроз завдяки своїй інтерактивній моделі графових даних. Автоматично агрегуючи та корелюючи дані журналів з таких сервісів, як CloudTrail, VPC Flow Logs та GuardDuty, Amazon Detective забезпечує єдине уявлення про активність облікових записів та ресурсів. Візуальний графік відображає взаємозв'язки між користувачами, активами, дозволами та змінами, щоб виявити тенденції, аномалії та зв'язки, які важко виявити за допомогою традиційного ведення журналу.

Вбудовані алгоритми машинного навчання допомагають виявляти підозрілі закономірності, водночас дозволяючи фільтрувати, перетворювати та динамічно досліджувати пов'язані події з високою швидкістю. Налаштована аналітика через блокноти Jupyter розширює можливості для вирішення нових загроз, адаптованих до кожної організації. Автоматизовані дії та інтеграції ще більше оптимізують робочі процеси реагування на інциденти, що запускаються на основі аналізу графів.

Хоча продумані політики джерел даних та їх збереження необхідні для управління складністю графів з часом, Amazon Detective змінює зміст пошуку загроз у хмарі. Його можливості безперервного аналізу на основі графів дозволяють командам безпеки проактивно досліджувати ризики та швидко відстежувати вплив подій, що розгортаються, в різних облікових записах, без необхідності вручну збирати та корелювати розподілені дані журналів. Це допомагає організаціям підвищити ефективність, результативність та гнучкість реагування на інциденти у сфері хмарної безпеки.

Література

1. John Lynch. Cloud intrusions have skyrocketed. CISOs should wise up. Tech Monitor, September 2, 2025. URL: https://www.techmonitor.ai/comment-2/cloud-intrusions-strategies?cf-view (дата звернення: 10.10.2025).

2. Christopher Adamson. AWS Detective for Security Analysis and Investigation. Medium, Dec 27, 2023. URL: https://medium.com/@christopheradamson253/aws-detective-for-security-analysis-and-investigation-0540dd82f15a (дата звернення: 10.10.2025).

3. Rich Vorwaller and Nicholas Doropoulos. Improve your security investigations with Detective finding groups visualizations. AWS Security Blog, 29 AUG 2023. URL: https://aws.amazon.com/blogs/security/improve-your-security-investigations-with-detective-finding-groups-visualizations/ (дата звернення: 10.10.2025).

4. Amazon Detective. User Guide. URL: https://docs.aws.amazon.com/detective/latest/userguide/what-is-detective.html (дата звернення: 10.10.2025).

Герман В.Д
студентка групи КІ-41, ННІАКОТ, НУВГП
Рівне, Україна

Рейнська В.Б.,
к.е.н., доц.кафедри обчислювальної техніки НУВГП
Рівне, Україна

БЕЗПЕКА ХМАРНИХ ТЕХНОЛОГІЙ В УКРАЇНСЬКОМУ ІНФОРМАЦІЙНОМУ БІЗНЕСІ: ДОСВІД SENDPULSE

Сучасний етап розвитку інформаційного бізнесу в Україні безпосередньо пов'язаний із поширенням хмарних технологій. Цифрова трансформація, яка відбувається в усьому світі, спричинила зміни у структурі національної економіки та відкрила нові можливості для українських компаній, що працюють у сфері SaaS-рішень. Використання хмарних сервісів стало необхідною умовою масштабованості бізнесу, його гнучкості та конкурентоспроможності на глобальному ринку. Проте одночасно із перевагами виникли й нові ризики: кібератаки на хмарні сервіси, витоки персональних даних, проблеми регуляторного характеру, які стосуються захисту інформації та збереження довіри клієнтів.[1]

Важливим прикладом інформаційного бізнесу в Україні є компанія **SendPulse** — одна з провідних SaaS-платформ, яка спеціалізується на сервісах email-маркетингу, SMS-розсилок, web push-повідомлень, чат-ботів і CRM-рішень. Саме ця компанія демонструє як потенціал, так і ризики, що виникають під час переходу до хмарної архітектури. Досвід SendPulse дозволяє оцінити, наскільки українські бізнес-структури готові до впровадження сучасних технічних систем захисту та до формування нової культури безпеки.

Постановка проблеми

Основним викликом для хмарних технологій є те, що вони інтегрують обробку та зберігання даних у середовищі, яке не завжди контролюється кінцевим користувачем. Якщо традиційні корпоративні системи безпеки можна було будувати навколо власних дата-центрів, то хмарні рішення передбачають постійний доступ до сервісів через мережу Інтернет, що значно збільшує площу потенційних атак. Для таких компаній, як SendPulse, які оперують мільйонами акаунтів, критично важливо зберегти довіру користувачів, адже будь-який витік інформації матиме катастрофічні наслідки для репутації та конкурентних позицій на ринку.

Серед проблем, із якими стикається інформаційний бізнес, особливе місце посідає несанкціонований доступ до хмарних акаунтів, уразливості в API-інтерфейсах, неправильні налаштування прав доступу, а також людський фактор, що проявляється у використанні слабких паролів або у фішингових атаках. Крім цього, компанії змушені враховувати вимоги різних регуляторів — українського законодавства, а також норм ЄС і США щодо захисту персональних даних (GDPR, CCPA). Для SendPulse, як компанії з міжнародною клієнтською базою,

це означає постійну адаптацію політик безпеки та оновлення внутрішніх процедур.[2]

Виклад основного матеріалу

Хмарні технології відкривають для українських SaaS-компаній значні переваги, проте вони стають і ареною постійного протиборства із зловмисниками. Досвід SendPulse свідчить, що ефективний захист у хмарному середовищі вимагає комплексного підходу, який включає як технічні рішення, так і організаційні механізми. Зокрема, компанія активно використовує багаторівневу систему автентифікації, що передбачає застосування мультифакторних методів доступу, поєднання паролів, біометричних даних та одноразових кодів. Це дозволяє зменшити ймовірність компрометації акаунтів навіть у випадку успішної фішингової атаки.

Важливим напрямом є впровадження принципів **Zero Trust Architecture**, коли кожен запит у системі підлягає перевірці незалежно від місця його походження. Такий підхід забезпечує захист не лише від зовнішніх атак, але й від внутрішніх загроз, що є особливо актуальним для багатокористувацьких SaaS-сервісів. Використання Zero Trust у поєднанні з інструментами сегментації мережі та ізоляції клієнтських даних зменшує ризик між-орендних витоків, які часто виникають у хмарних середовищах.[3]

SendPulse застосовує методи криптографічного захисту, зокрема шифрування даних як під час зберігання, так і під час передавання. Це відповідає міжнародним стандартам і забезпечує конфіденційність даних користувачів. Крім того, компанія інтегрувала у свою інфраструктуру системи моніторингу безпеки, які дозволяють у реальному часі виявляти підозрілі активності та аномалії. Використання технологій машинного навчання в системах виявлення загроз створює можливості для проактивного виявлення атак ще до того, як вони матимуть руйнівний ефект.

Окремої уваги заслуговує людський фактор. У SendPulse розроблені внутрішні програми з підвищення кібергігієни персоналу. Працівники проходять регулярні тренінги з виявлення фішингових листів, правильного поводження з обліковими записами та реагування на потенційні інциденти. Це дає змогу мінімізувати ризики, які виникають через необережність співробітників.

Попри наявність розвинених механізмів, компанія стикається із серйозними викликами. Одним із них є залежність від сторонніх хмарних провайдерів, яка означає, що будь-які збої або атаки на інфраструктуру постачальника можуть паралізувати роботу сервісу. Іншим викликом є швидке зростання клієнтської бази: збільшення навантаження вимагає не лише масштабування ресурсів, але й удосконалення систем контролю доступу, що підвищує складність управління безпекою.[4]

Ситуація ускладнюється й тим, що Україна перебуває в умовах гібридної війни, де кібератаки є одним із інструментів агресії. Тому такі компанії, як SendPulse,

стають потенційними цілями не лише для кримінальних груп, але й для державних акторів, які прагнуть порушити роботу критичних цифрових сервісів. Це вимагає створення планів безперервності бізнесу та стратегій швидкого відновлення після інцидентів, що є важливим аспектом кіберстійкості.[5]

Висновки

Аналіз діяльності SendPulse свідчить, що безпека хмарних технологій є одним із ключових викликів для українського інформаційного бізнесу. Ефективна стратегія захисту повинна враховувати комплексність загроз, які охоплюють технічний, організаційний і людський рівні. В умовах швидкої цифрової трансформації успішність інформаційних компаній залежить від здатності не лише реагувати на атаки, але й передбачати їх.

Українські SaaS-платформи повинні посилювати співпрацю з державними та міжнародними структурами у сфері кібербезпеки, впроваджувати найкращі світові практики та дбати про дотримання етичних норм і прав користувачів. Лише поєднання технічних інновацій, нормативного регулювання і формування культури безпеки здатне забезпечити стійкість інформаційного бізнесу та створити умови для його подальшого розвитку у глобальному цифровому середовищі.

Список використаних джерел

1. Колб С. О., Пирога М. І. Інформаційна безпека: нові виклики та стратегії захисту. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2025. Вип. 90, ч. 5. С. 437–441. DOI: 10.24144/2307-3322.2025.90.5.58.
2. Cyber Resilience 2025: підсумки національного дослідження. European Business Association. 2025. URL: https://eba.com.ua/cyber-resilience-2025 (дата звернення: 28.09.2025).
3. Cyber incidents remain top business risk concern globally 2025. 10Guards. 2025. URL: https://10guards.com/ua/blog/2025/02/13/cyber-incidents-remain-top-business-risk-concern-globally-2025 (дата звернення: 28.09.2025).
4. SendPulse: розвиток платформи SaaS. SendPulse. 2025. URL: https://sendpulse.ua/blog/development-of-sendpulse-platform (дата звернення: 28.09.2025).
5. SGS4Business. ТОП-7 кіберзагроз для бізнесу у 2025 році. 2025. URL: https://sgs4business.com/news/top-7-kiberzagroz-dla-biznesu-v-2025-roci.html (дата звернення: 28.09.2025).

Твердохліб Я.М.
студентка групи БСД-43, ННІКБЗІ ДУІКТ,

Київ, Україна

ВПРОВАДЖЕННЯ МОДЕЛІ НУЛЬОВОЇ ДОВІРИ (ZERO TRUST) ДЛЯ ЗАБЕЗПЕЧЕННЯ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Впровадження моделі нульової довіри (Zero Trust) є ключовим етапом розвитку корпоративної кібербезпеки, спрямованим на мінімізацію ризиків несанкціонованого доступу, витоку даних та внутрішніх загроз. Концепція Zero Trust базується на принципі «ніколи не довіряй, завжди перевіряй» і передбачає безперервну автентифікацію користувачів, перевірку пристроїв, а також контроль кожного запиту до ресурсів. Такий підхід забезпечує високий рівень адаптивності системи безпеки, ефективне управління ризиками та відповідність сучасним викликам цифрової трансформації. Модель Zero Trust формує основу «розумної» кібербезпеки майбутнього.

Ключові слова: Zero Trust, кібербезпека, корпоративна безпека

Традиційна модель кібербезпеки, побудована на концепції периметрової безпеки, поступово втрачає свою ефективність. На протязі десятиліть організації покладались на укріплену периметрову оборону – брандмауери, системи виявлення вторгнень та інші засоби, які мали утримувати зловмисників за межами мережі. Однак реалії сучасного кіберпростору докорінно змінилися. Поширення хмарних технологій, віддаленої роботи, BYOD та збільшення кількості кіберзагроз зробило такий підхід недостатнім. Концепція Zero Trust (нульова довіра) виникла як революційна відповідь на ці виклики.

Модель Zero Trust ґрунтується на ключовому принципі – ніколи не довіряй, завжди перевіряй. Це означає, що жоден користувач, пристрій або запит не вважається безпечним за замовчуванням, навіть якщо він походить з внутрішньої мережі. Доступ до ресурсів надається лише після багаторівневої перевірки автентичності, авторизації та відповідності політикам безпеки. Як зазначено в документі NIST SP 800-207, Zero Trust зміщує фокус із захисту мережевого периметра на захист конкретних ресурсів, зменшуючи невизначеність при прийнятті рішень про доступ [1, с.4].

Zero Trust будується на семи основних принципах, які разом формують цілісну концепцію безпеки. Ключовий принцип полягає в тому, що жоден користувач, пристрій, мережа чи сервіс не повинні отримувати автоматичного доступу лише тому, що вони знаходяться «всередині» мережі або належать організації. Замість одноразової автентифікації при вході в систему, Zero Trust вимагає безперервної верифікації. Користувач повинен постійно підтверджувати свою особу та право доступу до конкретного ресурсу через аналіз поведінки, контекстуальні фактори та динамічні дані. Окрему роль відіграє мікросегментація, яка розділяє мережеве середовище на ізольовані сегменти, обмежуючи поширення загроз у разі їх виникнення. Кожному користувачу та пристрою надається лише мінімально необхідний набір прав доступу для виконання їхніх функцій – принцип найменших привілеїв (Principle of Least Privilege). Це не лише обмежує потенційну шкоду від компрометованого облікового запису, але й значно розширює видимість несанкціонованої діяльності.

Сучасні корпоративні IT-інфраструктури дедалі частіше є гібридними – поєднують локальні сервери з хмарними сервісами. Це ускладнює контроль і моніторинг, а отже, потребує централізованого управління безпекою. Впровадження Zero Trust дає змогу об'єднати всі рівні корпоративної інфраструктури – від робочих станцій і мобільних пристроїв до хмарних платформ – під єдиною політикою перевірки доступу.

Водночас ефективна реалізація Zero Trust у корпоративних системах потребує не лише технологічних рішень, а й трансформації корпоративної культури безпеки. Необхідно навчати персонал, стандартизувати процеси доступу, формалізувати політики безпеки та впроваджувати автоматизовані засоби контролю. Як показує звіт Microsoft Security (2024), організації, які перейшли до Zero Trust, скоротили кількість інцидентів із несанкціонованим доступом на понад 50% та зменшили час реагування на кіберінциденти удвічі.[2]

Крім того, впровадження моделі Zero Trust сприяє підвищенню загальної стійкості організації до кіберзагроз завдяки інтеграціям з сучасними технологіями моніторингу та аналітики. Використання засобів штучного інтелекту (AI) та машинного навчання (ML) дає змогу виявляти аномалії у поведінці користувачів і пристроїв у реальному часі, автоматично реагувати на потенційні інциденти безпеки та блокувати підозрілі дії ще до завдання шкоди. Штучний інтелект суттєво підсилює архітектуру Zero Trust, дозволяючи автоматично реагувати на загрози: наприклад, ізолювати скомпрометовані пристрої, призупиняти права доступу та запускати процедури реагування без людського втручання.[3] Такі підходи забезпечують проактивний захист, зменшують навантаження на IT-персонал і підвищують ефективність управління ризиками. Таким чином Zero Trust стає основою побудови «розумної» кібербезпеки майбутнього, орієнтованої на безперервний контроль, автоматизацію та довіру, що базується на доказах, а не припущеннях.

Отже, Zero Trust є не просто технічним рішенням, а стратегічною моделлю управління кібербезпекою корпоративних інформаційних систем. Вона створює багаторівневий, адаптивний і динамічний контур захисту, який відповідає сучасним вимогам цифрової економіки та дозволяє організаціям забезпечити стабільність і довіру у взаємодії з клієнтами, партнерами та користувачами.

1. NIST Special Publication 800-207. *Zero Trust Architecture*. National Institute of Standards and Technology, 2020.
2. Microsoft Security. *Zero Trust Maturity Model*. Microsoft Corporation, 2024. URL: https://aka.ms/zerotrust
3. How is AI Strengthening Zero Trust? | CSA. Home | CSA. URL: https://cloudsecurityalliance.org/blog/2025/02/27/how-is-ai-strengthening-zero-trust

Гончаренко Матвій Федорович
Студент групи БСДМ-52, ННІКБЗІ ДУІКТ, Київ, Україна

SHADOW SaaS ЯК ВИКЛИК КОРПОРАТИВНІЙ КІБЕРБЕЗПЕЦІ

Shadow SaaS – це хмарні сервіси, які співробітники використовують без узгодження з IT-відділом, що створює численні загрози для корпоративної безпеки. Дослідження показують, що у середній організації використовується втричі більше SaaS-додатків, ніж відомо відділу інформаційної безпеки. Dropbox, ChatGPT, Notion та інші популярні інструменти підвищують продуктивність, але одночасно створюють канали витоку конфіденційних даних, обходять політики безпеки та ускладнюють контроль за інформаційними активами. Вирішення проблеми потребує балансу між безпекою та зручністю роботи через впровадження CASB-рішень, Zero Trust архітектури та політик прозорого управління доступом.

Ключові слова: Shadow IT, Shadow SaaS, витік даних, CASB, корпоративна кібербезпека.

Цифрова трансформація бізнесу супроводжується масовим впровадженням хмарних сервісів, проте значна частина цих інструментів залишається поза контролем служб інформаційної безпеки. Shadow SaaS – це хмарні застосунки, які співробітники самостійно обирають для вирішення робочих завдань, не повідомляючи IT-департамент. Це створює "сліпі зони" у периметрі захисту та відкриває шлях для витоку критичної інформації.

Основні ризики Shadow SaaS пов'язані з втратою контролю над корпоративними даними. Коли співробітник завантажує конфіденційний документ у власний Dropbox або вставляє фрагменти коду у ChatGPT для допомоги у розробці, ці дані виходять за межі захищеного периметру. За даними Palo Alto Networks, конфіденційна інформація зберігається у 66% хмарних сховищ та у 63% публічно доступних сховищ [1]. Більше того, такі платформи часто не відповідають вимогам GDPR, ISO 27001 чи галузевим стандартам, що створює юридичні ризики для організації.

Технічні виклики включають відсутність централізованої автентифікації, неможливість застосування корпоративних політик безпеки та обмежену можливість відстежувати мережевий трафік. Співробітники використовують особисті облікові записи для доступу до цих сервісів, що унеможливлює застосування Single Sign-On (SSO) та багатофакторної автентифікації (MFA). За даними Obsidian Security, понад 80% застосунків не інтегровані з корпоративними системами ідентифікації, що робить їх особливо вразливими до атак на основі компрометації облікових даних [2]. У разі компрометації такого акаунту зловмисники отримують доступ не лише до особистих даних, але й до корпоративної інформації.

Для вирішення проблеми організації впроваджують Cloud Access Security Brokers (CASB) – посередників між користувачами та хмарними сервісами. CASB-рішення забезпечують виявлення несанкціонованих застосунків, моніторинг передачі даних, застосування DLP-політик (Data Loss Prevention) та

контроль доступу на основі контексту. Ринок CASB демонструє стрімке зростання: за прогнозами, його обсяг зросте з $9,48 млрд у 2024 році до $51,11 млрд у 2034 році, що відображає критичну потребу організацій у таких рішеннях [3].

Альтернативним підходом є впровадження Zero Trust Network Access (ZTNA), що базується на принципі "ніколи не довіряй, завжди перевіряй". Замість блокування всіх несанкціонованих сервісів організації створюють "білий список" дозволених застосунків з необхідними налаштуваннями безпеки. Це дозволяє легітимізувати популярні інструменти з контрольованими правами доступу та шифруванням [3].

Важливою складовою протидії Shadow SaaS є організаційні заходи. Прозора політика використання хмарних сервісів, швидке схвалення запитів на нові інструменти та навчання співробітників кібер-грамотності знижують бажання працювати "в тіні". За даними JumpCloud, 69% технічних керівників вважають Shadow IT головною проблемою безпеки, а 59% борються з неконтрольованим зростанням SaaS-застосунків [4]. Спрощення процедур узгодження та створення каталогу рекомендованих альтернатив підвищує рівень комплаєнсу без шкоди продуктивності.

Фінансові наслідки некерованого Shadow SaaS включають не лише прямі збитки від витоку даних, але й штрафи за порушення регуляторних вимог, дублювання підписок та витрати на розслідування інцидентів. За оцінками, 30-40% витрат великих компаній на IT припадає на Shadow IT, а середня вартість кібератак, пов'язаних із Shadow IT, перевищує $4,2 млн [4].

Shadow SaaS є неминучим наслідком демократизації IT та зростання потреб у гнучких інструментах для роботи. Ефективна стратегія кібербезпеки має балансувати між контролем та інноваційністю, використовуючи технічні рішення (CASB, ZTNA, DLP) та організаційні підходи для мінімізації ризиків без блокування продуктивності команд.

Перелік посилань:

1. Palo Alto Networks. Cloud Security Statistics 2024. Published 2024 [Електронний ресурс] – Режим доступу: https://www.stationx.net/cloud-security-statistics/

2. Obsidian Security. What Is Shadow SaaS? Published 2024 [Електронний ресурс] – Режим доступу: https://www.obsidiansecurity.com/blog/what-is-shadow-saas

3. Precedence Research. Cloud Access Security Broker Market Size to Hit USD 51.11 Billion by 2034. Published April 2025 [Електронний ресурс] – Режим доступу: https://www.precedenceresearch.com/cloud-access-security-broker-market

4. JumpCloud. What Is Shadow IT? 2024 Statistics & Solutions. Published October 2024 [Електронний ресурс] – Режим доступу: https://jumpcloud.com/blog/shadow-it

Таран В. Д.
студент групи БСДМ-52, ННІКБЗІ ДУІКТ
Київ, Україна

ПОТОЧНИЙ СТАН СТАНДАРТІВ ТА ПРАВИЛ БЕЗПЕКИ ІНТЕРНЕТУ РЕЧЕЙ (IoT)

У сучасному світі Інтернет речей (IoT) став одним із ключових напрямів цифрової трансформації, однак його швидкий розвиток супроводжується зростанням кіберризиків. Уряди та міжнародні організації активно формують нормативно-правові акти та стандарти, покликані підвищити рівень безпеки підключених пристроїв. У тезі розглянуто поточний стан стандартизації безпеки IoT, основні міжнародні ініціативи, проблеми фрагментації нормативної бази та перспективи створення єдиної системи вимог для підвищення надійності екосистеми IoT.

Інтернет речей (IoT) активно інтегрується у всі сфери людської діяльності — від промисловості до побуту. Проте масштабне використання «розумних» пристроїв створює нові виклики у сфері кібербезпеки. За статистикою, у світі щомісяця здійснюється понад 5200 атак на пристрої IoT, а щодня компрометується близько 7 мільйонів записів даних. Така динаміка підкреслює необхідність запровадження чітких стандартів і правил безпеки.

З 2019 року спостерігається активне зростання кількості нормативних актів, спрямованих на регулювання безпеки IoT. Країни світу поступово впроваджують закони, які зобов’язують виробників дотримуватися базових принципів кіберзахисту. Наприклад, у штаті Каліфорнія (США) діє закон, що вимагає наявності унікальних паролів для кожного пристрою, а у 2020 році в Європейському Союзі набув чинності стандарт ETSI EN 303 645, який визначає 13 ключових вимог до безпеки споживчих IoT-продуктів, серед яких — заборона універсальних паролів, контроль оновлень та прозорість політик безпеки.

У Великій Британії уряд запровадив «Кодекс практики Secure by Design», який встановлює вимоги щодо розробки безпечних пристроїв з урахуванням принципів безпеки за задумом. Такий підхід дозволяє створювати продукти, у яких захист інтегровано з самого початку життєвого циклу. Аналогічні ініціативи поступово впроваджуються і в інших країнах, що свідчить про формування глобальної тенденції до посилення регуляторного контролю у сфері IoT.

Попри позитивні зрушення, існує серйозна проблема фрагментації нормативно-правової бази. Різні держави мають власні вимоги до безпеки, що ускладнює для виробників процес сертифікації пристроїв і призводить до плутанини в галузі. За даними звіту PSA Security Report 2021, 48% опитаних компаній вважають саме розрізненість стандартів найбільшою проблемою у сфері безпеки IoT.

Для подолання цієї проблеми необхідно створити спільну глобальну основу — «базовий рівень безпеки» (baseline security), що забезпечить

уніфікацію вимог і спільну мову для всіх учасників ринку. Такий підхід сприятиме реалізації концепції «безпека за дизайном» (Security by Design), у межах якої механізми захисту закладаються у пристрій ще на етапі його розробки. Це дозволить зміцнити довіру до IoT-рішень та забезпечити стійкість усієї екосистеми.

Ключову роль у цьому процесі відіграє міжгалузева співпраця. Для ефективного впровадження стандартів безпеки необхідно залучати не лише урядові органи, а й приватні компанії, виробників пристроїв, наукові установи та спільноти експертів. Важливо також розробляти сертифікаційні програми, що гарантуватимуть відповідність пристроїв міжнародним вимогам безпеки та сприятимуть їх взаємній сумісності.

Таким чином, сучасна система регулювання безпеки IoT перебуває у стадії активного формування. Попри складність і розрізненість нормативних вимог, позитивна тенденція до глобальної уніфікації стандартів дозволяє сподіватися на формування більш захищеної цифрової інфраструктури.

Безпека IoT залишається одним із ключових викликів сучасного цифрового суспільства. Хоча уряди та організації вже зробили значні кроки у напрямку стандартизації, подальший прогрес можливий лише за умови міжнародної співпраці, уніфікації вимог і впровадження принципів «безпеки за дизайном». Тільки так можна створити цілісну та надійну екосистему Інтернету речей, яка гарантуватиме безпеку користувачів, бізнесу та держави.

Перелік посилань:

1. IoT Security Standards and Regulations: Where Are We Now?. IoT For All. URL: https://www.iotforall.com/iot-security-standards-and-regulations-where-are-wenow (Дата звернення: 17.10.2025).

Михайленко Юлія Іванівна
Студентка групи БСДМ-52, ННІКБЗІ ДУІКТ,
Київ, Україна

ШТУЧНИЙ ІНТЕЛЕКТ ЯК ЗАГРОЗА І ЗАСІБ ЗАХИСТУ В КІБЕРБЕЗПЕЦІ

У другій декаді XXI століття штучний інтелект (ШІ) стає базовою технологією в IT-індустрії й одночасно — потужним ресурсом у сфері кібербезпеки. Впровадження методів машинного навчання та глибинного навчання дозволяє автоматизувати виявлення атак, обробляти великі обсяги логів і швидко реагувати на інциденти. Проте з появою таких можливостей виростає і ризик їхнього використання зловмисниками: ШІ може підвищити масштаб і точність атак, автоматизувати створення фішингу, deepfake-контенту або шкідливого коду. Тому завдання сучасної кібербезпеки — знайти баланс між ефективним використанням ШІ й мінімізацією супутніх загроз.

Ключові слова: штучний інтелект, кібербезпека, захист, adversarial атаки, отруєння даних, етичне використання, оновлення систем.

Під штучним інтелектом розуміють технології, що здатні виконувати завдання, які зазвичай потребують людського мислення: аналіз даних, навчання, прогнозування та ухвалення рішень (ENISA, 2024). У сфері кібербезпеки ШІ використовується для моніторингу мереж, виявлення підозрілої активності, автоматичного реагування на загрози та прогнозування потенційних вразливостей систем. Наприклад, алгоритми машинного навчання можуть автоматично визначати, коли в системі відбувається аномальна поведінка користувачів або програм, що дозволяє швидко локалізувати та блокувати потенційні атаки [1].

Однак, за даними NIST (2024), моделі ШІ залишаються вразливими до «adversarial атак» — ситуацій, коли зловмисники спеціально змінюють вхідні дані, щоб змусити систему помилитися. Також поширеною проблемою є отруєння даних, коли під час навчання моделі до набору додають шкідливу інформацію, що впливає на результати. Крім того, використання ШІ супроводжується ризиком автоматизації кібератак, коли алгоритми здатні самостійно генерувати фішингові повідомлення, шкідливі програми або інші загрози, підвищуючи швидкість і точність атак [2].

Ще однією важливою складовою безпеки є постійне оновлення моделей та баз даних загроз, адже зловмисники постійно створюють нові типи атак. Регулярне оновлення дозволяє підтримувати ефективність алгоритмів і зменшувати ризик використання застарілих систем. Крім того, інтеграція ШІ з іншими технологіями кіберзахисту, такими як багаторівневе шифрування, багатофакторна аутентифікація та поведінковий аналіз користувачів, забезпечує комплексний підхід до безпеки.

Разом з тим, використання ШІ вимагає етичного підходу — захисту приватності користувачів, прозорості рішень систем і запобігання зловживанню технологією (Microsoft, 2023). Етичні аспекти включають контроль за автоматичними рішеннями ШІ, аудит алгоритмів і створення політик, що обмежують потенційні ризики. Саме тому важливо, щоб фахівці з кібербезпеки не лише розуміли технічні аспекти, а й дотримувались принципів відповідальності, прозорості та постійного вдосконалення [3].

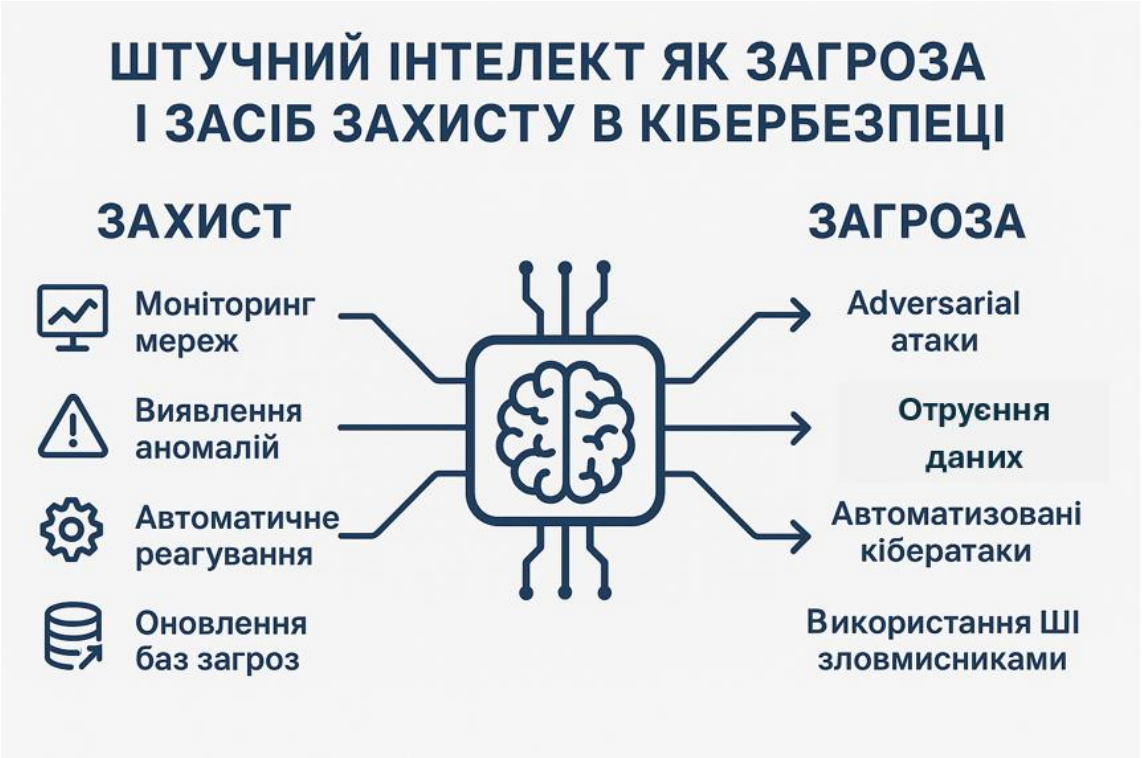

Рис.1. Подвійна роль ШІ у кібербезпеці: захист і загроза

Перелік посилань:

1. European Union Agency for Cybersecurity (ENISA). AI Cybersecurity Challenges: Threat Landscape for Artificial Intelligence. URL: https://www.enisa.europa.eu.
2. National Institute of Standards and Technology (NIST). Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations. URL: https://www.nist.gov.
3. Microsoft Security Blog. Artificial Intelligence in Cybersecurity: Benefits and Risks. URL: https://www.microsoft.com/security/blog.

Душник Володимир Володимирович
Студент групи БСДМ-52, ННІКБЗІ ДУІКТ, Київ, Україна

ВИКЛИК СУЧАСНИМ ЗАГРОЗАМ. DEEPFAKE PHISHING

Deepfake-фішинг є атакою нового покоління, де технології штучного інтелекту використовуються для реалістичного синтезу голосу та відео керівництва чи ключових співробітників з метою фінансового шахрайства або отримання несанкціонованого доступу. Такі атаки ефективно обходять стандартні методи захисту, оскільки апелюють безпосередньо до довіри та психологічних аспектів комунікації.У доповіді буде детально розглянуто механізми цих загроз, проаналізовано їхню небезпеку для сучасного бізнесу та представлено ключові стратегії захисту, що поєднують впровадження сучасних технологій верифікації, розробку чітких внутрішніх процесів та підвищення рівня обізнаності команди.

Ключові слова: Deepfake, фішинг, кіберзагроза.

Еволюція технологій штучного інтелекту (ШІ) не лише оптимізує бізнес-процеси, але й створює нові вектори кіберзагроз. Одним із найбільш небезпечних проявів є deepfake-фішинг — вид цільової атаки (spear-phishing), що використовує синтезовані аудіо- та відеоматеріали для маніпуляції персоналом.

На відміну від класичних фішингових атак, що експлуатують технічні вразливості або неуважність, deepfake-фішинг спрямований на фундаментальні аспекти людської психології та довіри, що робить його виявлення та нейтралізацію значно складнішими. Дана стаття аналізує механізм цієї загрози та пропонує комплексну модель захисту на корпоративному рівні.

Аналіз вектора атаки

Технологічною основою deepfake-фішингу є генеративно-змагальні мережі (GAN) та інші моделі машинного навчання, здатні створювати реалістичні цифрові копії голосу та зовнішності людини на основі обмеженого набору вихідних даних. Зловмисник, використовуючи загальнодоступні матеріали (публічні виступи, інтерв'ю, контент із соціальних мереж), може згенерувати аудіо- чи відеоповідомлення від імені керівника або іншої довіреної особи.

Ключовим фактором успіху такої атаки є поєднання технологічної досконалості та психологічного тиску. Сценарій атаки зазвичай включає елементи терміновості, конфіденційності та авторитету, що змушує об'єкт атаки діяти негайно, ігноруючи стандартні протоколи безпеки.

Практичне підтвердження високого рівня загрози було продемонстровано в інциденті, що стався на початку 2024 року. Фінансовий співробітник гонконгського відділення міжнародної компанії здійснив транзакцію на суму 25 мільйонів доларів США після участі у відеоконференції, де всі учасники, окрім нього самого, були deepfake-копіями [1]. Цей випадок ілюструє, що якість сучасних підробок досягла рівня, за якого візуальна та аудіальна ідентифікація людиною стає ненадійним методом верифікації.

Ключовим фактором, що прискорює поширення цієї загрози, є стрімка демократизація інструментів на основі штучного інтелекту. Якщо раніше подібні технології були доступні лише державним структурам чи великим дослідницьким центрам, то сьогодні створити переконливу підробку голосу можливо за допомогою комерційно доступних онлайн-платформ, що значно знижує поріг входу для зловмисників.

Це розширює потенційні вектори атак: шахраї можуть імітувати не лише вище керівництво , а й представників контрагентів чи постачальників, вимагаючи змінити платіжні реквізити у чинних договорах. Прогнозується, що майбутні атаки стануть ще більш комплексними, поєднуючи deepfake-дзвінки з фішинговими листами для створення багатоетапних, повністю правдоподібних шахрайських сценаріїв.

Комплексна модель протидії

Враховуючи багатогранність загрози, стратегія захисту повинна бути ешелонованою та охоплювати технологічний, процедурний та людський компоненти.

1. **Технологічний рівень.** Основою технічного захисту є безумовне впровадження багатофакторної автентифікації для доступу до критично важливих інформаційних систем та фінансових інструментів. MFA слугує надійним бар'єром, який неможливо подолати лише методами соціальної інженерії. Додатково, перспективним є впровадження рішень, що використовують ШІ для аналізу медіапотоків у реальному часі з метою виявлення цифрових артефактів, що вказують на синтетичне походження контенту.
2. **Процедурний (організаційний) рівень.** Центральним елементом цього рівня є розробка та суворе дотримання внутрішніх регламентів. Ключовим протоколом має стати "позаканальна верифікація" (out-of-band verification). Відповідно до цього протоколу, будь-який запит, що стосується фінансових операцій, зміни прав доступу чи передачі конфіденційної інформації, отриманий через один канал зв'язку (напр., відеодзвінок, електронна пошта), повинен бути підтверджений через інший, незалежний та заздалегідь визначений канал (напр., дзвінок на верифікований мобільний номер).
3. **Людський фактор та корпоративна культура**. Програми навчання персоналу потребують оновлення. Акцент має бути зміщений з розпізнавання традиційного фішингу на формування "культури здорового скептицизму". Співробітники повинні бути навчені ідентифікувати не лише технічні, але й контекстуальні ознаки атаки: нетиповість запиту, надмірний тиск, апелювання до терміновості. Важливо, щоб процедура перевірки не сприймалася як прояв недовіри, а як стандартна та обов'язкова частина корпоративної політики безпеки.

Перелік посилань:

1. Новина CNN// “Finance worker pays out $25 million after video call with deepfake ‘chief financial officer’,” CNN, лютий 4, 2024.// URL: https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk

Кутовий Денис Сергійович
Студент групи БСДМ-52, ННІКБЗІ ДУІКТ, Київ, Україна

АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ. ФІШИНГ

Фішинг є однією з найпоширеніших форм кіберзлочинності, спрямованою на отримання конфіденційних даних користувачів шляхом обману. Зловмисники активно використовують підроблені електронні листи, сайти та повідомлення, імітуючи легітимні ресурси організацій. Розвиток технологій сприяє появі нових форм атак, таких як смішинг та вішинг, що ускладнює їх виявлення. Однак на сьогодні багато наукових праць було присвячено для підвищення обізнаності користувачів та для реалізації технічних бар'єрів, щоб знизити ризик компрометації облікових записів.

Ключові слова: фішинг, кібербезпека, кіберзагроза.

Фішинг продовжує залишатися однією з головних загроз у сфері кібербезпеки, адже поєднує технічні прийоми з елементами соціальної інженерії. Основна мета фішингових атак полягає у викраденні конфіденційних даних користувачів – облікових записів, фінансової інформації, персональних даних тощо. За даними звітів Verizon (2024) та APWG (2024), близько 36 % усіх кіберінцидентів мають ознаки фішингу, що робить цей вид атак наймасовішим у сучасному цифровому середовищі [2;3].

Класичний фішинг передбачає надсилання електронних листів, які імітують офіційні повідомлення від банків, державних органів або популярних сервісів. Такі повідомлення містять посилання на підроблені вебсторінки, створені для збору облікових даних. Сучасні фішингові кампанії все частіше використовують персоналізовані підходи (spear phishing), коли зловмисники збирають попередню інформацію про жертву через соціальні мережі або відкриті джерела OSINT [1, с. 23–27].

З розвитком мобільних технологій з'явилися нові види фішингу: smishing – атаки через SMS, та вішинг – через телефонні дзвінки. Такі атаки орієнтовані на отримання доступу до банківських рахунків або корпоративних даних співробітників. Дослідження показують, що користувачі мобільних пристроїв частіше стають жертвами фішингу, оскільки обмежений розмір екрана ускладнює перевірку достовірності посилань і відправників [4,с.118].

Інтелектуальні системи на основі машинного навчання дедалі частіше застосовуються для виявлення фішингових повідомлень. Використання глибоких нейронних мереж, ансамблевих методів та алгоритмів класифікації дозволяє автоматично аналізувати великі обсяги вхідних листів і визначати ознаки підробленого контенту. Проте навіть найточніші алгоритми можуть давати хибні спрацювання, якщо зловмисники адаптують свої техніки під фільтри безпеки [4]. Це створює потребу у постійному вдосконаленні моделей та використанні комбінованих методів – технічних, поведінкових та освітніх.

Окрім технічних аспектів, важливу роль відіграє людський фактор. Більшість успішних фішингових атак відбуваються через необізнаність

користувачів. Тому організації впроваджують програми підвищення кіберграмотності, які включають тренінги, симуляції фішингових атак та регулярне тестування персоналу. Такі підходи дозволяють зменшити ймовірність переходу користувачів за шкідливими посиланнями на 60–70% [1, с.44]. Серед технічних засобів захисту особливе місце займають системи автентифікації багатьма факторами (MFA), фільтрація електронної пошти, використання DNSSEC та протоколів DMARC, SPF, DKIM для перевірки достовірності відправників. На рівні організаційної безпеки доцільним є впровадження політик обмеження доступу, регулярне оновлення паролів та моніторинг активності користувачів [2; 3].

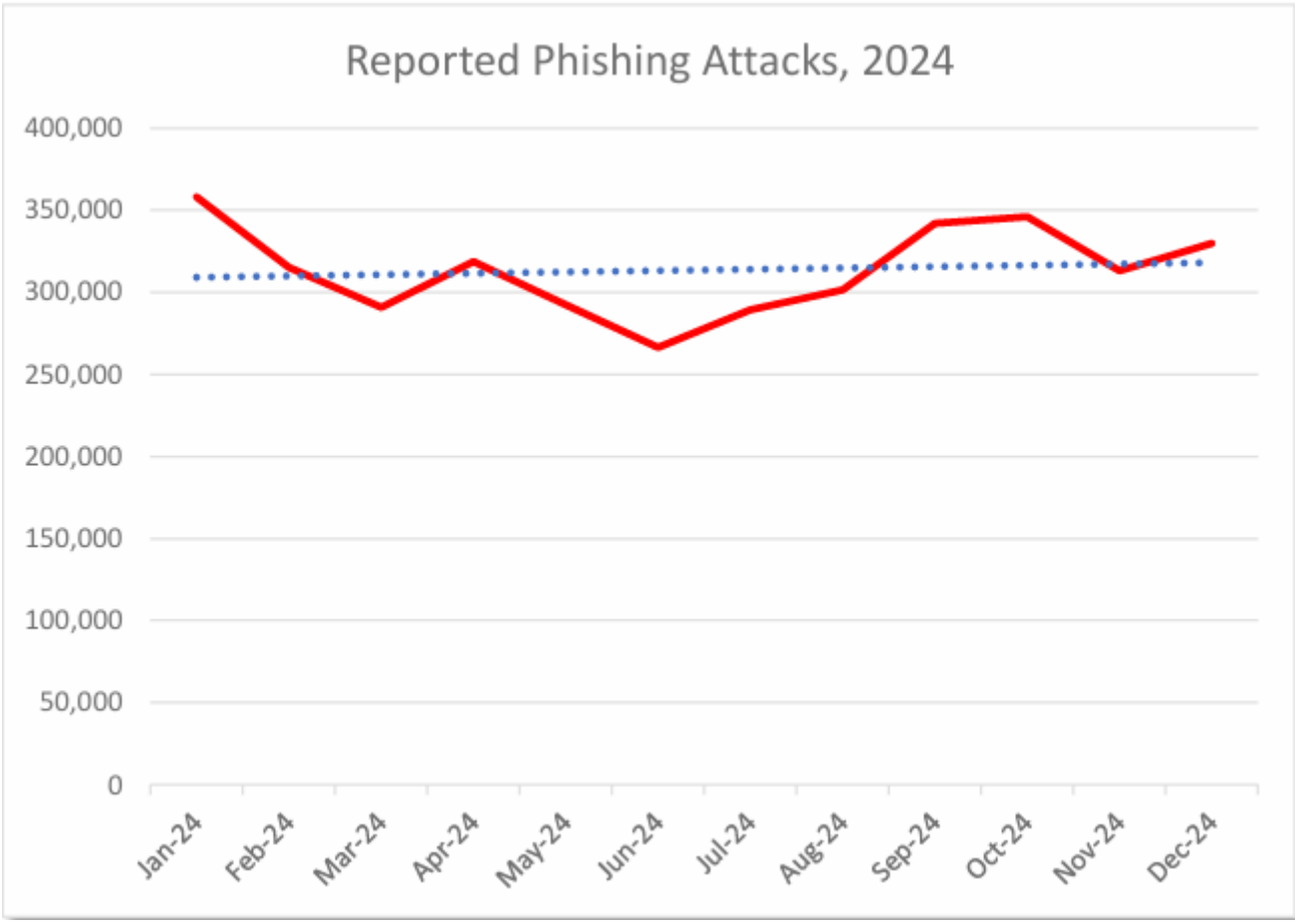

Рис.1. Звіт про тенденції фішингових атак за 4-й квартал 2024 року

Перелік посилань:

1. Jakobsson M., Myers S. Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft. Wiley, 2006.

2. APWG Phishing Activity Trends Report — 4th Quarter 2024. APWG. URL: APWG report.

3. Verizon. 2024 Data Breach Investigations Report (DBIR). Verizon Business, 2024. URL: 2024 Data Breach Investigations Report | Verizon

4. Thakur K. et al. A Systematic Review on Deep-Learning-Based Phishing Detection. Electronics, 2023.

Свалов Л.В.
студент групи 125-22-3,
НТУ «Дніпровська політехніка»,
Дніпро, Україна

Мєшков В.І.
старший викладач каф. БІТ,
НТУ «Дніпровська політехніка»,
Дніпро, Україна

ФРЕЙМВОРК SNITCH ЯК НОВИЙ ПІДХІД ДО ПАСИВНОГО ВИЯВЛЕННЯ ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖ (VPN)

Сучасні кібератаки створюють значні ризики для онлайн-платформ, оскільки зловмисники постійно вдосконалюють методи обходу механізмів геолокаційного контролю та обмеження доступу. Одним із базових інструментів кіберзлочинців є використання технологій віртуальних приватних мереж (VPN) або проксі-сервісів, які дають змогу логічно виходити в Інтернет через інший мережевий сегмент, маскуючи реальну IP-адресу користувача. Такі технології забезпечують ефекти геоспуфінгу, тунелювання та шифрування трафіку. Водночас VPN і проксі мають і позитивне соціальне застосування – дозволяють користувачам у країнах з обмеженим доступом до Інтернету обходити цензуру та зберігати можливість комунікації із зовнішнім світом.

Ключові слова: VPN, проксі, маскування IP-адреси, кібератаки, тунелювання, геоспуфінг.

Існує декілька підходів до виявлення VPN-з’єднань з боку сервера. Пасивний підхід базується на використанні баз даних IP-адрес, поведінковому аналізі та оцінці репутації. Такі бази можуть включати дані про зловживання, результати офлайн-сканування портів та аналіз джерел трафіку. Основними провайдерами подібних сервісів є MaxMind, SEON та IPQualityScore [2-4].

Активний підхід передбачає сканування портів і служб для пошуку типових конфігурацій VPN-програм, однак методи відбитків (fingerprinting) часто дають хибнонегативні результати через можливість зміни стандартних портів або модифікації протоколів. Новіший метод CalcuLatency інтегрує запити ICMP та вимірювання 0trace для визначення наявності VPN чи проксі [5], проте його ефективність обмежується необхідністю отримання ICMP-відповідей, що легко блокується сервером.

Метод глибокої інспекції пакетів (DPI) базується на аналізі аномалій у TCP-заголовках і змін у розмірі MTU/MSS, спричинених інкапсуляцією трафіку, однак для точного визначення потрібні великі обсяги даних і складні моделі машинного навчання. Наприклад, дослідження Goel A. et al. [6] досягло точності 93,8%, а Miller S. et al. [7] – до 97,82% на власних наборах даних.

Новітній підхід SNITCH (Server-side Non-intrusive Identification of Tunneled CHaracteristics) базується на аналізі геолокаційних характеристик з’єднання [1]. Система порівнює фактичний час відповіді між клієнтом і сервером (CSRTT) з очікуваним часом (LSRTT), розрахованим на основі еталонних географічних точок (landmarks), розташованих поблизу ймовірного місцезнаходження клієнта, визначеного через IP-геолокацію. Якщо фактичний час суттєво перевищує теоретично можливий із урахуванням похибки, робиться висновок про

використання VPN або проксі. Додатково SNITCH використовує алгоритм BADPASS для виявлення проксі-серверів і MITM-пристроїв.

Математично залежність описується рівнянням:

$$CS_{RTT} > LS_{RTT} \cdot (1 + C_{EM}) + LS_{STD} + \frac{D_{CL} + GE}{\omega}$$

де CS_{RTT} – фактичний RTT між клієнтом і сервером; LS_{RTT} – мінімальний RTT від сервера до еталонних точок; C_{EM} – коефіцієнт допустимої похибки; LS_{STD} – стандартне відхилення RTT; D_{CL} – географічна відстань між клієнтом і орієнтирами; GE – очікувана похибка IP-геолокації; ω – швидкість поширення сигналу мережею.

У межах дослідження було виміряно понад 130 тисяч з'єднань між 24 тисячами VPN-серверів і клієнтських вузлів по всьому світу [1]. Результати показали, що у випадках, коли традиційні методи не працюють, SNITCH досягає точності до 93% без потреби у попередньому зборі даних. Це робить його перспективним інструментом для підвищення безпеки вебсервісів, захисту від зловживань та ідентифікації прихованого трафіку.

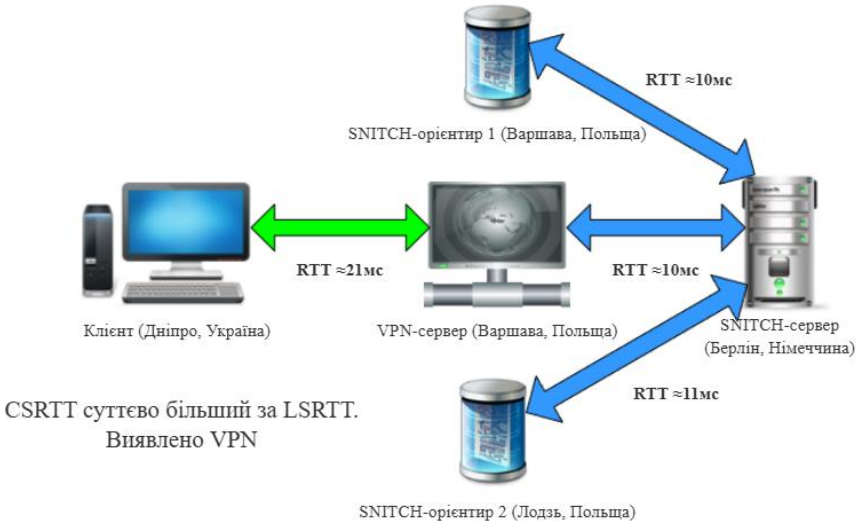

Рис. 1 – Ілюстрація принципу роботи SNITCH

Протидія фреймворку SNITCH можлива, але обмежена фізичними законами передачі сигналів. Єдиним ефективним способом є мінімізація затримки RTT, що досягається використанням VPN-серверів, фізично розташованих поруч із клієнтом, або застосуванням легких високошвидкісних протоколів (XRAY, Hysteria 2), які забезпечують до 90% реальної пропускної здатності. Важкі протоколи, як-от OpenVPN, збільшують затримку через шифрування, а загальна швидкодія VPN визначається також кількістю ядер процесора, виділених серверу для обробки трафіку.

Висновок.

Фреймворк SNITCH демонструє новий, ефективний та неінвазивний підхід до виявлення VPN і проксі-з'єднань на основі геолокаційних характеристик

затримки [1]. Його перевагою є незалежність від попередніх баз даних або сигнатур та висока точність навіть за умов модифікованих протоколів. У той же час метод потребує врахування впливу фізичної відстані, пропускної здатності мережі та типу шифрування. SNITCH можна розглядати як перспективний інструмент для систем виявлення аномалій, запобігання шахрайству та підвищення рівня кібербезпеки онлайн-платформ, а дослідження напрямів його обходу створює нові можливості для розвитку технологій захисту приватності та стійкості мережевих протоколів.

Перелік посилань

1. Schwartz, T., Manor, O., Otung, A. SNITCH: Leveraging IP Geolocation for Active VPN Detection // Proceedings of the 2025 Network and Distributed System Security Symposium (NDSS 2025). – San Diego, CA, USA: The Internet Society, 2025. – С. 1–12.
2. MaxMind. Proxy/VPN Fraud Detection [Електронний ресурс]. – Режим доступу: https://www.maxmind.com/en/solutions/proxy-vpn-fraud-detection (дата звернення: 20.10.2025).
3. SEON. VPN Detection Tests and Screening to Prevent Fraud [Електронний ресурс]. – Режим доступу: https://seon.io/resources/vpn-detection-tests/ (дата звернення: 20.10.2025).
4. IPQualityScore. Proxy & VPN Detection [Електронний ресурс]. – Режим доступу: https://www.ipqualityscore.com/ (дата звернення: 20.10.2025).
5. Ramesh, R., Winter, P., Korman, S., Ensafi, R. CalcuLatency: Leveraging Cross-Layer Network Latency Measurements to Detect Proxy-Enabled Abuse // Proceedings of the 33rd USENIX Security Symposium (USENIX Security ’24). – 2024. – С. 2263–2280.
6. Goel, A., Kashyap, A., Reddy, B. D., Kaushik, R., Nagasundari, S., Honnavali, P. B. Detection of VPN Network Traffic // IEEE Delhi Section Conference (DELCON). – 2022. – С. 1–9.
7. Miller, S., Curran, K., Lunney, T. Detection of Virtual Private Network Traffic Using Machine Learning // International Journal of Wireless Networks and Broadband Technologies. – 2020. – Т. 9. – С. 60–80.

Школовий Д.А.
студент групи БСДМ-62, ННІКБЗІ
ДУІКТ,
Київ, Україна

ПОНЯТТЯ ТА ВАЖЛИВІСТЬ КОРЕЛЯЦІЙ ПОДІЙ БЕЗПЕКИ У КОРПОРАТИВНІЙ МЕРЕЖІ

Зростання кіберзагроз вимагає ефективного моніторингу та швидкого реагування в корпоративних мережах. Ручний аналіз великих обсягів логів з різних джерел є неефективним і схильним до помилок. Для вирішення цієї проблеми критично необхідним є впровадження системи керування інформацією та подіями безпеки (SIEM).

AlienVault OSSIM пропонує потужне рішення для збору, нормалізації, кореляції та аналізу подій безпеки. Його можливості, такі як виявлення вторгнень (IDS), оцінка вразливостей, моніторинг активів та аналіз поведінки користувачів, дозволяють створити комплексну картину безпеки.

Кореляція подій є ключовою функцією, яка об'єднує розрізнені інциденти в єдині, значущі сценарії атак. Це дозволяє фахівцям з безпеки пріоритизувати загрози, скоротити час виявлення та посилити захист мережі.

Ключові слова: кореляція, SIEM, безпека, логи, аналіз подій, AlienVault, події безпеки, SOC.

В IT-інфраструктурі щосекунди відбуваються тисячі подій: користувачі входять у систему, надсилають листи, змінюють налаштування, завантажують файли. Більшість із цих дій — звичайна активність, але деякі можуть бути

частиною атаки. Проблема в тому, що окремо ці події не виглядають підозріло. І саме тут потрібна кореляція [1].

Кореляція — один із ключових механізмів, що лежить в основі SIEM-систем (Security Information and Event Management), які використовуються в SOC (Security Operations Center). Вона дозволяє автоматично виявляти складні, багатоступеневі атаки, які неможливо розпізнати через окремі події [1].

Кореляція подій безпеки (Security Event Correlation) — це автоматизований процес аналізу та зв'язування між собою великої кількості розрізнених подій (логів) з різних джерел у корпоративній мережі для виявлення закономірностей, які можуть вказувати на реальну загрозу, атаку або порушення політики безпеки.

Одним із інструментів є AlienVault OSSIM. В основі AlienVault лежить спрощення операцій з безпеки шляхом об'єднання критично важливих функцій моніторингу в єдину платформу. Традиційні стеки безпеки часто вимагають використання декількох продуктів — одного для управління журналами, іншого для виявлення загроз і окремого інструменту для звітності. AlienVault усуває цю фрагментацію, об'єднуючи всі ці функції в одному рішенні.

Платформа діє як уніфікована система SIEM, забезпечуючи збір, кореляцію та оповіщення про події в режимі реального часу [2]. Інструмент AlienVault SIEM є центральним елементом платформи. Він інтегрується з мережами, серверами та додатками, корелюючи журнали та застосовуючи інформацію про загрози в режимі реального часу. Панелі інструментів забезпечують аналітикам чітку видимість, а автоматизовані правила виділяють аномалії, які потребують уваги.

Рис. 1. The AlienVault OSSIM Dashboard [3]

Основні можливості AlienVault:

Уніфікований збір журналів — платформа збирає дані про безпеку як з локальної інфраструктури, так і з хмарних сервісів, забезпечуючи аналітикам можливість спостерігати за всією активністю в єдиному інтерфейсі.

Інтегрована інформація про загрози — правила виявлення автоматично оновлюються за допомогою останніх інформаційних каналів, що допомагає командам захищатися від нових методів атак.

Інструменти для забезпечення відповідності вимогам аудиту – вбудовані шаблони звітів спрощують підготовку до стандартів, таких як HIPAA, PCI-DSS та SOX, зменшуючи навантаження на команди, що відповідають за відповідність вимогам.

Гнучка масштабованість – AlienVault адаптується до зростання бізнесу, дозволяючи безперешкодно розширюватися від невеликих впроваджень до розгортання в масштабах підприємства [2].

Кореляційний рушій SIEM не просто зіставляє логи, а використовує кілька інтелектуальних методик для перетворення сирих даних на інциденти:

— кореляція на основі правил (Rule-Based Correlation) — основний метод, де аналітики (або сама система) задають чіткі умови. Наприклад: «Якщо 5 невдалих входів на критичний сервер (Подія А) відбулися протягом 10 секунд після сканування портів із того ж джерела (Подія Б), то згенерувати інцидент — «Брутфорс-атака» (Високий ризик)». AlienVault OSSIM використовує попередньо встановлені правила, які постійно оновлюються, застосовуючи інформацію про загрози.

— кореляція на основі евристики/аналізу поведінки (Behavioural Analysis)— ця техніка виявляє аномалії. Система спочатку створює «базовий рівень» нормальної поведінки для користувача, сервера чи програми. Будь-яке значне відхилення від цього рівня автоматично вважається підозрілою подією, яка потребує кореляції та розслідування.

— кореляція на основі топології — зв'язування подій з активами та їхньою критичністю. AlienVault, інтегрує моніторинг активів та оцінку вразливостей, що дозволяє механізму кореляції призначати вищий пріоритет подіям, які стосуються найбільш вразливих або цінних активів [3].

Успішна кореляція залежить від якості вхідних даних. AlienVault вирішує цю проблему, інтегруючи кілька модулів безпеки в єдину платформу:

— Log Management — забезпечує централізований збір даних як з локальної, так і з хмарної інфраструктури, що є основою для подальшого аналізу.

— вбудований IDS (Intrusion Detection System) він відповідає за виявлення мережевих вторгнень, генеруючи події, які потім подаються на кореляційний рушій.

— сканер вразливостей, що виявляє слабкі місця в активах. Якщо корельований інцидент пов'язаний із відомою вразливістю на цільовому сервері, рівень ризику інциденту автоматично підвищується.

Кореляція та аналіз подій безпеки є фундаментальним стовпом корпоративної кібербезпеки, що перетворює розрізнений потік логів на структуровані дані, а впровадження системи AlienVault OSSIM забезпечує організаціям необхідну уніфікацію інструментів безпеки, дозволяючи автоматично ідентифікувати складні сценарії атак, скорочувати час реакції та ефективно запобігати загрозам.

Перелік посилань:

1. Сіленко В. Хаос чи контроль? Як кореляція подій допомагає бізнесу тримати безпеку під контролем. IT Specialist. URL: https://my-itspecialist.com/korelyatsiya-podiy-v-siem (дата звернення: 15.10.2025).
2. Sem. What Is AlienVault? Overview, Benefits, and Use Cases. ClearNetwork, Inc. URL: https://www.clearnetwork.com/what-is-alienvault-platform-advantages/ (дата звернення: 15.10.2025).
3. AlienVault OSSIM Guide. Winmill. URL: https://www.winmill.com/securing-your-work-from-home-network/ (дата звернення: 15.10.2025).

Святський Г.В.
студент групи БСДМ-62, ННІКБЗІ ДУІКТ,
Київ, Україна

ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ АНАЛІТИЧНИМИ ДАНИМИ ЩОДО АТАК РОСІЙСЬКИХ APT-ГРУП

В умовах кібервійни російські APT-групи застосовують складні, довготривалі тактики, спрямовані проти об’єктів критичної інфраструктури (ОКІ). Традиційні реактивні методи неефективні через значний час прихованості (dwell-time) зловмисників. Метою роботи є розробка технології, яка перетворює оперативні дані CERT-UA на аналітичні дані (CTI). Технологія базується на стандартизованій методиці профілювання APT-груп за фреймворком MITRE ATT&CK та створенні автоматизованих наборів вказівок (Playbooks) для швидкого реагування, що мінімізує час реагування на інциденти.

Ключові слова: Аналітичні дані, APT, MITRE ATT&CK, CERT-UA, Playbook.

Обґрунтування необхідності технології

В умовах повномасштабної агресії РФ кібервійна стала невід’ємною складовою стратегічних операцій. Advanced Persistent Threats (APTs), що спонсоруються державою-ворогом, є ключовим інструментом для шпигунства та саботажу, переважно спрямованого проти ОКІ. Тривалий час прихованості APT-атак робить традиційні, реактивні методи захисту, засновані на індикаторах компрометації (IOCs), неефективними. Основна проблема полягає у необхідності перетворення величезного потоку сирих даних про інциденти на структуровану, проактивну та придатну до автоматизації розвідувальну інформацію про загрози (CTI). Метою роботи є розробка технології забезпечення фахівців з кібербезпеки аналітичними даними щодо російських APT-груп.

Аналіз проблеми та джерел аналітичних даних

Кіберзахист повинен змістити фокус з сигнатурної на поведінкову безпеку, оскільки APT-групи активно використовують кастомне ШПЗ та тактики LotL. Тенденції, виявлені CERT-UA, свідчать про зміну тактики на користь довготривалих (6–8 місяців) операцій та атак на ланцюги постачання (Supply Chain Attacks), які слугують основним вектором проникнення до ОКІ. Така складність вимагає від захисту механізмів, які дозволяють прогнозувати наступні кроки зловмисника, а не лише фіксувати факт його присутності.

Джерела Аналітичних Даних та Стандартизація

Національна команда реагування CERT-UA є автентичним джерелом інформації про російські кібероперації, надаючи детальний аналіз TTPs та атрибуції. Для перетворення цих національно-специфічних даних на універсальні, дієві аналітичні дані використовується фреймворк **MITRE ATT&CK®**. ATT&CK є стандартизованою базою знань про тактики та техніки супротивників, що дозволяє проводити картування, оцінку зрілості (SOC Maturity Assessment) та ідентифікацію прогалин у захисті (Defensive Gap Assessment).

Технологія забезпечення аналітичними даними

Запропонована технологія є технологічним внеском і базується на циклічному процесі, що перетворює неструктуровану інформацію про інциденти CERT-UA на стандартизовані, дієві профілі загроз (CTI) та автоматизовані Playbooks.

Методика побудови профілю APT-Групи. Профіль APT є ключовим елементом операційної CTI. Методика складається з:

1. **Співвідношення з ATT&CK:** Кожен елемент поведінки зловмисника, описаний у звітах CERT-UA, повинен бути співвіднесений з конкретними Tactics та Techniques фреймворку ATT&CK. Це перетворює ізольовані IOCs на модель поведінки.
2. **Створення «Теплової Карти» та Gap Assessment:** Візуалізація частоти та критичності TTPs APT-групи дозволяє фахівцям пріоритезувати захисні ресурси. Профіль дозволяє проводити оцінку прогалин у захисті (Gap Assessment), ідентифікуючи TTPs супротивника, проти яких SOC не має механізмів виявлення.

Методика Розробки Наборів Вказівок (Playbook). Playbooks є прямим, дієвим виходом з APT-профілю, призначеним для стандартизації та автоматизації реагування. Головний принцип — мінімізація часу, необхідного зловмиснику для дій. Playbooks мають бути структуровані на основі TTPs MITRE , містити чітко визначені розділи: Tactic/TTP ID, Джерела Логів (Telemetry), Ключові Індикатори Атаки (IOAs) та Кроки Реагування (Remediation Steps). Для досягнення необхідної швидкості Playbooks повинні бути інтегровані в системи автоматизації та оркестрації безпеки (SOAR/XSOAR), що дозволяє автоматично запускати стримуючі заходи (Containment) при виявленні IOA.

Висновки та перспективи

Розроблена технологія забезпечує необхідний методологічний перехід від реактивного аналізу до проактивного управління ризиками, заснованого на TTPs супротивника. Вона створює міст між оперативними звітами CERT-UA та дієвими операціями SOC, дозволяючи: 1) Контекстуалізувати загрози через MITRE ATT&CK; 2) Підвищити швидкість реагування завдяки автоматизованим Playbooks; 3) Оцінити зрілість захисту на основі фактично використовуваних супротивником технік. Практична значущість технології полягає у підвищенні кіберрезистентності ОКІ України.

Перелік посилань:

1. CERT-UA. Російські кібероперації: Аналітика (звіт за перше півріччя 2023)
2. MITRE ATT&CK. https://attack.mitre.org/groups/G0007/

3. Mandiant (Google Cloud). Sandworm Disrupts Power in Ukraine Operational Technology. https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology/
4. УНН. CERT-UA: російські хакери змінили тактику, операції готують пів року. https://unn.ua/news/cert-ua-rosiiski-khakery-zminyly-taktyku-operatsii-hotuiut-piv-roku

Хавер А.В.,
аспірантка групи АІКБ-11, Кафедри ІКБ
ДУІКТ,
Київ, Україна

МЕТОД РАНЖУВАННЯ КРИТИЧНОСТІ ТЕХНОЛОГІЧНИХ ПІДСИСТЕМ ДЛЯ ВИЗНАЧЕННЯ ПРІОРИТЕТНОСТІ ЇХ КІБЕРЗАХИСТУ НА ПРОМИСЛОВИХ ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

В умовах обмежених часових, людських та фінансових ресурсів необхідно раціонально підійти до питання забезпечення кібербезпеки технологічних систем на промислових об'єктах критичної інфраструктури. Отримання несанкціонованого доступу до таких систем може стати передумовою деструктивної кібератаки та як наслідок – загрози життю людей, значним екологічним загрозам та фінансовим збиткам. Своєчасна та повна оцінка кіберризиків для технологічних систем промислових об'єктів критичної інфраструктури дозволяє точно ідентифікувати найбільш критичні інформаційні підсистеми та здійснити їх ефективний кіберзахист.

Ключові слова: кіберзахист, оцінка кіберризиків, об'єкти критичної інфраструктури, критичні підсистеми технологічної системи.

Однією з найбільших загроз з кіберпростору для функціонування технологічних систем промислових об'єктів критичної інфраструктури (далі — ПОКІ) є їх деструктивне ураження з використанням спеціалізованого технологічного троянського програмного забезпечення (далі – СТТПЗ). СТТПЗ – це вид кіберзброї, що має функції маскування від засобів виявлення та/або імітує легітимне програмне забезпечення, може мати функції віддаленого управління та призначене для застосування в конкретній технологічній мережі/конкретних типах технологічних мереж (з урахуванням технологічних особливостей будови інформаційних систем) з метою здійснення кібершпигунства та/або деструктивного кібервпливу.

СТТПЗ для здійснення деструктивного кібервпливу на функціонування технологічної системи ПОКІ, з високою долею ймовірності, буде спрямоване на одну з критичних підсистем. Тому заходи першочергового забезпечення кіберстійкості для таких підсистем мають неухильно та своєчасно виконуватися, а також бути включені до оцінки кіберризиків технологічної системи ПОКІ [1, с. 572].

Основним критерієм критичності підсистеми є її належність до систем, які формують основу технологічного процесу та вимагають безперебійного функціонування. Додатковий ряд критеріїв дозволяє встановити ступінь критичності такої підсистеми:

зупинка або аварія на якій може призвести до шкоди для людей (персоналу/населення), завдати шкоди довкіллю, спричинити значні економічні збитки державі (в окремих випадках), регіону або завдати значних фінансових збитків власнику ПОКІ;

вихід з ладу якої унеможливлює або суттєво ускладнює контрольоване (кероване оператором або автоматикою технологічного процесу) зниження

навантаження або зупинку установки у штатному технологічному режимі, без переходу до аварійного/захисного відключення (так як а**варійна зупинка майже завжди створює вищі ризики**, ніж штатна, що потенційно може порушити безпеку людей, довкілля або завдати значних фінансових збитків);

від якої залежить робота однієї **і більше** інших критичних підсистем (які, в першу чергу самі підпадають під критерії 1–3, так порушення роботи яких може викликати так званий каскадний ефект (така підсистема виконує роль вузла залежностей) [2, с. 82];

відмова принаймні одного елемента якої призводить до критичного порушення технологічного процесу (наявність єдиної точки відмови в системі, наприклад: один ключовий конденсатор у системі охолодження чи/або один блок подачі палива, унікальний пірометр у системі контролю температури котла і т.д.);

відмова якої створює часткову чи повну втрату інформаційно-управлінський функцій — тобто втрачається контроль, моніторинг або координація інших систем (в залежності від обсягів, локально чи глобально може розглядатися більш критичним критерієм та переміщатися на третій пункт з подальшим зсувом решти критеріїв);

відсутність оперативно доступного резерву такої підсистеми (або такий резерв не здатен **покрити мінімально необхідну продуктивність**) або дублюючої потужності.

Вищезазначене корелюєть з критеріями, які зазначені в міжнародних стандартах **ISO 20815/ ISO 14224, IEC 61508/IEC 61511,** IEC 62443.

Розглянуті критерії критичності підсистем технологічної системи покликані виділити найбільш важливі функціональні підсистеми для ефективного розподілу ресурсів їх кіберстійкості.

	Operational			Financial			HSE		
Category	Outage at one site	Outage at multiple sites	National infrastructure and services	Cost (Million USD)	Legal	Public confidence	People onsite	People offsite	Environment
A (High)	>7 days	>1 day	Impacts multiple sectors or disrupts community services in a major way	>500	Felony criminal offense	Loss of brand image	Fatality	Fatality or major community incident	Citation by regional agency or long-term significant damage over large area
B (Medium)	<2 days	>1 hour	Potential to impact sector at a level beyond the company	>5	Misdemeanor criminal offense	Loss of customer confidence	Loss of work day or major injury	Complaints or local community impact	Citation by local agency
C (Low)	<1 day	<1 hour	Little to no impact to sectors beyond the individual company. Little to no impact on community.	<5	None	None	First aid or recordable injury	No complaints	Small, contained release below reportable limits

Рис. 1 Приклад підходу до оцінки критичності систем технологічної системи ПОКІ згідно Leveraging ISA 62443-3-2 For IACS Risk Assessment and Risk Related Strategies"

Проте, для ефективного практичного ресурсорозподілу необхідно визначити механізм, який би дозволяв виділяти пріоритетність кіберзахисту між такими підсистемами всередені технологічної системи. У публікації "Leveraging ISA 62443-3-2 For IACS Risk Assessment and Risk Related Strategies" описано один

з підходів, який полягає в ранжуванні критичності за наслідками, які потенційно можуть наступити у разі реалізації кіберризиків (Рис.1) [3, 7-8].

Автор пропонує використати його як основу та застосувати багатокритеріальний аналіз з ваговими коефіцієнтами для розподілу пріоритетності критичних підсистем технологічної системи ПОКІ.

На першому кроці методу кожному з критеріїв критичності підсистем технологічної системи ПОКІ присвоюється умовна назва/змінна C_x. Передбачено, що, зазвичай, щонайменше одна підсистема технологічної системи ПОКІ відповідає декільком критеріям критичності, при цьому чим більшій кількості критеріїв відповідає підсистема, тим потенційно важливішою є забезпечення її кіберстійкості (збільшується рівень її критичності).

Другим кроком є присвоєння вагових коефіцієнтів (унормовано від 0 до 1, де 0 – найменша критичність, а 1 – максимальна) критеріям за рівнем критичності їх наслідків. Обраний діапазон розділяємо на три семантичні класи: від 0 до 0, 3 — низька критичність; 0,3 — 0, 6 — помірна критичність; 0,6 — 1 — висока критичність.

Розглянемо їх в Таблиці 1 (критерії в таблиці розглядаються в порядку їх зазначення в тексті).

Таблиця 1. Вагові коефіцієнти для критеріїв критичності систем технологічної системи ПОКІ

№ з/п	Умовна назва критерію	Ваговий коефіцієнт	Обгрунтування вагового коефіцієнту
1.	C1	1	Небезпека для людей/довкілля, значні збитки
2.	C2	0,9	Неможливість контрольованої зупинки з переходом до стану “аварії”
3.	C3	0,8	Каскадний ефект
4.	C4	0,7	Єдина точка відмови
5.	C5	0,6	Втрата управління/моніторингу
6.	C6	0,5	Відсутність резерву/дублювання

$$KT_n = C_2 + C_3 + C_x \quad (1),$$

де KT_n - коефіцієнт критичності підсистеми технологічної системи ПОКІ

Третій крок передбачає сумування всіх критеріїв релевантних для обраної підсистеми (Формула 1). Така процедура розрахунків повторюється для всіх критичних підсистем технологічної системи ПОКІ для подальшого ранжування рівня їх критичності та визначення пріоритетності їх кіберзахисту, що документально відображається в оцінці кіберризиків технологічної системи ПОКІ.

Перелік посилань:

1.“Industrial Cybersecurity Second Edition” – Pascal Ackerman, 2021. – 800 p.;

2. Ілона Лагун, Юрій Яцук “Супервізорні системи керування та збору даних”: навчальний посібник. Львів, 2025. с 222;

3. Leveraging ISA 62443-3-2 For IACS Risk Assessment and Risk Related Strategies – [Електрон.ресурс] – режим доступу: https://21577316.fs1.hubspotusercontent-na1.net/hubfs/21577316/2023%20ISA%20Website%20Redesigns/ISAGCA/PDFs/ISAGCA_Leveraging%20ISA%2062443-3-2_White%20Paper.pdf?utm_source=chatgpt.com.

Чумак Михайло Олександрович
Студент групи БСДМ-61, ННІКБЗІ ДУІКТ, Київ, Україна

ЗАСТОСУВАННЯ STRIDE ДЛЯ ОЦІНКИ ЗАГРОЗ У СИСТЕМІ BIG DATA PYTHIA НА БАЗІ SDN

У роботі розглянуто застосування методології STRIDE для аналізу безпеки системи **Pythia**, яка поєднує технології **Big Data** та **програмно-конфігурованих мереж (SDN)** з метою підвищення ефективності обробки даних у платформі **Apache Hadoop**. Наведено опис архітектури Pythia та її взаємодії з контролером **OpenDaylight**, що забезпечує централізоване керування потоками даних через протокол **OpenFlow**. Проведено оцінку основних категорій загроз згідно з методологією STRIDE (спуфінг, втручання, відмова, розкриття інформації, відмова в обслуговуванні, підвищення привілеїв) і визначено механізми їх пом'якшення, серед яких — автентифікація на основі токенів, використання TLS, система Defense4All та модуль AAA. Застосування запропонованого підходу дозволяє підвищити рівень безпеки SDN-інфраструктури та захистити процеси обробки великих даних.

Сучасні системи обробки великих даних (Big Data) потребують високої продуктивності, масштабованості та стійкості до збоїв і атак. Зі зростанням обсягів інформації, що генерується соціальними мережами, сенсорами, мобільними пристроями та вебсервісами, виникає необхідність у створенні ефективних інфраструктур для її обробки та аналізу. Однією з найпоширеніших платформ для цього є **Apache Hadoop**, яка забезпечує розподілене зберігання та паралельну обробку даних [2].

Для підвищення ефективності Hadoop дедалі частіше застосовуються **програмно-конфігуровані мережі (SDN).** Їх ключова особливість полягає у відокремленні площини керування від площини пересилання, що дозволяє централізовано керувати мережевими потоками, адаптуючи їх до поточних потреб застосунків. Такий підхід дає змогу оптимізувати використання пропускної здатності та зменшити затримки, однак водночас створює нові вектори атак. Компрометація SDN-контролера або втручання у трафік можуть поставити під загрозу цілісність і конфіденційність великих даних [1].

Система **Pythia** поєднує переваги Hadoop та SDN, забезпечуючи прогнозування майбутніх комунікацій між вузлами обчислювального кластера і динамічне керування трафіком у реальному часі. Вона складається з двох основних компонентів: проміжного програмного забезпечення Hadoop, яке прогнозує обсяги передач між маперами та редукторами, і оркестраційного контролера, що керує комутаторами через протокол **OpenFlow**. Для централізованого керування Pythia інтегрована з контролером **OpenDaylight (ODL),** який має глобальне уявлення про топологію мережі та навантаження каналів [3]. Це дає змогу мінімізувати переміщення даних і скоротити час виконання завдань MapReduce.

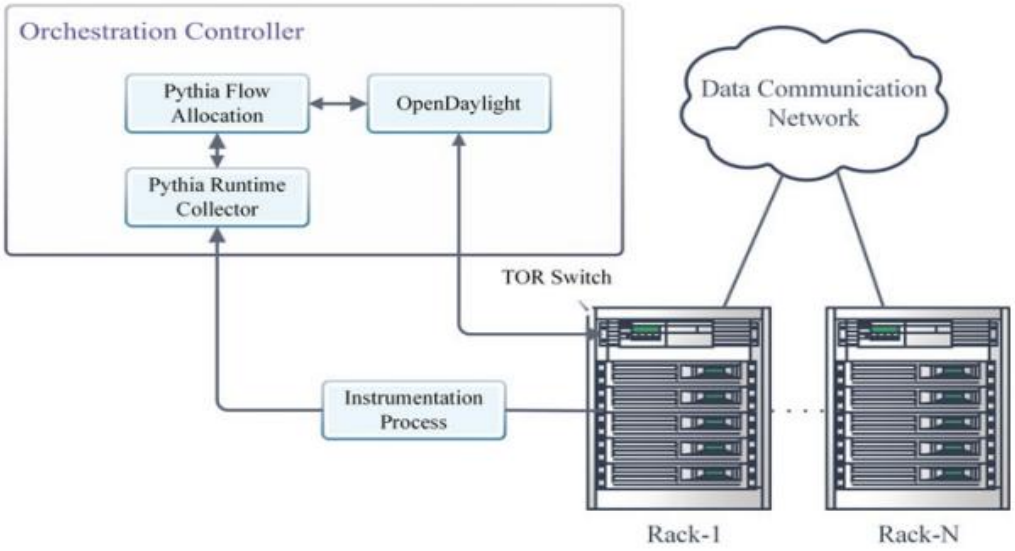

Рис. 1. Архітектура Pythia

Процес роботи системи відбувається так: на кожному вузлі Hadoop інструментальний процес відстежує стан завдань, прогнозує розмір проміжних даних, що підлягають передачі, й надсилає ці прогнози до контролера Pythia. Контролер аналізує отриману інформацію, визначає оптимальні маршрути та передає відповідні правила комутаторам SDN. Таким чином досягається баланс між ефективністю використання мережевих ресурсів і швидкістю обробки даних.

Оскільки Pythia безпосередньо взаємодіє з SDN-контролером, питання безпеки стає критичним. Для аналізу вразливостей застосовано **методологію STRIDE**, розроблену Microsoft. Вона дозволяє системно оцінювати ризики за шістьма категоріями: спуфінг, втручання, відмова, розкриття інформації, відмова в обслуговуванні та підвищення привілеїв. Цей метод є особливо ефективним для проєктів, де важливо оцінити безпеку ще на етапі розробки архітектури [1].

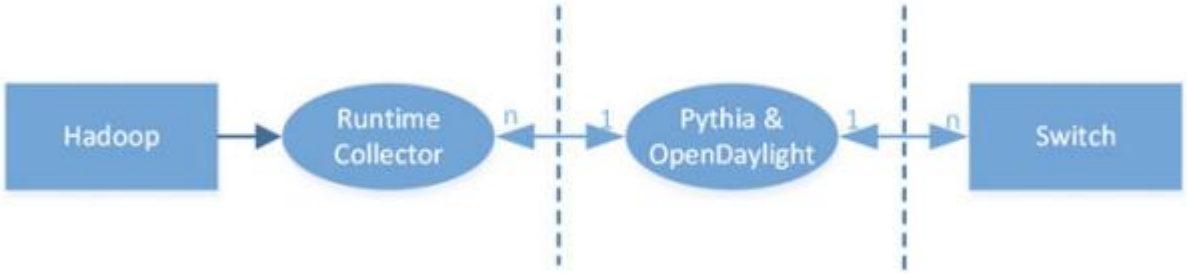

Рис. 2. DFD of Pythia

Результати STRIDE-аналізу показали, що система має кілька критичних точок, але передбачає ефективні механізми пом’якшення ризиків. **Спуфінг (S)** усувається за допомогою модуля **AAA (Authentication, Authorization, Accounting)**, який реалізує токенну автентифікацію користувачів і процесів, запобігаючи несанкціонованому доступу.

Втручання (T) контролюється розширенням **TopGuard**, що виявляє атаки на топологію SDN у реальному часі, а зв'язок між контролером і комутаторами захищено протоколом **TLS**.
Відмова (R) або спроби заперечення дій користувача усуваються через журналювання всіх запитів у модулі AAA, що дозволяє фіксувати будь-які аномальні дії.
Розкриття інформації (I) мінімізується завдяки принципу найменших привілеїв і ізоляції колектора виконання, який має доступ до проміжних даних Hadoop.
Відмова в обслуговуванні (D) запобігається використанням системи **Defense4All**, що відстежує атаки типу DoS на інтерфейси NBI, SBI та сховище даних ODL [3].
Підвищення привілеїв (E) запобігається централізованою політикою керування ролями у AAA, що виключає можливість самовільного розширення прав користувачів.

Проведене дослідження підтверджує, що інтеграція системи Pythia з SDN-технологіями забезпечує підвищення продуктивності Hadoop при збереженні високого рівня безпеки. Методологія STRIDE дала змогу класифікувати потенційні загрози, виявити слабкі місця системи та розробити рекомендації щодо їх усунення. Зокрема, впровадження автентифікації на основі токенів, шифрування TLS, засобів виявлення аномалій та централізованого контролю доступу створює багаторівневий захист як для мережевої інфраструктури, так і для компонентів Hadoop.

У перспективі подальші дослідження можуть бути спрямовані на розробку модулів автоматичного моніторингу безпеки, що використовуватимуть поведінковий аналіз трафіку для виявлення атак у режимі реального часу. Інтеграція Big Data, SDN і методів моделювання загроз відкриває можливості для створення ефективних та безпечних обчислювальних середовищ нового покоління.

Перелік посилань:

1. Khondoker, R. *SDN and NFV Security: Security Analysis of Software-Defined Networking and Network Function Virtualization.* Lecture Notes in Networks and Systems, vol. 30. Springer, 2018. 235 p.
2. Dean, J., & Ghemawat, S. *MapReduce: Simplified Data Processing on Large Clusters.* Communications of the ACM, 2008.
3. OpenDaylight Project. *OpenDaylight Documentation Portal*. [Online]. Available: https://www.opendaylight.org

Шапко Олег Олександрович
студент групи БСДМ-51, ННІЗІ ДУІКТ, Київ, Україна

Фішинг як ключова загроза кібербезпеки: механіки, психологія та захист

Фішинг — це один з найпоширеніших та найнебезпечніших методів кібератак, основним об’єктом якого є людина. Він не є технологічним порушенням, а використовує методи соціальної інженерії, такі як психологічний тиск та створення відчуття терміновості, щоб маніпулювати поведінкою користувача. Метою фішингу є викрадення конфіденційних даних: логінів, паролів, платіжної інформації та інших цінних активів.Актуальність цієї загрози полягає в її масштабах та ефективності. Від атак страждають як приватні особи, так і великі організації, включаючи фінансові установи, медичні заклади та державні структури. Незважаючи на розвиток технологічних засобів захисту, саме людський фактор залишається найслабшою ланкою у ланцюзі безпеки.

Ключові слова: фішинг, соціальна інженерія, кібербезпека, конфіденційні дані, двофакторна автентифікація, менеджер паролів, людський фактор, навчання персоналу.

На чому грунтується фішинг

Загалом це різновид кібершахрайства, мета якого — отримання конфіденційної інформації (логінів, паролів, банківських даних, персональних відомостей) шляхом масової розсилки підробних повідомлень від імені відомих компаній або осіб. В основі його ефективності лежить не технічна перевага, а тонка маніпуляція людською психікою. Шахраї вміло експлуатують два ключові психологічні тригери: тиск та терміновість. Повідомлення створюються так, щоб викликати у жертви сильну емоцію — страх («Ваш акаунт буде заблоковано!»), жадібність («Ви виграли приз!»), цікавість чи відчуття обов'язку («Терміново підтвердьте дані!»). Вказівка на обмежений час для реакції («Якщо ви не відповісте протягом 24 годин...») позбавляє користувача можливості критично оцінити ситуацію, перевірити автентичність листа та змушує діяти імпульсивно, переходячи за зловмисним посиланням або відкриваючи небезпечний вкладень.

Еволюція та різноманіття фішингових атак

З часом фішинг еволюціонував від примітивних масових розсилок до високоцільових та витончених атак. Сьогодні можна виділити кілька основних видів:

- Масовий фішинг: Розсилка тисяч листів у надії, що хтось «клюне».
- Цільовий фішинг (Spear Phishing): Атака, спрямована на конкретного співробітника або відділ. Шахраї заздалегідь вивчають жертву через соцмережі, щоб повідомлення звучало максимально правдоподібно.
- Валінг (Whaling): Різновид цільового фішингу, націлений на «велику здобич» — топ-менеджерів , які мають доступ до найцінніших даних.
- Вішинг (Vishing) та Смішинг (Smishing): Використання для атак телефонних дзвінків та SMS-повідомлень відповідно.

Чому фішинг зараз настільки популярний

Фішинг залишається надзвичайно популярним з кількох причин. По-перше, це висока рентабельність та низький поріг входу. Для зловмисника не потрібні значні технічні ресурси; достатньо орендувати готові фішингові конструктори та бази email-адрес. По-друге, людський фактор — найслабша

ланка в безпеці. Можна вибудувати багаторівневу технічну захист, але одна невдала дія співробітника зводить її нанівець. По-третє, поширення віддаленої роботи та хмарних сервісів значно розширило поверхню атаки, надавши зловмисникам більше точок для входу та способів імітувати корпоративні комунікації.

Необхідність цілеспрямованого захисту

Саме через опору на людський фактор неможливо захиститися від фішингу виключно технічними засобами (антивірусами, фільтрами пошти). Навіть найдосконаліші системи можуть пропустити хитромудро сконструйованого листа. Тому кожна сучасна компанія зобов'язана приділяти окрему увагу боротьбі з фішингом. Це не просто «пункт у бюджеті ІБ», а критично важлива інвестиція в людський капітал, яка включає безперервне навчання співробітників, регулярне тестування їхньої пильності за допомогою навчальних фішингових атак та вироблення чітких регламентів дій у підозрілих ситуаціях. Ігнорування цієї загрози неминуче веде до фінансових втрат, репутаційної шкоди та витоку конфіденційної інформації.

Основи захисту: технології та правила

- Двофакторна автентифікація (2FA) — найпотужніший бар'єр
  Це найефективніший захід для блокування наслідків фішингу. Суть в тому, що для входу в систему потрібно знати не тільки пароль (що можуть викрасти), але й мати доступ до фізичного пристрою — вашого телефону. Навіть якщо співробітник введе свої дані на фішинговому сайті, зловмисник не зможе увійти в систему без одноразового коду з застосунку (наприклад, Google Authenticator) або SMS-підтвердження. Обов'язкове впровадження 2FA для корпоративної пошти та критичних сервісів — це «золотий стандарт» безпеки, який нейтралізує 99% успішних краж облікових даних.
- Менеджери паролів та контроль цифрової гігієни
  Менеджери паролів (наприклад Bitwarden, 1Password або інш.) вирішують одразу дві критичні проблеми. По-перше, вони дозволяють створювати та зберігати складні унікальні паролі для кожного сервісу. Це запобігає катастрофі, коли один викрадений пароль відкриває доступ до всіх акаунтів співробітника. По-друге, вони часто мають функцію автоматичного заповнення, яка не спрацює на фальшивому сайті, що є додатковим сигналом небезпеки для користувача. Це не просто зручність, а фундаментальний інструмент для запобігання доміно-ефекту після успішної фішингової атаки.
- Антифішингові фільтри та чіткий регламент дій
  Технічний захист поштових скриньок — це перший і обов'язковий бар'єр. Спеціалізовані системи на основі штучного інтелекту аналізують метадані, заголовки, посилання та вкладення листів, блокуючи до 99% спаму та очевидних фішингових атак. Однак,

технології не всемогутні. Тому в парі з ними має працювати простий і зрозумілий кожному співробітнику регламент: «Знайшов підозрілий лист — не клацай, не відповідай, негайно перешли в IT-відділ». Це перетворює кожного працівника з потенційної жертви на активний елемент системи безпеки.

- Постійне навчання працівників,в тому числі через симуляцію фішингів. Будь-які інструкції без практики неефективні. Найкращим методом навчання є регулярні навчальні фішингові атаки. Компанія створює безпечні копії реальних фішингових листів і розсилає їх співробітникам. Той, хто «потрапив на гачок», не несе покарань, а отримує миттєвий зворотний зв'язок і коротке пояснення, на що треба було звернути увагу. Це схоже на тренувальну тривогу — вони допомагають співробітникам не лише знати правила, але й застосовувати їх в стресовій ситуації, коли зловмисник тисне на терміновість.

Перелік посилань:

1. **How to Protect Yourself from Phishing Attacks** [Електронний ресурс] // Cybersecurity and Infrastructure Security Agency. – 2025. – URL: https://www.cisa.gov/news-events/news/how-protect-yourself-phishing-attacks (дата звернення: 21.10.2025).
2. **Your Pa$$word doesn't matter** [Електронний ресурс] / Alex Weinert // Microsoft Tech Community. – 2025. – URL: https://techcommunity.microsoft.com/t5/azure-active-directory-identity/your-pa-word-doesn-t-matter/ba-p/731984 (дата звернення: 21.10.2025).
3. **Digital Identity Guidelines: Authentication and Lifecycle Management** [Електронний ресурс] // National Institute of Standards and Technology. – 2025. – URL: https://pages.nist.gov/800-63-3/sp800-63b.html#sec5 (дата звернення: 21.10.2025).
4. **Defense in Depth Explained** [Електронний ресурс] // Cybersecurity and Infrastructure Security Agency. – 2025. – URL: https://www.cisa.gov/news-events/news/defense-depth-explained (дата звернення: 21.10.2025).

Піскунов Костянтин Валерійович
студент групи БСДМ-51, ННІЗІ ДУІКТ, Київ, Україна

Кібербезпека корпоративних інформаційних систем за допомогою Active Directory

Active Directory Domain Services (AD DS) може слугувати ядром кіберзахисту корпоративних систем у парадигмі Zero Trust. Запропоновано практичний підхід, що поєднує сегментацію керуючої площини (Tier 0) і використання привілейованих робочих станцій (PAW), мінімізацію «стоячих»

секретів (LAPS, gMSA, ротація KRBTGT), централізоване впровадження політик (GPO, безпекові базлайни, WDAC/AppLocker), зміцнення автентифікації (Kerberos-first, Credential Guard, смарт-картки/AD CS) та безперервний моніторинг (Defender for Identity, SIEM), включно з відпрацьованим планом відновлення лісу AD. Очікуваний ефект — зменшення площі атаки, обмеження бічного руху, підвищення стійкості бізнес-процесів і спрощення відповідності галузевим стандартам.

Ключові слова: Active Directory, Zero Trust, керування ідентичностями, GPO, LAPS, gMSA, WDAC (AppLocker), Credential Guard, привілейований доступ (PAM/PAW), Defender for Identity, SIEM, відновлення лісу AD.

Active Directory є ієрархічною службою каталогів для зберігання й надання даних про облікові записи, комп'ютери, групи, політики й довірчі відносини, а також забезпечує автентифікацію та авторизацію через Kerberos і взаємодіє з іншими механізмами безпеки Windows. Логічна модель AD включає ліси, домени, сайти, контролери домену та організаційні одиниці, що дозволяє розмежувати повноваження, створити чіткі межі довіри та відобразити структуру організації у політиках безпеки. Усе це робить AD центральним контрольним пунктом для реалізації принципів найменших привілеїв, сегментації доступу.

Zero Trust у контексті AD. У моделі Zero Trust ключовими стають перевірка ідентичності та стану пристрою, мікросегментація мережі, мінімізація привілеїв та постійна аналітика сигналів. AD забезпечує основу для цих принципів: групи безпеки формують «шлюзи рішень» для доступу, а GPO дозволяють централізовано впроваджувати вимоги до конфігурації, журналювання та контролю виконання. Інтеграція з Microsoft Entra ID додає MFA, умовний доступ і оцінку ризику входів, зберігаючи контроль локальних активів через доменні політики.

Захист автентифікації та облікових даних. Класичні атаки на AD — це викрадення та повторне використання хешів (Pass-the-Hash), компрометація облікового запису KRBTGT з підробкою «золотих квитків» Kerberos, зловживання делегаціями та слабкими протоколами. Зниження ризику починається з архітектурних рішень: використання групи Protected Users для критичних облікових записів з забороною кешування секретів і слабких алгоритмів, регулярна ротація пароля KRBTGT за затвердженим планом, вимкнення застарілих схем автентифікації та примус NTLMv2 із підписуванням. Для підвищення стійкості варто впроваджувати смарт-картки або інші сертифікатні методи входу на базі AD CS та PKINIT, що переводить автентифікацію на криптографічні ключі, зменшуючи залежність від паролів.

Керування привілеями та доступом адміністраторів. Привілейований доступ має бути тимчасовим, цільовим та відслідковуваним. Модель розмежування рівнів (Tier 0/1/2) виділяє AD, контролери домену та інші «керуючі площини» в найбільш захищену категорію, де діють окремі облікові записи та пристрої. Привілейовані робочі станції (PAW) забезпечують жорстко загартоване середовище для виконання чутливих завдань, зведене до мінімально необхідного набору функцій. Для тимчасової ескалації прав у локальних доменах може застосовуватися Windows-орієнтована модель PAM на базі Microsoft Identity Manager, яка надає рольові привілеї з обмеженим часом дії та журналює використання.

Централізоване впровадження політик і контроль виконання. GPO залишаються базовим механізмом для нав’язування конфігурацій безпеки в домені: від аудиту подій, UAC та мережних параметрів до вимог криптографії та політик паролів. Практична відправна точка — застосування Security Baselines з інструментарію Microsoft Security Compliance Toolkit з поетапним тестуванням, адаптацією під сумісність і подальшим порівнянням поточних GPO із рекомендованими значеннями. Для зменшення площі атаки на виконання коду ефективним є застосування AppLocker або Windows Defender Application Control, які дозволяють працювати за принципом «дозволено лише довірене». Слабку ланку локальних адміністраторів на кінцевих точках усуває Windows LAPS, що автоматично обертає та зберігає у каталозі унікальні паролі локальних адмін-акаунтів, тоді як для сервісних акаунтів у фермах та кластерах доцільно використовувати gMSA з автоматичною ротацією ключів і керуванням SPN.

Моніторинг, виявлення і реагування. Жодна політика не буде достатньою без постійного моніторингу та кореляції подій. Microsoft Defender for Identity встановлює сенсори, що аналізують трафік та журнали AD, виявляючи підозрілу автентифікацію, розвідку, бічний рух, зловмисні делегації, спроби «золотого квитка» та інші тактики. Інтеграція з Microsoft Defender XDR і вивантаження подій до SIEM спрощує розслідування, підсилює детекції між доменами безпеки та автоматизує реакції.

Відмовостійкість і план відновлення. Оскільки AD є критичним реєстром прав, необхідні регулярні повні та стан-системи резервні копії контролерів домену, перевірка відновлюваності та документований план відновлення лісу з відпрацюванням кроків у тестових середовищах. Наявність сценарію «лісового відновлення» з чіткими ролями, порядком розгортання перших контролерів у кореневому домені, авторитетною синхронізацією SYSVOL, перевиданням сертифікатів та перевірками реплікації знижує RTO і ризик помилок у кризовій ситуації. Важливо включити до плану й періодичну ротацію чутливих секретів, зокрема KRBTGT, а також процедури перевірки цілісності політик і довірених відносин після інцидентів.

Гібридні сценарії та розширення можливостей. Сучасні корпоративні системи часто поєднують локальні домени AD із Microsoft Entra ID. Такі сценарії дозволяють масштабувати Zero Trust за межі кампуса через умовний доступ, оцінку ризиків входів, керування пристроями та політики комплаєнсу, водночас зберігаючи силову роль GPO на серверах і робочих станціях. Керування LAPS і WDAC через Intune, кореляція подій Defender for Identity із сигналами з хмари та централізована оркестрація реакцій утворюють єдине «поле зору» для SecOps. При цьому принципова вимога залишається незмінною: чітко визначене «ядро керування» (Tier 0) із мінімальною площею атаки, сегментацією доступів та сильними контролями автентифікації.

Практичний план впровадження. Реалістичний маршрут починається з аудиту ризиків і побудови карти прав, далі — ізоляція Tier 0, розгортання й загартування PAW, застосування базових GPO-базлайнів, увімкнення розширеного аудиту та журналювання, впровадження LAPS і gMSA, поступове

переведення критичних облікових записів до Protected Users з вимогою смарт-карток, увімкнення WDAC або AppLocker у режимі аудиту з подальшим переведенням в режим примусу, розгортання Defender for Identity та інтеграції із SIEM, а також підготовка, документування і регулярне відпрацювання плану відновлення лісу. Важливо встановити вимірювані показники зрілості, зокрема частку ресурсів під керуванням базлайнів, відсоток покриття LAPS, час виявлення і усунення критичних вразливостей, частоту ротації KRBTGT і сервісних секретів, а також частоту тренувань з відновлення.

Active Directory залишається опорою безпеки корпоративних інформаційних систем, оскільки концентрує керування ідентичностями, політиками та довірою. Поєднання принципів Zero Trust, жорсткої гігієни привілеїв, централізованого нав'язування конфігурацій і сучасного моніторингу дає змогу різко знизити ризики бічного руху та ескалації, а відпрацьований план резервування та відновлення забезпечує стійкість до інцидентів. Такий підхід узгоджується з міжнародними стандартами управління безпекою, а також із національними вимогами, і практично доводить, що «периметр ідентичності», належно спроєктований на платформі AD, є найдієвішою лінією захисту для цифрових активів організації.

Перелік посилань:

1. Active Directory Domain Services overview [Електронний ресурс] // Microsoft Learn. — Режим доступу: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview (дата звернення: 10.10.2025).
2. Group Policy overview for Windows Server [Електронний ресурс] // Microsoft Learn. — Режим доступу: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/group-policy/group-policy-overview (дата звернення: 11.10.2025).
3. NIST SP 800-207: Zero Trust Architecture [Електронний ресурс] // National Institute of Standards and Technology (NIST). — Режим доступу: https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf (дата звернення: 15.10.2025).
4. Securing privileged access: Enterprise access model (Tiering) [Електронний ресурс] // Microsoft Learn. — Режим доступу: https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-access-model (дата звернення: 20.10.2025).

Карпеченков Микита Павлович
студент групи УБДМ-61, ННІКБЗІ ДУІКТ,
Київ, Україна

ВИКОРИСТАННЯ ШІ: ЗАГРОЗИ ДЛЯ КІБЕРБЕЗПЕКИ ТА ІНСТРУМЕНТ ЗАХИСТУ

Штучний інтелект зарекомендував себе як цінний інструмент у кібербезпеці, оскільки завдяки використанню алгоритмів машинного навчання, спроможний аналізувати великі обсяги даних і виявляти загрози, які невловимі для операторів та аналітиків з кібербезпеки. Виявлення шкідливого програмного забезпечення, фішингових атак, фіксація підозрілої поведінки в мережах відбувається швидше за використання системи штучного інтелекту, ніж відслідковується командою людей. Це робить їх революційним інструментом для організацій, які прагнуть посилити свій захист в епоху все більш витончених кібератак, однак треба враховувати загрозу використання ШІ зловмисниками, щоб вчасно розробляти кібербезпекові контрзаходи.

Ключові слова: штучний інтелект, кіберзагрози ШІ, автономні кібератаки, контрзаходи, кібербезпека

У міру вдосконалення штучного інтелекту концепція автономних кібератак стає реальністю. На відміну від традиційних кібератак, які часто залежать від втручання людини, автономні атаки можуть ініціюватися та виконуватися без будь-якого прямого втручання людини. Це створює новий рівень непередбачуваності та масштабу, який може перевантажити існуючу інфраструктуру кібербезпеки.

Наприклад, автономне шкідливе програмне забезпечення може адаптуватися до середовища, навчаючись обходити протоколи безпеки та змінювати свою поведінку на основі зворотного зв'язку в режимі реального часу. Така поведінка призводить до швидкої адаптації та появи вторинних загроз, і означає, що навіть первинна атака за використання шкідливого програмного забезпечення буде виявлена та нейтралізована Слід враховувати, що цілеспрямована атака за використання штучного інтелекту, може самонавчатися та адаптуватися, що робить традиційні механізми захисту, такі як: антивірусне програмне забезпечення або брандмауери, менш ефективними. Результатом є потенційно нескінченна гра "в кота і мишу", в якій захисники постійно намагаються наздогнати зловмисників.

Штучний інтелект також може використовуватися в атаках типу "відмова в обслуговуванні" (DDoS) [1] . Ці атаки перевантажують мережу великим трафіком, що призводить до відмови в обслуговуванні. За допомогою штучного інтелекту зловмисники можуть використовувати розподілені ботнети для запуску масштабних, складних DDoS-атак, які набагато складніше нейтралізувати. Штучний інтелект також може оптимізувати атаку в режимі реального часу, забезпечуючи її максимальну ефективність, що потенційно може спричинити широкомасштабні порушення у функціонуванні інформаційної системи [1].

Більше того, кібератаки на основі штучного інтелекту здатні виявляти вразливі місця з раніше недосяжною точністю. Завдяки машинному навчанню зловмисники можуть автоматизувати виявлення слабких місць у програмному забезпеченні, мережах і навіть у поведінці людей. Така особливість робить кібератаки на основі штучного інтелекту небезпечними, оскільки вони можуть завдавати ударів з високою точністю, часто залишаючись непоміченими, поки не стане занадто пізно.

Хоча роль ШІ в кібербезпеці часто розглядається як оборонна, його інтеграція в повсякденні технології також викликає значні занепокоєння щодо конфіденційності. Для функціонування системи ШІ потребують величезних обсягів даних, які часто є особистими, конфіденційними, іноді збираються без відома користувачів. У міру свого вдосконалення системи ШІ здатні аналізувати великі дані, створюючи детальні профілі окремих осіб і груп, часто без їхньої явної згоди.

Однією з найбільших проблем є використання ШІ в цілях спостереження. Технологія розпізнавання облич, що базується на штучному інтелекті набуває

широкого використання. Так, уряди, корпорації, приватні особи використовують технології ШІ для відстеження та спостереження за людьми. В свою чергу, це викликає серйозні питання щодо права на приватність та того, чи не перебувають люди постійно під спостереженням без їхнього відома. Хоча ця технологія може використовуватися в цілях безпеки, наприклад для ідентифікації злочинців або запобігання тероризму, вона також відкриває можливості для масового спостереження з боку авторитарних режимів або корпоративних структур з сумнівними мотивами [2].

Системи штучного інтелекту також використовуються для збору величезних обсягів персональних даних із соціальних мереж, онлайн-взаємодій та інших цифрових слідів. Ці дані потім використовуються для прогнозування поведінки, таргетування реклами та впливу на рішення. Проблема виникає, коли ці дані не захищені належним чином або використовуються в цілях, про які особи не знають або, на які не давали згоди. Скандал навколо Cambridge Analytica, який розкрив, як дані Facebook використовувалися для впливу на вибори, є суворим нагадуванням про те, як особиста інформація може бути використана в спосіб, що підриває приватність і демократію.

У міру інтеграції систем штучного інтелекту в цифрову інфраструктуру, інформація про клієнтів банків та установ охорони здоров'я становить підвищений інтерес з боку кіберзлочинців. Крадіжка або маніпулювання конфіденційними даними, такими як: медичні записи або фінансова інформація, може мати руйнівні наслідки, як для окремих осіб, так і для організацій. Складність атак, що базуються на штучному інтелекті, означає, що навіть невелика вразливість системи може бути використана в більших масштабах, ставлячи під загрозу безпеку даних користувачів інформаційних систем.

Хоча ШІ обіцяє бути неупередженим інструментом, він не позбавлений недоліків. Однією з найважливіших проблем у сфері ШІ та кібербезпеки є потенційна упередженість. Системи ШІ настільки ефективні, наскільки ефективні дані, на яких вони навчаються, і якщо ці дані є недосконалими або упередженими, ШІ може поширювати ці упередження [2].

Наприклад, було доведено, що системи розпізнавання обличчя менш точні в ідентифікації людей з темнішим відтінком шкіри, особливо жінок. Це викликало занепокоєння, що спостереження на основі ШІ може непропорційно націлюватися на меншини, що призведе до несправедливого спостереження та профілювання. Аналогічно, системи ШІ, що використовуються при прийнятті рішень про найм або надання кредитів, можуть посилити існуючі суспільні упередження, що призведе до дискримінації певних груп.

Отже, виходячи із вищезазначеного стає зрозумілим, що контрзаходи є необхідністю, і вбачаються у:

– ШІ проти ШІ (дієвий спосіб боротьби з кібератаками, керованими штучним інтелектом, — це використання більш досконалих оборонних систем на основі ШІ). Такий підхід називають принципом "ШІ проти ШІ", де "хороші" системи ШІ протидіють "поганим". Проактивне полювання на загрози

передбачає не пасивне очікування атак, а постійний аналіз мережевого трафіку, системних журналів та поведінки користувачів за допомогою [4].

– ШІ з метою виявлення аномалій, що можуть сигналізувати про потенційний напад. Такий підхід дозволяє виявляти й нейтралізувати небезпеку ще до того, як вона здатна завдати шкоди [3].

– Питання упередженості (для підвищення надійності систем ШІ важливо використовувати різноманітні й репрезентативні набори даних, що відображають багатогранність реального світу, адже це знижує ризик упередженості та неточності щодо окремих демографічних груп).

– Збереження людського контролю. Підхід “human-in-the-loop” передбачає, що остаточні рішення у важливих ситуаціях не повинні повністю залежати від алгоритмів, а людина має можливість переглянути й за потреби змінити або скасувати висновки системи, якщо вони можуть мати значні наслідки.

Отже, штучний інтелект виступає потужним каталізатором фундаментальних змін у сфері кібербезпеки, водночас, генеруючи безпрецедентні виклики як технологічного, так і етичного характеру.

З іншого боку, інтеграція ШІ у повсякденні технології створює значні ризики для конфіденційності та безпеки даних. Залежність систем ШІ від масивів даних уможливлює масштабне спостереження, зокрема через технології розпізнавання облич та несанкціоноване профілювання поведінки. Крім того, виявлено проблему систематичної упередженості алгоритмів, що виникає через нерепрезентативні навчальні дані та може призводити до посилення дискримінації. Тож, мають розроблятися контрзаходи у режимі реального часу з урахуванням постійного удосконалення кібератак через використання ШІ та його самонавчання.

Перелік посилань:

1. Nick Bostrom; Artifical Inteligence – strategies, vulnerabilities - https://www.oxfordmartin.ox.ac.uk/blog/nick-bostrom-on-artificial-intelligence
2. Stuart Rassel – Airtifical Inteligence and control problem - https://www.researchgate.net/publication/356505374_Artificial_Intelligence_and_the_Problem_of_Control
Here’s Why AI May Be Extremely Dangerous - Whether It’s Conscious or Not
3. https://www.scientificamerican.com/article/heres-why-ai-may-be-extremely-dangerous-whether-its-conscious-or-not/
4. The 15 Biggest Risks Of Artificial Intelligence
https://www.forbes.com/sites/bernardmarr/2023/06/02/the-15-biggest-risks-of-artificial-intelligence/

Дасюк Юрій Євгенійович
студент групи БСДМ-52, ННІКБЗІ ДУІКТ, Київ, Україна

СУЧАСНІ OSINT-ТЕХНОЛОГІЇ В РАМКАХ КІБЕРАГРЕСІЇ ПРОТИ УКРАЇНИ

Дана теза має на меті розглянути OSINT-технології як один з сучасних інструментів в рамках агресії проти України, її національної безпеки. В сучасному світі, збір та аналіз інформації з відкритих джерел став простіше, ніж будь-коли для цього. Основними загрозами, що виникають через доступність методів OSINT, є: фішинг, викрадення персональних даних, несанкіонований доступ та втручання в державні інформаційні системи, збір, аналіз та використання корпоративної інформації. Окремо також розглянуто методи захисту від, та протидії загрозам, що виникли внаслідок використання OSINT-інструментів.

Ключові слова: OSINT, кібербезпека, кіберзагроза.

Можливість ворожої розвідки збирати та аналізувати дані з відкритих джерел про об’єкти критичної та військової інфраструктури України є однію з ключових загроз для безпеки держави.

До негативних варіантів використання OSINT можна віднести:

– Фішинг, соціальна інженерія: аналіз даних з відкритих джерел інформації дозволяє ворожій розвідці збирати персональні дані та компромат і робити дос’є на потенційних жертв. Це дозволяє робити персоналізовані атаки, ціллю яких будуть конкретні особи або підприємства, а також значно підвищити ефективність атак.

– Аналіз корпоративних даних: ворожі агенти збирають публічну інформацію про структуру, місцезнаходження, діяльність бізнесу, або ж дані про ключових співробітників та їх діяльність. Ця інформація потім використовується для організації атак.

– Виявлення останніх вразливостей: зловмисники можуть використовувати інформацію з технічних журналів, блогів, форумів, груп, тощо, для пошуку останніх вразливостей в програмному забезпеченні сервісів.

Основними відкритими джерелами інформації в розвідці є:

– Доступні супутникові знімки: різноманітні безкоштовні та комерційні супітникові платформи, такі як Geo-Airbus Defense, Maxar Technologies та Sentinel Browser, дозволяють відслідковувати та порівнювати зміни на бажаних об’єктах в режимі реального часу, що створює ризики для національної безпеки України.

– Відкриті державні реєстри України: доступні відкриті бази даних України дозволяють збирати ПІБ, номери телефонів, адреси електроних поштових скриньок та іншу інформацію про власників та робітників об’єктів критичної та оборонної інфраструктури. В результаті за допомогою отриманих даних можливо сформувати вектор атаки на підприємства.

– Геолокаційні сервіси: доступні сервіси на кшталт Google Maps, OpenStreetMap, Google Earth та інші картографічні онлайн сервіси для навігації

дозволяють отримати координати стратегічно важливих об’єктів та критичної інфаструктури: різноманітних транспортних вузлів, електростанцій та енерговузлів, військових баз, заводів оборонного комплексу, промислових об’єктів, складів, тощо.

– Сервіси для пентестингу та збору інформації про IT-інфраструктуру та її вразливості: безкоштовні та комерційні платформи для дослідження вразливостей IT-інфраструктури України дозволяють збирати інформацію про відкриті вузли мережі, що відкриває простір для різноманітних загроз, хакерських атак та розвідки.

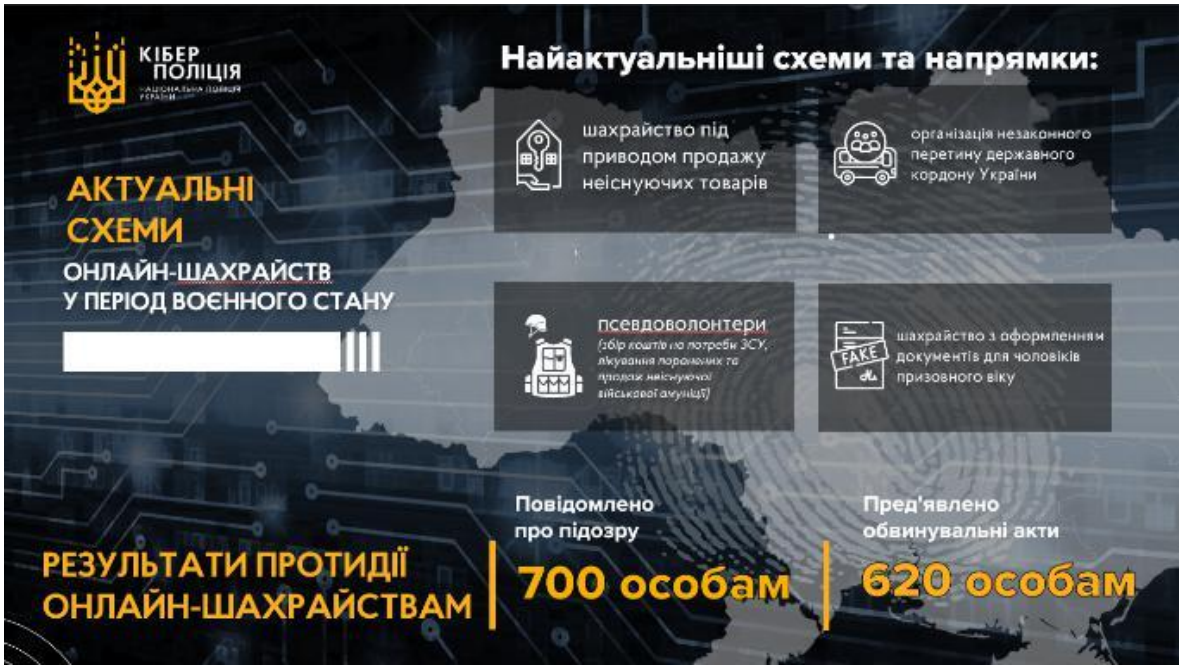

Рис. 1. Актуальні схеми онлайн-шахрайств у період воєнного стану

Для протидії сучасним OSINT-інструментам на державному рівні варто обрати комплексний підхід для захисту персональних даних та інформації.

Зокрема:

– Підвищення рівня обізнаності про інформаційну безпеку та гігієну, поведення контр-OSINT освітніх заходів: розуміння управління конфіденційною інформацію, вміння розпізнавати фішингові атаки, розуміння суті та механізмів функціонування OSINT-інструментів, тощо.

– Законодавче регулювання доступу до відкритих джерел даних: юридичне регулювання та вдосконалення політики розкриття державної інформації, обмеження публікації відомостей про стратегічнії об’єкти та їх працівників, обмеження публікації потенційно небезпечних даних, обмеження доступу до деяких публічних баз даних та державних реєстрів, тощо.

– Розвиток державної міжвідомчої співпраці: координація зусиль державних органів, бізнесу та громадянського суспільства у сфері кібербезпеки

для оперативного реагування на кіберзагрози та вдосконалення встановлених механізмів протидії їм.

– Проведення регулярних аудитів безпеки та моніторинг інтернет мережі для пришвидшеного виявлення витоків даних: огляд тематичних форумів та груп, перевірка витоків паролів та моніторинг доступності інформації в пошукових агрегаторах.

Для безпеки особистих даних в мережі важливо виконувати наступні дії:

– Обмежити потрапляння особистої інформації в мережу.

– Використовувати анонімні або фальшиві акаунти для роботі в мережі.

– Відмовитись від безкоштовних сервісів та програм, що збирають і аналізують персональні дані.

– Підміняти та маніпулювати вказаними даними та технічною інформацією (IP-адреси, технічні дані системи або браузера).

– Використовувати сервіси багаторазової автентифікації.

– Уникати витоку геолокації та видаляти EXIF-метадані з файлів при публікації фото або відео в мережу.

– Робити публікацію фото та відео з затримкою у часі.

Перелік посилань:

1. Report on the activities of the CyberPolice Department of the National Police of Ukraine in 2024 (2025). CyberPoliceDepartment of the National Police of Ukraine. https://cyberpolice.gov.ua/news/zvitpro-diyalnist-departamentu-kiberpolicziyi-naczionalnoyi-policziyi-ukrayiny-u--roczi-7074/ (дата звернення 13.10.2025).

2. CERT-UA processed 4315 cyber incidents last year (2025). State Service for Special Communications and Information Protection of Ukraine. https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv (дата звернення 12.10.2025).

3. Hwang, Y.-W., Lee, I.-Y., Kim, H., Lee, H., & Kim, D. (2022). Current Status and Security Trend of OSINT. Wireless Communications and Mobile Computing, 2022. https://doi.org/10.1155/2022/1290129 (дата звернення 12.10.2025).

4. Ivkova, V., & Opirsky, I. (2025). OSINT-TECHNOLOGY AS A THREAT TO STATE'S CYBERSECURITY. Electronic professional scientific publication "Cybersecurity: education, science, technology". https://doi.org/10.28925/2663-4023.2024.26.682 (дата звернення 12.10.2025).

Боярчук Віталій Ярославович
Студент групи ФІТ 1-7м ДТЕУ
Науковий керівник - Терейковський Ігор
Київ, Україна

ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ЛОГІСТИЧНИХ ІНФОРМАЦІЙНИХ СИСТЕМ АГРАРНИХ ПІДПРИЄМСТВ

Цифрова трансформація аграрного сектору зумовлює активне впровадження логістичних інформаційних систем (ERP, CRM, WMS), які забезпечують автоматизацію постачання, транспортування, зберігання та аналітики. Проте зростання рівня інтеграції IT-рішень створює нові ризики для інформаційної безпеки, зокрема витік конфіденційних даних, порушення цілісності маршрутної інформації або зупинку логістичних процесів унаслідок кібератак.

За даними досліджень [1;2], понад 60% підприємств агросектору, що використовують ERP-системи, не мають комплексного захисту інформаційних потоків. Основними загрозами є несанкціонований доступ до корпоративних мереж, DDoS-атаки на веб-портали, маніпуляції з логістичними даними та ураження інфраструктури шкідливим ПЗ. Особливо вразливими залишаються системи, що об’єднують IoT-пристрої (датчики транспорту, складські сенсори тощо), оскільки вони часто не мають вбудованих механізмів автентифікації.

Метою дослідження є підвищення рівня кібербезпеки логістичних інформаційних систем аграрних підприємств шляхом розроблення рекомендацій щодо побудови захищеної архітектури та впровадження систем моніторингу подій безпеки.

Для досягнення мети застосовано методи системного аналізу, ризик-орієнтований підхід відповідно до стандартів **ISO/IEC 27001:2022** [3], **NIST SP 800-82** [4], а також інструменти моделювання бізнес-процесів (BPMN, ERD) для ідентифікації точок контролю безпеки в логістичних ланцюгах.

У результаті запропоновано архітектуру кіберзахисту логістичної інформаційної системи агропідприємства (рис. 1), яка включає такі рівні:

- користувацький рівень із багатофакторною автентифікацією;
- рівень прикладних систем (ERP/CRM) із моніторингом доступу до критичних модулів;
- рівень мережевого захисту з фаєрволом, IDS/IPS-системами та шифруванням трафіку;
- SOC-модуль (Security Operation Center) для централізованого збору, кореляції та аналізу подій;
- рівень резервного копіювання із географічним дублюванням даних.

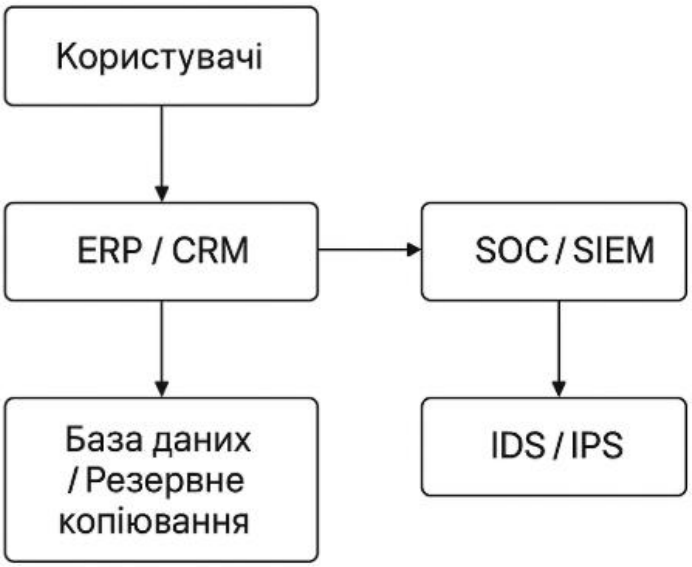

Рис. 1 – Архітектура захищеної логістичної інформаційної системи аграрного підприємства.

Даний підхід дозволяє мінімізувати час реагування на інциденти, запобігти внутрішнім порушенням і забезпечити безперервність логістичних процесів навіть у разі кібератак. Впровадження SIEM-платформ (IBM QRadar, Splunk, Wazuh) забезпечує автоматичний аналіз журналів ERP-систем та підвищує прозорість управління ризиками.

Отже, забезпечення кібербезпеки логістичних інформаційних систем аграрних підприємств вимагає поєднання системного аналізу, багаторівневого технічного захисту та постійного моніторингу. Реалізація запропонованої архітектури сприятиме підвищенню стійкості агрологістичних компаній до сучасних кіберзагроз та ефективній інтеграції IT-рішень у виробничі процеси.

Ключові слова: кібербезпека, логістика, аграрне підприємство, інформаційна система, SOC, ERP, системний аналіз, кіберризики.

Перелік посилань:

1. Cybersecurity in Smart Agriculture: A Systematic Literature Review. Computers & Security, 2025.
2. Cybersecurity Threats in Agriculture Supply Chains: A Comprehensive Review. ResearchGate, 2024.
3. ISO/IEC 27001:2022 Information Security Management Systems.
4. NIST SP 800-82 Rev. 3. Guide to Industrial Control Systems Security. NIST, 2023.

Проценко М.В.
Студент групи БСДМ-51, ННІКБЗІ ДУІКТ,
Київ, Україна

СИСТЕМА ВИЯВЛЕННЯ ФІШИНГОВИХ АТАК У ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ

Фішингові атаки є однією з найпоширеніших загроз сучасного інформаційного простору. Їхня мета — отримання конфіденційних даних користувачів шляхом обману, зокрема через підроблені вебсайти, електронні листи або повідомлення у соціальних мережах. З кожним роком фішинг стає дедалі складнішим: зловмисники вдосконалюють методи підробки інтерфейсів, доменів і навіть сертифікатів безпеки. Саме тому створення системи, здатної автоматично виявляти такі атаки, є актуальним завданням у сфері кіберзахисту організацій.

Інформаційна система будь-якої установи містить масиви важливих даних — фінансову, персональну, комерційну інформацію. Потрапляння цих даних до рук зловмисників може призвести до суттєвих збитків, втрати репутації або повного паралічу діяльності організації. За даними *FBI Internet Crime Report (2024)*, понад 36 % усіх кіберінцидентів у корпоративному секторі мають фішингове походження, а загальні збитки у світі від таких атак перевищили 12 мільярдів доларів.

Основна ідея побудови системи виявлення фішингових атак полягає у створенні комплексу програмних модулів, які здатні здійснювати аналіз електронних повідомлень, вебресурсів і мережевого трафіку в реальному часі. Такі системи повинні визначати потенційно небезпечні елементи за сукупністю ознак: структури URL-адреси, наявності підозрілих ключових слів, відсутності безпечного з’єднання, а також поведінкових факторів користувачів.

У межах дослідження було проаналізовано існуючі рішення у сфері виявлення фішингу — *PhishTank API*, *Google Safe Browsing*, *SpamAssassin*, а також сучасні підходи з використанням алгоритмів машинного навчання. Зокрема, застосування методів **Random Forest**, **Support Vector Machine** та **Logistic Regression** дозволяє досягати точності класифікації понад 95 % при достатньому обсязі навчальних даних.

Запропонована система виявлення фішингових атак у інформаційній системі організації має багаторівневу архітектуру (рис. 1):

Рис. 1 - Архітектура системи виявлення фішингових атак

1. **Модуль збору даних** — здійснює моніторинг вхідних повідомлень, журналів доступу та запитів до вебресурсів.
2. **Модуль попередньої обробки** — видаляє шум, нормалізує дані та виділяє ключові атрибути (довжина URL, кількість піддоменів, використання IP у домені тощо).
3. **Аналітичний модуль** — реалізує класифікацію повідомлень на основі алгоритмів машинного навчання.
4. **Модуль реагування** — автоматично блокує підозрілі запити або сповіщає адміністратора безпеки.

Для навчання системи було використано корпус даних із понад 10 000 реальних URL-адрес, з яких 60 % — фішингові. Результати тестування показали, що запропонована модель демонструє точність виявлення 96,1 %, при цьому кількість хибних спрацьовувань не перевищує 3,5 %. Така ефективність свідчить про доцільність використання машинного навчання як основного інструменту боротьби з фішинговими загрозами.

Ключовим аспектом ефективності системи є її адаптивність. Модель повинна регулярно оновлюватися відповідно до нових типів атак, адже зловмисники постійно модифікують свої методи. Для цього у системі передбачено механізм самонавчання, який оновлює базу ознак на основі зібраних даних у процесі експлуатації.

Впровадження подібної системи в інформаційне середовище організації дозволяє:

- зменшити ризики компрометації користувацьких облікових записів;
- автоматизувати процес перевірки вхідної кореспонденції;
- мінімізувати людський фактор у виявленні підозрілих повідомлень;
- забезпечити швидке реагування на кіберінциденти.

Система може бути інтегрована у внутрішні корпоративні рішення або використовуватися як окремий модуль безпеки. Перспективним напрямом подальших досліджень є розширення функціоналу за рахунок гібридного підходу — поєднання традиційних сигнатурних методів із поведінковим аналізом, а також використання технологій глибокого навчання (*Deep Learning*) для аналізу контенту електронних листів і вебсторінок.

Таким чином, розроблена система виявлення фішингових атак підвищує рівень інформаційної безпеки організації, забезпечує раннє попередження загроз і сприяє зменшенню наслідків кібератак. Вона може бути впроваджена як у державних, так і в приватних структурах, де є потреба у надійному захисті персональних і корпоративних даних.

Ключові слова: фішинг, інформаційна безпека, машинне навчання, кіберзахист, виявлення атак, аналіз даних.

Перелік посилань:

1. Symantec Enterprise Security Report (2023). *Phishing Trends and Tactics*. Режим доступу: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/phishing-trends

2. Basnet, R. B., Mukkamala, S., & **Sung, A. H.** (2012). *Detection of Phishing Attacks: A Machine Learning Approach*. *Studies in Fuzziness and Soft Computing*, Springer, pp. 373–383.

3. Verma, R., Das, A. (2021). *What's in a URL? Fast Feature Extraction and Machine Learning-Based Phishing Detection*. *Journal of Cybersecurity*, Vol. 7(1). Режим доступу: https://doi.org/10.1093/cybsec/tyaa006

Харькевич Д.О.
студент групи БСДМ-51, ННІЗІ ДУІКТ,
Київ, Україна

ЗАСТОСУВАННЯ ГОМОМОРФНОГО ШИФРУВАННЯ ДЛЯ ЗАХИСТУ КОНФІДЕНЦІЙНИХ ОБЧИСЛЕНЬ У ХМАРНИХ СЕРЕДОВИЩАХ

З розвитком цифровізації та масового переходу бізнесу й державних установ до хмарних сервісів питання збереження конфіденційності даних набуло особливої актуальності. Попри те, що більшість провайдерів хмарних послуг гарантують захист інформації під час її зберігання та передавання, момент обробки даних залишається найбільш уразливим. У цей час інформація зазвичай розшифровується, що створює ризики витоку навіть у разі формального дотримання політик безпеки.

Ключові слова: Гомоморфне шифрування, хмарні обчислення, конфіденційність даних, криптографічний захист, безпечна обробка, хмарна безпека, гібридний підхід.

Одним із найперспективніших напрямів вирішення цієї проблеми є використання гомоморфного шифрування, яке дає змогу виконувати обчислення над зашифрованими даними без їх розшифрування. Це означає, що навіть сторонній хмарний сервер може проводити операції з конфіденційними даними, не маючи доступу до їхнього змісту (рис. 1). Такий підхід відкриває нові можливості для безпечного використання хмарних обчислень у сферах, де конфіденційність має критичне значення — наприклад, у фінансових технологіях, медицині або державному управлінні.

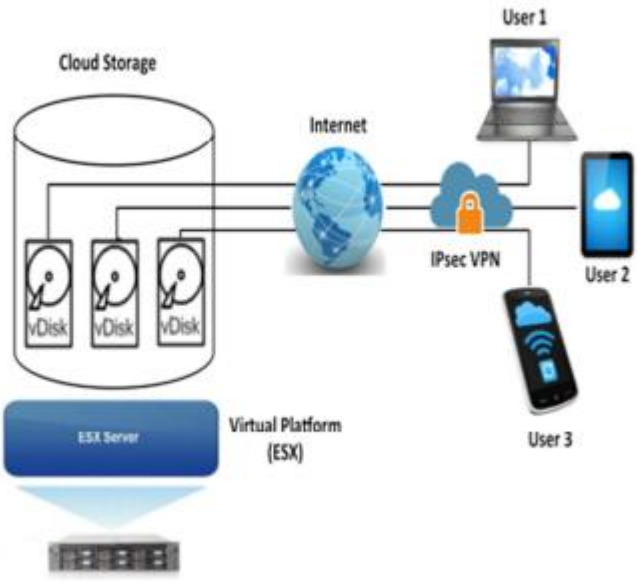

Рис. 1 - Схема, що представляє базову архітектуру хмарних обчислень

Проте широке впровадження гомоморфного шифрування стримується високими обчислювальними витратами. Виконання навіть простих арифметичних операцій над зашифрованими даними потребує значно більше часу й ресурсів, ніж над відкритими. На практиці це призводить до затримок, які можуть у десятки разів перевищувати час виконання звичайних обчислень.

Додатковою проблемою є суттєве збільшення обсягу шифротекстів, що впливає на вимоги до пам’яті та пропускної здатності каналів зв’язку.

Проаналізувавши кілька сучасних реалізацій гомоморфного шифрування — зокрема бібліотеки Microsoft SEAL, HEAAN та PALISADE. Вони відрізняються рівнем повноти підтримуваних операцій і ступенем гомоморфізму: від часткового (PHE) до повного (FHE). Спостереження показали, що повне гомоморфне шифрування забезпечує найвищий рівень безпеки, однак має найбільші накладні витрати. Обмежені або часткові схеми можуть бути більш доцільними для задач, де потрібна лише базова обробка даних — наприклад, підрахунок статистичних показників чи агрегування.

У результаті спостереження запропоновано гібридний підхід до використання гомоморфного шифрування у хмарних середовищах. Його суть полягає в тому, що найчутливіші дані (ідентифікаційна інформація, медичні записи, фінансові баланси) обробляються у зашифрованому вигляді, тоді як менш критичні фрагменти проходять традиційну обробку (рис. 2). Це дозволяє досягти балансу між безпекою та продуктивністю, не перевантажуючи систему надлишковими обчисленнями.

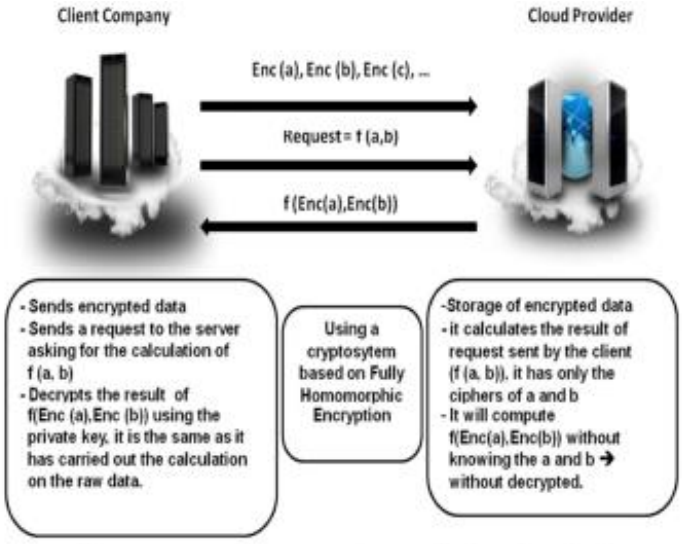

Рис. 2 - Повністю гомоморфне шифрування, застосоване до хмарних обчислень

Випробування показали, що при застосуванні такого підходу час обчислень зростає у 2–3 рази порівняно зі звичайними методами, однак рівень захисту значно підвищується. Для ряду застосувань, де швидкодія не є критичним фактором, такий компроміс можна вважати прийнятним. Зокрема, це стосується аналітичних систем, сервісів прогнозування або систем медичної діагностики, які обробляють персональні дані пацієнтів.

Отже, гомоморфне шифрування є одним із найбільш перспективних напрямів розвитку криптографічного захисту в умовах поширення хмарних технологій. Його впровадження дозволяє істотно знизити ризики несанкціонованого доступу до конфіденційної інформації навіть у разі компрометації інфраструктури провайдера. Подальші дослідження мають бути спрямовані на оптимізацію алгоритмів і пошук ефективних способів інтеграції гомоморфного шифрування у практичні хмарні рішення без значних втрат у продуктивності.

Перелік посилань:

1. Homomorphic Encryption for Secure Cloud Computing / Z. Brakerski, C. Gentry, V. Vaikuntanathan. arXiv. [Електронний ресурс] – Режим доступу: https://arxiv.org/pdf/1409.0829

2. Potential of Homomorphic Encryption for Cloud Computing Use / A. Gentry, S. Halevi, N. Smart. MDPI Journal of Cybersecurity and Privacy. [Електронний ресурс] – Режим доступу: https://www.mdpi.com/2624-800X/3/1/4

Глущенко В. О.
студентка групи 1-7м, ФІТ ДТЕУ,
науковий керівник — Терейковський І. А.
м. Київ, Україна

БЛОКЧЕЙН ЯК ГАРАНТ ЦІЛІСНОСТІ ДАНИХ ТА АУДИТНОГО СЛІДУ

Технологія блокчейн (Distributed Ledger Technology, DLT) зазвичай асоціюється з криптовалютами, однак її потенціал значно ширший. Вона може стати потужним інструментом для підвищення кібербезпеки корпоративних і державних інформаційних систем. Головною перевагою DLT є незмінність (immutability) даних, що забезпечує довіру до цифрової інформації та унеможливлює приховані маніпуляції.

Метою дослідження є дослідження можливості блокчейн-технології для забезпечення цілісності аудитних журналів та запобігання несанкціонованим змінам у корпоративних інформаційних системах.

Ключові слова: блокчейн, розподілена книга (DLT), незмінність (Immutability), цілісність даних, журнали аудиту, кібербезпека, криптографічне хешування, децентралізація, усунення ризику маніпуляцій, Єдина Точка Відмови (SPOF).

1. Незмінність і децентралізація як основи безпеки.

Блокчейн — це послідовність взаємопов’язаних блоків даних, кожен з яких містить криптографічний хеш попереднього. Зміна будь-якої інформації в одному блоці автоматично змінює хеші наступних блоків, що дозволяє іншим вузлам виявити спробу підробки. Таким чином, дані стають незмінними, а довіра до системи — незалежною від одного адміністратора [1; 2].

2. Вразливості централізованих систем.

Традиційні системи зберігання даних страждають від трьох ключових проблем [3]:

- можливість видалення або зміни логів після зламу;
- залежність від адміністратора, який може приховати сліди порушень;
- наявність Єдиної Точки Відмови (SPOF) — злам центрального сервера призводить до втрати даних і зупинки роботи всієї системи.

3. Використання блокчейну для захисту аудитних журналів.

Застосування блокчейн-технології (DLT) дозволяє ефективно вирішити проблему забезпечення незмінності та достовірності аудитних журналів у корпоративних і державних інформаційних системах [1; 2].

У традиційних централізованих базах даних журнали подій можуть бути змінені або видалені адміністратором чи зловмисником після кібератаки, що унеможливлює точне відновлення подій. Використання блокчейну усуває ці ризики, адже всі дані зберігаються у вигляді послідовно пов'язаних блоків, а будь-яка спроба зміни запису призводить до зміни хеш-коду всіх наступних блоків, що робить підміну помітною [1].

У системах аудиту доцільно не зберігати повні лог-файли у блокчейні, а фіксувати лише цифрові відбитки (хеш-коди), створені криптографічними алгоритмами. Через певний інтервал часу система генерує хеш поточного стану журналів і зберігає його у блокчейні разом із часовою міткою.

У результаті будь-яке втручання в логи (навіть зміна одного символу) призведе до невідповідності між збереженим у DLT хешем і новим обчисленням. Це дозволяє однозначно виявити факт модифікації, що є особливо цінним під час розслідування кіберінцидентів [3].

Таким чином, блокчейн не запобігає самій зміні файлів на сервері, але гарантує виявлення і доказовість таких змін, перетворюючи аудитні журнали з вразливого ресурсу на незаперечний цифровий доказ. Цей підхід є ефективним інструментом підвищення кіберстійкості корпоративних систем і об'єктів критичної інфраструктури [2; 3].

4. Виклики впровадження.

Попри значний потенціал, впровадження блокчейн-рішень у корпоративне середовище супроводжується низкою технологічних і економічних викликів [1; 3].

Основною проблемою є низька швидкість обробки транзакцій у розподіленій мережі порівняно з централізованими системами. Кожен блок має бути підтверджений великою кількістю вузлів, що суттєво уповільнює роботу та робить публічні блокчейни малопридатними для високонавантажених бізнес-процесів, таких як банківські чи торговельні операції [1].

Ще одним обмеженням є незворотність записів. Дані, одного разу внесені до розподіленої книги, не можуть бути змінені або видалені, навіть якщо вони містять помилку. Це потребує підвищеної точності введення інформації та створює ризики для компаній, де часто відбуваються зміни даних [2].

Окрім цього, інтеграція DLT потребує істотних фінансових і людських ресурсів: спеціалізованих розробників, адаптації IT-архітектури, а також узгодження між усіма учасниками мережі. Це робить процес упровадження складним і довготривалим, особливо для великих організацій [3].

Втім, попри ці обмеження, блокчейн залишається перспективним напрямом розвитку систем захисту даних, оскільки створює недовірне середовище та гарантує цілісність і прозорість інформації, що є ключовими чинниками для кібербезпеки сучасних інформаційних систем [2; 3].

Перелік посилань

1. Гончарук І. А., Бойко О. В., Сущенко О. М. (2020). Аналіз і обґрунтування використання наявних блокчейн-рішень для захисту цифрових активів. *Open Archive NURE*. URL: https://openarchive.nure.ua/bitstreams/99ac7828-cb4c-4f74-82f5-9712df370006/download
2. Гавриловська Л. М., Захарчук Р. В. (2024). Застосування блокчейн-технологій у формуванні безпеки електронного документообігу. Журнал якості та математичних технологій. URL: https://jqmth.donnu.edu.ua/article/download/14956/14862
3. Оніщенко М. С., Касьян Р. О. (2023). Перспективи використання технології блокчейн у сфері захисту інформації для потреб сектора безпеки і оборони. Системи і технології зв'язку, інформатизації та кібербезпеки. URL: https://journal.viti.edu.ua/index.php/cicst/article/view/95

Бідник Н.С.
студент групи БСДМ-62, ННІКБЗІ ДУІКТ,
Київ, Україна

РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ

Розслідування кіберінцидентів є ключовим елементом системи кібербезпеки, що забезпечує своєчасне виявлення, аналіз та усунення наслідків несанкціонованих дій у цифровому середовищі. Така діяльність поєднує технічні, організаційні та аналітичні методи, спрямовані на встановлення джерела інциденту, відновлення подій та підвищення стійкості інформаційних систем. Ефективність розслідування залежить від використання сучасних технологій, які дозволяють швидше обробляти великі обсяги даних і забезпечувати точніший аналіз цифрових доказів.
Ключові слова: кіберінциденти, системи кібербезпеки, сучасні технології.

Кіберінцидентом вважається будь-яка подія, що порушує або може порушити конфіденційність, цілісність чи доступність інформаційних ресурсів. До таких випадків належать фішингові атаки, шкідливе програмне забезпечення, несанкціонований доступ до облікових записів, DDoS-атаки, експлуатація вразливостей або витоки даних. Для запобігання наслідкам подібних подій важливо мати ефективну систему реагування та ретельно організований процес розслідування.

Процес розслідування кіберінцидентів охоплює кілька ключових етапів: 1. Виявлення та ідентифікація. Здійснюється аналіз сповіщень із систем моніторингу (SIEM, IDS/IPS) для визначення типу загрози та її критичності. 2. Локалізація та ізоляція. На цьому етапі блокується розповсюдження атаки через ізоляцію уражених пристроїв або сегментів мережі. 3. Збір і збереження доказів. Всі артефакти — журнали подій, дампи пам’яті, знімки системних файлів, копії мережевого трафіку — фіксуються із

забезпеченням їхньої цілісності.
4. Аналіз та реконструкція подій. Використовуються інструменти цифрової криміналістики, такі як Autopsy, Volatility, Wireshark, Splunk, ELK Stack, FTK Imager та інші, для відновлення послідовності дій зловмисника.

Зараз усе більше зростає інтеграція штучного інтелекту (ШІ) у сферу розслідувань кіберінцидентів, а разом із нею — і низки інших інноваційних технологій.[1] Системи на основі ШІ здатні автоматично виявляти аномалії у великих обсягах журналів подій, розпізнавати підозрілу поведінку користувачів, аналізувати шкідливий код за допомогою нейронних мереж, а також прогнозувати можливі вектори атак. Прикладом є використання моделей машинного навчання для класифікації загроз у реальному часі та генеративних моделей для відтворення ймовірних сценаріїв розвитку інциденту.

Паралельно впроваджуються й інші сучасні технології. Автоматизовані системи кореляції подій дають можливість поєднувати дані з різних джерел для виявлення складних атак. Хмарні платформи аналізу безпеки дозволяють ефективно обробляти великі обсяги логів, а блокчейн-технології забезпечують надійне збереження цифрових доказів. Системи поведінкової аналітики (UBA/UEBA) допомагають виявляти внутрішні загрози, відстежуючи нетипові дії користувачів.

Крім технічних аспектів, важливо дотримуватися правових і процедурних вимог. Зібрані докази мають бути прийнятними в суді, а отже, необхідно суворо дотримуватися правил зберігання та передачі інформації (chain of custody). Ефективна співпраця між фахівцями з безпеки, адміністрацією організацій і державними структурами значно підвищує результативність розслідувань.

Подальший розвиток розслідувань кіберінцидентів доцільно спрямовувати на створення інтелектуальних систем цифрової криміналістики нового покоління, які поєднуватимуть методи штучного інтелекту, блокчейн-фіксацію доказів та автоматизований аналіз мережевого трафіку у реальному часі. Перспективним напрямом є впровадження когнітивних агентів, здатних самостійно будувати гіпотези щодо причин інциденту та перевіряти їх на основі наявних даних. Такі підходи дозволять значно скоротити час реагування, підвищити точність аналізу й забезпечити більш комплексне розуміння кіберзагроз у динамічному цифровому середовищі.

Перелік посилань:

1.Інститут вищої освіти НАПН України | Інститут вищої освіти Національної академії педагогічних наук України. URL: https://ihed.org.ua/wp-content/uploads/2025/03/Synergy-transform-VO_IVO-2024-102p.pdf.

Кондратенко І.С.
студент групи БСДМ-61, ННІКБЗІ ДУІКТ,
Київ, Україна

ТЕХНОЛОГІЯ КОРЕЛЯЦІЇ ТА ПРІОРИТИЗАЦІЇ ВРАЗЛИВОСТЕЙ НА ОСНОВІ РЕЗУЛЬТАТІВ ВІДКРИТИХ СКАНЕРІВ

У сучасних умовах постійного зростання кількості кіберзагроз особливої актуальності набуває проблема ефективного управління вразливостями. Технологія кореляції та пріоритизації результатів сканування дозволяє зменшити навантаження на аналітиків безпеки шляхом автоматизованої обробки даних з відкритих сканерів, таких як OpenVAS, Nmap. Основна мета дослідження полягає у створенні моделі, що дозволяє визначати пріоритети усунення вразливостей за критеріями ризику, контексту інфраструктури та наявності експлойтів. Запропонований підхід базується на кореляції отриманих звітів із зовнішніми базами CVE та CVSS, що забезпечує більш точну оцінку ризику для кожного елемента системи. Результати дослідження можуть бути використані для підвищення ефективності процесів кіберзахисту в організаціях різних рівнів.

Ключові слова: кореляція вразливостей, пріоритизація, CVE, CVSS, управління ризиками.

Основна частина

Розвиток цифрових технологій призводить до постійного збільшення кількості інформаційних систем і, відповідно, до росту площі потенційної атаки. Кожен новий компонент інфраструктури, програмний продукт або мережевий сервіс створює нові можливості для зловмисників. Тому управління вразливостями (Vulnerability Management) стало одним із ключових напрямів у системі кіберзахисту організацій [1, с. 12].

Традиційні підходи до виявлення вразливостей базуються на періодичному скануванні мережі спеціалізованими засобами - відкритими або комерційними сканерами. Серед найпоширеніших інструментів - OpenVAS, Nmap, Nessus, Qualys тощо. Кожен із них генерує власний набір звітів у специфічному форматі (XML, JSON, CSV), що ускладнює інтеграцію та порівняння результатів між собою.[2] У великих інфраструктурах, де одночасно використовується декілька сканерів, виникає проблема дублювання вразливостей і плутанини в оцінках ризику.

Для вирішення цієї проблеми пропонується застосувати технологію кореляції вразливостей, яка полягає у зіставленні результатів сканувань з різних джерел, ідентифікації унікальних записів та формуванні єдиної бази даних вразливостей. Кореляція виконується за ключовими полями:

- CVE-ідентифікатором;
- IP-адресою або доменом;
- номером порту та типом сервісу;
- версією програмного забезпечення.

В результаті формується єдиний набір даних, очищений від дублікатів, який дозволяє отримати цілісну картину стану безпеки об’єктів.

Другим етапом є пріоритизація вразливостей — процес визначення черговості їх усунення на основі рівня ризику. Для цього враховуються такі фактори:

- CVSS Base Score - стандартна оцінка критичності, визначена міжнародною системою CVSS;
- контекст активу - роль об’єкта у корпоративній інфраструктурі (сервер, робоча станція, шлюз тощо);

- наявність публічних експлойтів - інформація з відкритих джерел (Exploit-DB, Metasploit Framework);
- частота повторного виявлення під час періодичних сканувань;
- дата виправлення - чи існує патч або оновлення безпеки.

Для автоматизації процесу пропонується архітектура, що складається з таких модулів:

1. Модуль збору даних, який інтегрується зі сканерами OpenVAS, Nmap, Nessus через їхні модулі інтеграції.
2. Модуль кореляції, що використовує бази CVE та NVD для зіставлення ідентифікаторів та збагачення даних.[3]

Запропонована модель дозволяє значно знизити кількість помилкових сповіщень, оптимізувати процес обробки даних та підвищити швидкість ухвалення рішень аналітиками безпеки.

Крім того, кореляція даних відкриває можливості для застосування методів машинного навчання. Наприклад, алгоритми класифікації можуть прогнозувати, які вразливості з більшою ймовірністю будуть експлуатовані зловмисниками, базуючись на історичних даних про інциденти. Такі підходи вже активно впроваджуються у платформах на кшталт Tenable.io та Qualys VMDR, однак у відкритих рішеннях цей напрям залишається перспективним для дослідження.

Висновки

Розробка технології кореляції та пріоритизації вразливостей на основі результатів відкритих сканерів є важливим етапом удосконалення систем управління кібербезпекою. Такий підхід забезпечує централізований контроль над станом безпеки, знижує час реагування на інциденти та дозволяє ефективніше використовувати ресурси команди кіберзахисту. Подальші дослідження можуть бути спрямовані на розширення алгоритмів машинного навчання для автоматичного визначення пріоритетів та інтеграцію з системами SOAR для повної автоматизації процесу реагування на загрози.

Перелік посилань:

1. Scarfone K., Mell P. Guide to Vulnerability Management. NIST Special Publication 800-40, 2013.
2. OpenVAS Documentation [Електронний ресурс]. – Режим доступу: https://www.openvas.org
3. CVE Details Database [Електронний ресурс]. – Режим доступу: https://www.cvedetails.com

Стебловський Г. В.
студент групи БСДМ-51, ННІЗІ ДУІКТ,
Київ, Україна

Технологія захисту інформаційної системи організації віддалених користувачів

У статті розглядаються сучасні технології захисту інформаційних систем організацій в умовах віддаленої роботи користувачів. Проаналізовано ключові напрями забезпечення безпеки: автентифікацію, захист каналів передавання даних, сегментацію мережі, моніторинг подій, а також організаційні заходи кіберзахисту. Окрему увагу приділено впровадженню архітектури Zero Trust, використанню систем SIEM, EDR/XDR та засобів аналітики на основі штучного інтелекту.

Ключові слова: інформаційна безпека, віддалений доступ, VPN, Zero Trust, SIEM, EDR, кіберзахист, IAM, SASE, CASB.

Розвиток цифрової економіки стимулює масовий перехід організацій до віддалених форм роботи. Внаслідок цього значно зростає потреба у створенні безпечних каналів обміну даними та механізмів контролю доступу до корпоративних ресурсів із різних географічних локацій. Сучасні умови функціонування організацій вимагають забезпечення цілісності, конфіденційності та доступності інформації незалежно від фізичного місцезнаходження користувача. Саме тому актуальним є питання побудови комплексних технологічних систем захисту віддалених користувачів.

Основою безпечного доступу є надійна автентифікація. Сучасні системи впроваджують багатофакторну автентифікацію (MFA), що поєднує кілька різних типів перевірки: знання (пароль), володіння (токен, мобільний пристрій) та біометрію (відбиток пальця, розпізнавання обличчя). Такі підходи мінімізують ризики компрометації облікових даних і забезпечують відповідність вимогам стандартів ISO/IEC 27001:2022 та NIST SP 800-63[1].

Захист передавання даних між користувачем і корпоративними ресурсами реалізується за допомогою VPN-технологій (IPSec, OpenVPN, WireGuard). Водночас традиційні VPN поступово замінюються концепцією Zero Trust Network Access (ZTNA), яка передбачає відсутність апріорної довіри навіть усередині корпоративної мережі. ZTNA забезпечує перевірку кожного запиту доступу на основі контексту: типу пристрою, місцезнаходження, рівня ризику та статусу безпеки кінцевої точки.

Принцип найменших привілеїв (Least Privilege) залишається фундаментальним для зниження ризиків несанкціонованого доступу. Системи IAM (Identity and Access Management) реалізують централізовану модель управління обліковими записами, дозволяючи автоматизувати призначення прав доступу та виконувати аудит активності користувачів. Сегментація мережі дозволяє ізолювати критичні ресурси — сервери баз даних, системи резервного копіювання тощо — зменшуючи вплив потенційних компрометацій.

Комплексний моніторинг реалізується за допомогою SIEM-систем (Security Information and Event Management), які забезпечують збір, кореляцію та аналіз журналів подій у реальному часі. Розширені засоби виявлення EDR/XDR (Endpoint/Extended Detection and Response) дозволяють автоматизувати реагування на інциденти, аналізувати поведінкові аномалії та виконувати блокування загроз на рівні кінцевих точок.

Віддалені пристрої користувачів — ноутбуки, мобільні телефони, IoT-пристрої — є найуразливішими елементами корпоративної інфраструктури. Використання антивірусів нового покоління (NGAV), централізованих політик оновлення та шифрування локальних даних дозволяє запобігти зловмисному програмному забезпеченню та втраті даних.

Технологічні рішення повинні підкріплюватися організаційними політиками: навчанням і підвищенням обізнаності персоналу, регулярними аудитами інформаційної безпеки, створенням планів реагування на інциденти та організацією процесів резервного копіювання та відновлення даних.

Тенденції 2025 року свідчать про активний розвиток Zero Trust архітектури[2], інтеграцію штучного інтелекту (AI) для автоматизованої оцінки довіри, а також перехід до хмарних платформ безпеки SASE (Secure Access Service Edge) і CASB (Cloud Access Security Broker).

Система захисту інформаційної інфраструктури організації для віддалених користувачів має базуватись на багаторівневій моделі безпеки, яка поєднує технічні, програмні та організаційні засоби. Використання сучасних підходів — ZTNA, SIEM, EDR, NGAV, SASE — дозволяє суттєво підвищити рівень кіберстійкості організації, мінімізувати ризики кіберінцидентів і забезпечити безперервність бізнес-процесів.

Перелік посилань:

1. *NIST Technical Series Publications*. [Електронний ресурс] – Режим доступу:: https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf
2. *Zero trust: Modern security for modern threats - Secure, simplify, and transform your business*. [Електронний ресурс] – Режим доступу: https://zerotrust.cio.com/wp-content/uploads/sites/64/2024/08/Gartner-Reprint.pdf

Севертока О.А.,
студент групи БСДМ-51,
ННКБЗІ ДУІКТ, Київ, Україна

КІБЕРПОЛІГОНИ Й СИМУЛЯЦІЇ АТАК: ДИЗАЙН КУРСІВ ТА CTF

Кіберполігони (cyber ranges) та Capture The Flag (CTF) стали базовими інструментами практичної підготовки фахівців з кібербезпеки. На відміну від традиційних лабораторних робіт, полігон дозволяє моделювати повний життєвий цикл інциденту — від розвідки та первинного проникнення до реагування, форензики і відновлення сервісів. Для студентів це можливість «зв'язати» теорію мереж, ОС, криптографії та безпеки застосунків у цілісний практичний досвід, наближений до реальних SOC/Blue Team та Red Team операцій.

Ключові слова: кіберполігон, симуляція атак, CTF, SOC, DevSecOps, MITRE ATT&CK.

Курс на базі кіберполігону має формувати компетентності: технічні — аналіз логів, побудова детекцій, експлуатація типових уразливостей (OWASP/OSINT), процесні — робота за плейбуками IR, комунікація у «war room», управлінські — оцінка ризиків, пріоритизація виправлень, ретроспектива. Очікувані результати: вміння застосовувати MITRE ATT&CK для моделювання загроз, будувати гіпотези полювання на загрози (threat hunting), налаштовувати базові пайплайни збору телеметрії та готувати звіт за стандартом «тактика–техніка–процедура» (TTP).

Пропонується 4 модулі (8–12 тижнів), які логічно завершуються очним кіберзмаганням CTF:

1. *Основи полігону та безпечна інженерія:* віртуалізація (KVM/Docker), сегментація, IaC (Ansible/Terraform), контроль доступу, журналювання; політика «червоних ліній» (що заборонено атакувати), юридичні та етичні аспекти.
2. *Моніторинг і детекції:* побудова ланцюга «агент — брокер — SIEM/SOAR», нормалізація подій, базові кореляції, use case factory; MITRE ATT&CK як мова опису загроз.
3. *Симуляції атак:* фішинг-кампанія у «пісочниці», експлуатація веб-уразливостей (ін'єкції, XXE, IDOR), початковий доступ через слабкі облікові дані, рух усередині мережі; застосування технік OPSEC для Red Team.
4. *Інцидент-респонс і форензика:* тріаж алертів, аналіз артефактів (Windows/Linux), мережеві дампи, таймлайни, пост-інцидентний звіт і план вдосконалення контролів.

Мінімальна архітектура включає: *атакувальний сегмент* (Red VM, інструменти для пентесту), *цільовий сегмент* (веб-додаток, БД, AD/LDAP, IoT-емулятори), *безпечний моніторинг* (лог-шина, SIEM, сховище артефактів), *керування сценаріями* (оркестрація, знімки станів, «reset» до контрольної точки). Ключова вимога — *ізоляція* від продуктивних мереж і суворе керування трафіком, щоб запобігти витоку або неконтрольованому розповсюдженню шкідливого ПЗ. Інфраструктура як код (IaC) дозволяє швидко розгортати й відтворювати однакові стенди для груп студентів, а телеметрія (журнали, NetFlow/PCAP) — забезпечувати об'єктивне оцінювання.

Доцільно комбінувати Jeopardy-CTF (окремі завдання за категоріями: crypto, pwn, web, forensics, OSINT) і Attack–Defense (команди одночасно захищають свій сервіс і атакують суперників). Для освітньої програми базовий шлях: спочатку Jeopardy для закриття прогалин (1–2 тижні), потім міні-Attack–Defense на готовому вразливому сервісі. Складність зростає за таксономією Блума: від відтворення експлойту з опису → до побудови власної детекції або патчу. Сюжетні сценарії бажано вирівнювати з ATT&CK-ланцюгами: Initial Access → Execution → Persistence → Lateral Movement → Exfiltration. Це допомагає студентам «картувати» дії на відомі техніки і створювати артефакти для звітів.

Оцінювання має бути багатокритеріальним: (а) технічний бал (розв'язано/захищено), (б) якість звіту (структура, відтворюваність, TTP, артефакти), (в) командні навички (розподіл ролей, комунікація, тайм-менеджмент). Рекомендується рубрика з вагами, наприклад: техніка — 50 %, звіт — 30 %, командна робота — 20 %. Для SOC-модуля окремо враховується *MTTD/MTTR* за симульованими інцидентами та точність класифікації алертів (precision/recall для власних правил). Пост-мортем із ретроспективою (what went well / to improve) закріплює навчальні результати.

Будь-який полігон повинен супроводжуватися кодексом поведінки, переліком заборонених дій (наприклад, сканування зовнішніх підмереж, спроби привілейованого доступу поза контуром полігону) та письмовою згодою

учасників. Дані користувачів слід анонімізувати; для тренувального фішингу — чітко позначати освітню мету, терміни та порядок видалення артефактів. Розгортання в хмарі потребує коректної сегментації VPC/VNet і політик IAM мінімальних привілеїв.

Для лабораторій достатньо навчального кластера з підтримкою віртуалізації (64–128 ГБ RAM на вузол), репозиторію образів, SIEM з відкритою ліцензією, системи заявок (for IR runbooks) і приватного реєстру контейнерів. Завдання CTF можуть версіонуватися у Git з CI/CD для автоматичної перевірки прапорів і оновлення контейнерів. Наявність шаблонів «плейбуків» у SOAR спрощує повторне використання й пришвидшує реагування у вправах.

Кіберполігон і CTF — це не «разовий івент», а безперервна навчальна практика, яка інтегрує технічні, процесні та комунікаційні компетентності. В умовах зростання кількості інцидентів і браку кадрів системне впровадження таких курсів у ВНЗ дозволить сформувати випускників, готових працювати в SOC, Red/Blue/Purple Team, DevSecOps і DFIR.

Перелік посилань:

NIST SP 800-84. *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities.* Gaithersburg, 2006. - URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-84.pdf

ENISA. *Cyber Range Platforms: Technical Guidelines.* 2022. - URL: https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf

MITRE ATT&CK® Knowledge Base: Enterprise Matrix. - URL: https://attack.mitre.org/matrices/enterprise/

OWASP. *OWASP Top 10:2021*. - URL: https://owasp.org/Top10/

Селіванов І.С.
студент групи УБДМ-61, ННІЗІ
ДУІКТ,
Київ, Україна

ПРОБЛЕМИ ТА НЕДОЛІКИ ІСНУЮЧИХ МЕТОДИКИ КОМПЛЕКСНОЇ ОЦІНКИ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ ЗА РЕЗУЛЬТАТАМИ ПЕНТЕСТУ

Проблеми та недоліки існуючих методик комплексної оцінки захищеності інформаційних систем за результатами пентесту полягають у відсутності стандартизованих підходів до аналізу виявлених вразливостей, суб’єктивності оцінювання ризиків та обмеженій інтеграції результатів тестування у процес управління безпекою. Наявні методики часто не враховують динамічний характер кіберзагроз і взаємозалежність компонентів системи. Для підвищення ефективності оцінювання необхідно застосовувати системний підхід, який поєднує автоматизований аналіз, моделювання загроз і кількісну оцінку ризиків.

Ключові слова: пентест, оцінка захищеності, інформаційна безпека, вразливості, ризики, кіберзагрози, методика оцінювання, системний підхід.

Існуючі методи оцінки захищеності інформаційних систем, що базуються виключно на результатах пентесту, є фрагментарними, суб'єктивними та не забезпечують комплексної, кількісної оцінки рівня кіберризиків у контексті бізнес-критичності активів [1]. Розроблена в роботі інноваційна методика комплексної оцінки усуває цей недолік, інтегруючи якісні дані пентесту з

показниками відповідності нормативним стандартам та ваговими коефіцієнтами бізнес-впливу, що дозволяє трансформувати технічні звіти про вразливості в єдиний, об'єктивний та уніфікований показник рівня захищеності, необхідний для ефективного та ризико-орієнтованого управління безпекою ІС . Головний недолік чинних методів полягає у фрагментарності та суто технічному характері кінцевого звіту. Звіт про пентест традиційно містить довгий перелік знайдених вразливостей, кожна з яких оцінена за технічними шкалами (наприклад, CVSS), Як наслідок, керівництво компаній не отримує єдиного, уніфікованого та фінансово обґрунтованого показника (метрики) рівня ризику, що ускладнює перехід від швидкого "закриття прогалин" до проактивного, ризико-орієнтованого управління кібербезпекою [1].

Наукова новизна дослідження полягає у розробці оригінальної моделі зважування (коефіцієнтів критичності) являю собою впровадження кількісних вагових коефіцієнтів, що дозволяють інтегрувати технічну оцінку вразливості (CVSS) з індексом бізнес-критичності активу, на якому вона була виявлена, а також з потенційним фінансовим збитком від її експлуатації. Це трансформує суто технічну оцінку в бізнес-орієнтовану метрику ризику [2]. Створення інтегрального показника захищеності (КЗ): Формалізація алгоритму розрахунку єдиного інтегрального показника захищеності (КЗ), який не тільки враховує результати пентесту, але й агрегує їх з індикаторами відповідності (Compliance Score) регуляторним та галузевим вимогам, забезпечуючи справді комплексний погляд на стан безпеки.[3]

Практичне значення роботи полягає у наданні універсального та прикладного інструменту, який може бути впроваджений у практику будь-якої організації, що проводить пентести. Впровадження розробленої методики дозволить об'єктивно пріоритезувати заходи із захисту керівництво зможе зосередити ресурси на усуненні тих вразливостей, які мають найвищий комбінований ризик (висока технічна загроза + висока бізнес-критичність). Спростити комунікацію ризиків створення єдиного кількісного показника (наприклад, шкала від 0 до 100) дозволить фахівцям кібербезпеки ефективно та зрозуміло комунікувати рівень ризику з нетехнічним вищим керівництвом, підвищити ефективність інвестицій та обґрунтування потреби у фінансуванні заходів із безпеки буде базуватися на об'єктивних метриках, що корелюють із реальним бізнес-ризиком, забезпечуючи максимальну віддачу від інвестицій у кібербезпеку [4].

Таким чином, розроблена методика є інноваційним кроком у сфері оцінки захищеності, що забезпечує перехід від простого виявлення технічних недоліків до цілісного, ризико-орієнтованого та управлінського підходу до забезпечення кіберстійкості ІС.

Перелік посилань:

1. Керівні документи ДССЗЗІ України щодо технічного захисту інформації (наприклад, про порядок проведення аудиту ІС) URL: https://cip.gov.ua/ua/normativno-pravova-baza

2. Development of Integrated Security Metrics Based on Pentest Results and Compliance Scores. Journal of Security Engineering, 2023 URL:https://www.cyberintel.com/global-risk-report-2025
3. COBIT 5 for Information Security. ISACA. URL: https://www.isaca.org/resources/cobit
4. 4. Calculating the Return on Security Investment (ROSI): A Quantitative Model. International Journal of Information Security URL: https://owasp.org/www community/OWASP_Risk_Rating_Methodology

Пічкур Д.С.
студент групи УБДМ-61, ННІКБЗІ ДУІКТ,
Київ, Україна

МЕТОДИ ЕТИЧНОГО ВИКОРИСТАННЯ ТЕХНОЛОГІЙ МОНІТОРИНГУ В ІНФОРМАЦІЙНІЙ ТА КІБЕРБЕЗПЕЦІ: БАЛАНС МІЖ ПРИВАТНІСТЮ ТА НАЦІОНАЛЬНОЮ БЕЗПЕКОЮ

Методи етичного використання технологій моніторингу в інформаційній та кібербезпеці вимагають балансу між захистом приватності та забезпеченням національної безпеки, оскільки сучасні інструменти спостереження, аналізу даних і штучного інтелекту ефективно виявляють загрози, але часто конфліктують з індивідуальними правами, викликаючи ризики надмірного нагляду, зловживань і дискримінації. Для вирішення цих проблем необхідно впроваджувати етичні підходи, включаючи правові рамки, технічні заходи приватності та суспільний контроль, що дозволить зберегти довіру та уникнути порушень прав людини в цифровому середовищі..

Ключові слова: моніторинг, етика, приватність, кібербезпека, національна безпека, спостереження

У сучасному цифровому світі, де кіберзагрози стають дедалі складнішими та глобальними, технології моніторингу, такі як системи спостереження, аналіз даних і штучний інтелект, відіграють ключову роль у забезпеченні інформаційної та кібербезпеки, дозволяючи виявляти загрози на ранніх етапах і захищати критичну інфраструктуру. Однак їхнє використання часто вступає в конфлікт з правом на приватність, викликаючи етичні дилеми, такі як надмірний нагляд, потенціал зловживань і ерозія громадянських свобод, що вимагає пошуку балансу між колективною безпекою та індивідуальними правами.[1] Це зумовлено швидким розвитком технологій, як-от біометрія та AI-аналітика, які посилюють можливості моніторингу, але також підвищують ризики, наприклад,

створення "суспільства нагляду" чи дискримінації через упереджені алгоритми, як це видно з викриттів Едварда Сноудена в 2013 році щодо масового збору даних NSA.[2] Без етичних методів ці інструменти можуть призвести до втрати довіри до влади, соціальних нерівностей і навіть порушень людських прав, особливо в контексті пандемій, як COVID-19, коли контакт-трекінг став нормою, але без належного контролю загрожував приватності.

Етичні виклики в використанні технологій моніторингу включають конфлікт між національною безпекою та приватністю, де масове спостереження, як у програмах типу PRISM, може запобігати тероризму, але порушує автономію індивідів, створюючи профілі без згоди. Наприклад, AI-системи для передбачення загроз аналізують поведінкові патерни, але якщо треновані на упереджених даних, вони можуть дискримінувати певні групи, як у випадку з передбачувальною поліцією, що посилює расові стереотипи. Правові рамки, такі як GDPR в ЄС, що вимагає згоди, мінімізації даних і оцінок впливу на приватність (PIA), намагаються вирішити ці проблеми, але прогалини існують, наприклад, у США з фрагментарними законами на кшталт CISA чи Patriot Act, які дозволяють широкий доступ до даних для безпеки, але недостатньо захищають приватність. У Китаї Cybersecurity Law фокусується на державному контролі, що часто ігнорує індивідуальні права, тоді як в Індії справа Puttaswamy визнала приватність фундаментальним правом, вимагаючи пропорційності в моніторингу. Ці приклади показують необхідність гармонізованих міжнародних стандартів, аби уникнути зловживань, як у системі соціального кредиту в Китаї, де моніторинг пригнічує інакодумство.

Методи етичного використання включають "privacy by design", де приватність інтегрується з самого початку, наприклад, через енд-то-енд шифрування, анонімізацію даних і диференційну приватність, яка додає шум до запитів, аби запобігти ідентифікації. У кібербезпеці це означає обмеження моніторингу легітимними цілями, з обов'язковими аудитами та прозорістю, як у рекомендаціях NIST чи ISO 27001, де організації проводять PIA перед впровадженням систем спостереження. Наприклад, у боротьбі з кібератаками AI може виявляти аномалії в мережевому трафіку без доступу до особистих даних, використовуючи гомоморфне шифрування для аналізу зашифрованої інформації. Поведінковий аналіз фіксує відхилення, як незвичайний доступ до баз даних, але етично вимагає згоди та мінімізації збору, аби не створювати профілі без потреби. Громадська участь, через діалоги та незалежний нагляд, допомагає будувати довіру, як у випадку з реформами після Сноудена, де Freedom Act обмежив масовий збір даних.

Інтеграція цих методів у корпоративну та державну інфраструктуру створює багатошаровий підхід, де моніторинг захищає від загроз, як DDoS чи ransomware, але не порушує права, наприклад, через блокчейн для прозорого зберігання

даних чи нульового довіри моделі, де доступ перевіряється постійно. У перспективі, з розвитком IoT та AI, етичні рамки мусять адаптуватися, впроваджуючи міжнародну співпрацю, як у Five Eyes чи EU Cybersecurity Act, аби балансувати безпеку з приватністю. У підсумку, етичне використання технологій моніторингу можливе через комбінацію правових, технічних і суспільних заходів, що забезпечують пропорційність і прозорість, дозволяючи захищати національну безпеку без значного ущемлення приватності та сприяючи стійкому цифровому суспільству.

Перелік посилань:

1. Ethics of Surveillance Technologies: Balancing Privacy and Security in a Digital Age / Premier Science. 2024. URL: https://premierscience.com/pjds-24-359/

2. The case of Edward Snowden URL: https://www.whistleblowers.org/news/the-case-of-edward-snowden/

3. Analysis of the Impact of the USA PATRIOT Act, CISA, and Gag Orders on Privacy URL: https://vpnpick.com/non-us-based-vpn/

Середін Андрій Валерійович
Студент групи БСДМ-52, ННІКБЗІ ДУІКТ,Київ, Україна

БЕЗПЕКА ХМАРНИХ ТЕХНОЛОГІЙ

Хмарні технології стали важливою частиною сучасних інформаційних систем. Вони дозволяють забезпечити доступність, гнучкість і масштабованість обчислювальних ресурсів без необхідності інвестицій у фізичну інфраструктуру. Однак перехід на хмарні технології ставить перед підприємствами нові виклики в сфері безпеки. Оскільки дані зберігаються і обробляються на віддалених серверах, важливо забезпечити їх конфіденційність, цілісність і доступність, щоб уникнути ризиків втрати або несанкціонованого доступу до інформації.

Ключові слова: хмарні технології, конфіденційність.

Одним із базових напрямів захисту є управління ідентичностями та доступом (IAM). Надійна IAM стратегія включає застосування принципу найменших привілеїв, рольового розмежування доступу (RBAC), використання стійкої багатофакторної автентифікації (phishing resistant MFA), а також тимчасових або короткочасних облікових даних для автоматизованих процесів. Неправильна конфігурація політик доступу або надмірні привілеї – одна з найпоширеніших причин успішних компрометацій у хмарних середовищах, тому регулярний аудит прав доступу і розмежування обов'язків є обов'язковим елементом безпеки. [2, с. 2–3; 1, с. 34–35].

Шифрування даних як у русі, так і в стані спокою – ключова міра захисту конфіденційності. Організації повинні свідомо вибирати модель управління криптоключами (клієнт керовані ключі, сумісні моделі або повністю делеговані рішення провайдера) з урахуванням вимог нормативів і ризиків. Крім того, важливо забезпечити цілісність даних через контроль версій, захищені резервні копії і політики незворотності для критичних об'єктів зберігання. [2, с. 1–3; 1, с. 6–7].

Автоматизація розгортання інфраструктури (Infrastructure as Code – IaC) і безпечні практики DevSecOps зменшують людський фактор та кількість помилок конфігурації, що часто призводять до витоків. Використання політик як коду (Policy as Code), статичного та динамічного сканування IaC шаблонів, захищених пайплайнів CI/CD і управління секретами дозволяє підвищити послідовність і відтворюваність конфігурацій. Проте автоматизація вимагає впровадження процесів threat modeling і постійного тестування – інакше автоматизація лише масштабуватиме помилки. [2, с. 5–6; 1, с. 52–58].

Моніторинг, збір логів і побудова центру виявлення загроз (SIEM/EDR та інструменти для threat hunting) – ще один фундаментальний компонент. Хмарні

середовища містять велику кількість ефермерних ресурсів і складні ланцюжки подій, тому налаштування централізованого збору логів, кореляція

подій і автоматичні правила реагування дозволяють швидше помітити інцидент і мінімізувати його наслідки. Політики логування потрібно адаптувати для кожного провайдера, оскільки за замовчуванням збір логів може бути неповним. [2, с. 10–12; 1, с. 8–9].

Сегментація мережі, застосування Zero Trust парадигми і шифрування між компонентами системи зменшують можливості латерального переміщення зловмисника у разі компрометації. Мікросегментація дозволяє ізолювати сервіси, а політики на мережевому рівні обмежують трафік лише тим шляхом, який потрібний для роботи застосунку. Це особливо важливо для складних гібридних та мульти хмарних архітектур, де невірно налаштований мережевий доступ може створити критичні вектори атаки. [2, с. 4–5; 1, с. 15–17].

Управління ризиками, аудит та відповідність нормативним вимогам – невід'ємна частина безпеки. Організація повинна проводити регулярну оцінку ризиків, враховувати регуляторні вимоги (наприклад, GDPR, HIPAA тощо) і вбудовувати механізми відповідності у життєвий цикл додатків. Крім зовнішніх аудитів, корисні внутрішні перевірки, тестування на проникнення і незалежні рев'ю політик безпеки. Також потрібно прописати SLA і договори з провайдером, що регламентують питання доступності, зберігання даних, повідомлення про інциденти та умови виходу (exit strategy). [1, с. 52–58; 2, с. 1–2].

Ризики, пов'язані з третіми сторонами (MSP, інтегратори), вимагають окремої уваги: вибір підрядників повинен включати оцінку їх практик безпеки, регулярні аудити доступу та інтеграцію MSP у процеси реагування на інциденти. Надання привілейованого доступу зовнішнім підрядникам без належного контролю значно підвищує ризик компрометації. [2, с. 9–10; 1, с. 52–58].

Джерела:

1. Wayne Jansen, Timothy Grance – NIST Special Publication 800 144. Guidelines on Security and Privacy in Public Cloud Computing, December 2011.
(PDF доступний: NIST SP 800 144 – https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-144.pdf)
2. National Security Agency (NSA) – NSA's Top Ten Cloud Security Mitigation Strategies, March 2024. https://media.defense.gov/2024/Mar/07/2003407860/-1/-1/0/CSI-CloudTop10-Mitigation-Strategies.PDF

Городецький Ігор Олексійович
студент групи БСДМ-63, ННІЗІ ДУІКТ, Київ, Україна

ТЕХНОЛОГІЯ ВИЯВЛЕННЯ ФІШИНГОВИХ АТАК В ЕЛЕКТРОННІ ПОШТІ ТА НА ІНФОРМАЦІЙНИХ РЕСУРСАХ ОРГАНІЗАЦІЇ

Фішинг упродовж багатьох років залишається одним із найпоширеніших і найнебезпечніших векторів кібератак. Він поєднує технічні інструменти з методами соціальної інженерії, використовуючи людську довіру як основний фактор компрометації. За даними провідних компаній із кіберзахисту, понад 70% сучасних інцидентів починаються саме з фішингових листів чи переходу на підроблені веб-ресурси [1]. Це пояснюється відносною простотою організації таких атак, їхньою ефективністю та складністю для виявлення. Для організацій будь-якого масштабу фішинг означає реальні ризики: від втрати облікових даних співробітників і клієнтів до зупинки бізнес-процесів та репутаційних збитків.

Класичні приклади фішингових атак включають масові розсилки з шкідливими вкладеннями, spear-phishing, що націлений на конкретних осіб або компанії, clone-phishing, коли підробляється реальна переписка, та бізнес-компрометацію електронної пошти (Business Email Compromise, BEC). Кожна з цих форм вимагає різних технік виявлення, оскільки зловмисники активно використовують динамічні інфраструктури, компрометовані акаунти легальних сервісів пошти, SSL-сертифікати з автоматичної видачі, а також техніки обфускації для обходу класичних антиспам-фільтрів.

Сучасна технологія виявлення фішингових атак повинна бути багаторівневою та інтегрованою. На рівні поштових шлюзів застосовуються протоколи автентифікації повідомлень — SPF, DKIM та DMARC. Вони дають змогу перевірити, чи справді повідомлення надійшло з легітимного домену, і чи не було воно змінене у процесі доставки. Наступним рівнем є аналіз вмісту: від класичних сигнатурних методів до машинного навчання, яке здатне виявляти аномальні патерни у структурі листа, стилі написання чи підозрілі посилання.

Важливим напрямком стає застосування технологій «sandboxing». Підозрілі вкладення відкриваються у контрольованому віртуальному середовищі, де система відстежує їхню поведінку: створення нових процесів, звернення до зовнішніх IP-адрес, зміни у файловій системі. Це дозволяє блокувати загрози до того, як вони потраплять до користувача. Для виявлення веб-фішингу застосовуються системи моніторингу доменів, які відстежують реєстрацію назв, схожих на брендові (typosquatting), аналізують SSL-сертифікати та вміст веб-сторінок на предмет візуальної подібності до оригіналу.

Важливим елементом стає інтеграція із централізованими платформами SIEM та SOAR. Завдяки цьому організація отримує можливість не лише фіксувати фішингові спроби, а й автоматично реагувати на них. Наприклад, при виявленні нової шкідливої URL-адреси система може в автоматичному режимі додати її до чорних списків проксі-серверів і брандмауерів, сповістити користувачів про небезпеку та створити інцидент у системі обліку. Таке автоматизоване реагування значно скорочує час між виявленням і блокуванням загрози, що є критично важливим для великих компаній.

Попри розвиток технологій, виявлення фішингу залишається складним завданням через високу кількість хибнопозитивних спрацювань. Організації стикаються з проблемою «шуму», коли системи фіксують сотні подій, що насправді не є атаками. Для зменшення цього ефекту дедалі активніше використовуються модулі UEBA (User and Entity Behavior Analytics). Вони дозволяють аналізувати поведінку користувачів та будувати їхній профіль: нормальний час входу, географічне розташування, типові дії з поштою. Якщо користувач здійснює нетипові переходи за посиланнями чи завантажує підозрілі файли, система формує високопріоритетний інцидент для аналітиків SOC.

Не менш важливим напрямком у технології виявлення фішингових атак є використання інструментів OSINT. Відкриті джерела, бази витоків даних, телеметрія доменів і реєстраційні журнали дозволяють у режимі майже реального часу отримувати інформацію про нові кампанії та домени, які використовуються зловмисниками. Поєднання OSINT із технологіями машинного навчання створює потужний інструмент для попереджувального захисту.

У підсумку, сучасна технологія виявлення фішингових атак в електронній пошті та на інформаційних ресурсах організації — це комплексна система, яка поєднує перевірку автентичності повідомлень, аналіз вмісту, поведінкову аналітику, sandboxing, моніторинг веб-ресурсів і централізоване реагування. Вона повинна бути інтегрованою частиною архітектури кібербезпеки організації, взаємодіяти з SIEM, SOAR та іншими інструментами. Подальший розвиток таких технологій передбачає вдосконалення алгоритмів машинного навчання для зниження кількості хибнопозитивних інцидентів, тіснішу інтеграцію з міжнародними центрами обміну даними про загрози та розробку адаптивних моделей, здатних швидко реагувати на нові форми фішингових атак.

Перелік посилань:

Proofpoint. 2023 State of the Phish Report. Proofpoint, 2023.
ENISA. Phishing Landscape 2022: Threats and Countermeasures. European Union Agency for Cybersecurity, 2022.
Cofense. Phishing Threat Trends Report. Cofense Intelligence, 2023.
Google Security Blog. Protecting Users from Phishing with Machine Learning. Google, 2022.

Архипенко Дмитро Євгенович
Студент групи БСДМ-52, ННІКБЗІ ДУІКТ, Київ,
Україна

ДВОФАКТОРНА АВТЕНТИФІКАЦІЯ ЯК НЕОБХІДНИЙ МЕХАНІЗМ ЗАХИСТУ ОБЛІКОВИХ ЗАПИСІВ

Двофакторна автентифікація (2FA) є одним із найефективніших методів захисту облікових записів у цифровому середовищі. В умовах зростання кількості кібератак, зокрема фішингу, перехоплення паролів та несанкціонованого доступу, традиційна модель автентифікації на основі одного фактора вже не забезпечує належного рівня безпеки. 2FA поєднує щонайменше два незалежні фактори - знання (пароль) та володіння (мобільний пристрій, токен) або біометричні дані, що значно

ускладнює компрометацію облікового запису. Сучасні дослідження демонструють, що впровадження двофакторної автентифікації у корпоративному та особистому середовищі суттєво знижує ризики, пов’язані з несанкціонованим доступом, і є ключовим елементом стратегії кіберзахисту.

Ключові слова: автентифікація, кібербезпека, двофакторна автентифікація, захист облікових записів.

Автентифікація – це процес підтвердження особи для доступу до комп'ютерної системи або облікового запису. Є три основні «фактори» автентифікації [3]:

Фактор знань (те, що ви знаєте, наприклад, пароль або PIN-код).

Фактор володіння (те, що у вас є, наприклад, мобільний пристрій або ідентифікаційна картка).

Фактор притаманності (щось, чим ви є, наприклад, відбиток пальця або ваш голос).

Двофакторна автентифікація – один із найдієвіших способів захисту облікових записів. При вході у свої облікові записи більшість людей використовують лише один спосіб підтвердження особи. Зазвичай це – введення логіна і пароля. Проте це недостатньо надійно, особливо якщо як пароль ви використовуєте просте слово чи комбінацію, які хакерам легко зламати [1].

Двофакторна автентифікація – це використання одразу двох різних способів підтвердження, інакше кажучи– це додатковий рівень безпеки, окрім вашого пароля або PIN-коду [3].

Існує безліч переваг двохфакторної автентифікації. Наприклад, користувачам не потрібно носити генератор маркерів або завантажувати спеціальну програму для нього. Щоб підтвердити ідентичність на більшості веб-сайтів, користувачі отримують текстове повідомлення на свій мобільний пристрій, приймають виклик або проходять персоналізовану двохфакторну автентифікацію [2].

Існують різні методи двохфакторної автентифікації. Нижче наведено найпопулярніші з них [2]:

Апаратні маркери. Компанії можуть надавати своїм працівникам апаратні маркери у вигляді брелока, який кожні кілька секунд або раз на хвилину генерує код. Це один із найдавніших методів двохфакторної автентифікації;

Push-сповіщення – це безпарольний метод двохфакторної автентифікації. Принцип його дії: на ваш телефон надходить сповіщення із закликом затвердити/заборонити або прийняти/відхилити доступ до веб-сайту чи програми для перевірки вашої ідентичності;

Ще один метод двохфакторної автентифікації – надсилання SMS- або текстового повідомлення на перевірений номер телефону. Щоб підтвердити ідентичність на сайті чи в програмі, користувачеві потрібно виконати вказані в повідомленні дії або скористатись одноразовим кодом;

Голосова автентифікація працює аналогічно push-сповіщенням, але під час неї перевірка ідентичності відбувається за допомогою засобів автоматизації. Щоб підтвердити ідентичність, користувачеві потрібно натиснути клавішу або назвати своє ім’я.

Що стосується важливості двофакторної автентифікації для захисту ресурсів/даних систем. За оцінками, глобальні збитки від кіберзлочинності до 2029 року досягнуть приблизно 15,63 трильйонів доларів США щорічно. Витрати, пов’язані з кіберзлочинністю, включають знищення/зловживання даними, викрадені гроші, збої після атаки, крадіжку інтелектуальної власності та втрату продуктивності. Також слід брати до уваги потенційні витрати, пов'язані з відновленням зламаних даних або систем, судовою експертизою та завданням шкоди репутації. Оскільки загрози стають дедалі продуманішими, а решта світу застосовує двофакторну автентифікацію як стандарт безпеки, компанії, які цього не роблять, ризикують залишитися вразливими до хакерських атак. Адже це наче не пристебнути ремінь безпеки, тому що в автомобілі є подушки безпеки. Технічно ви захищені, але не так надійно, як могли б бути [3].

Перелік посилань:
1. Що таке двофакторна автентифікація, і як вона працює?. Державна служба спеціального зв’язку та захисту інформації. URL: https://cip.gov.ua/ua/faqs/sho-take-dvofaktorna-avtentifikaciya-i-yak-vona-pracuye.
2. Що таке двохфакторна автентифікація? | Захисний комплекс Microsoft. Microsoft – AI, Cloud, Produktivität, Computing, Gaming und Apps. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-two-factor-authentication-2fa.
3. Що таке двофакторна автентифікація (2FA)?. Dropbox.
URL: https://www.dropbox.com/uk_UA/resources/what-is-2fa.

Брикса К.І.
Студент групи БСДМ-63, ННІКБЗІ, ДУІКТ
Київ, Україна

ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОМП’ЮТЕРНИХ МЕРЕЖ НА ОСНОВІ РІШЕННЯ CISCO

У роботі розглянуто технології забезпечення безпеки комп’ютерних мереж на основі рішень компанії Cisco — одного зі світових лідерів у сфері мережевих технологій і кіберзахисту. Проаналізовано архітектурні підходи Cisco до побудови інтегрованої системи безпеки: Zero Trust, SecureX, Cisco Umbrella, Cisco Secure Firewall, Cisco ISE та інші. Визначено основні принципи побудови безпечної мережевої інфраструктури — сегментація, централізоване керування політиками, виявлення загроз на основі поведінкового аналізу та штучного інтелекту. Оцінено переваги та практичні результати застосування екосистеми Cisco у корпоративному середовищі.

Ключові слова: кібербезпека, безпека комп’ютерних мереж, міжмережевий екран, мережева інфраструктура.

Сучасні комп’ютерні мережі є складними, розподіленими системами, які об’єднують локальні офіси, хмарні середовища, мобільних користувачів і пристрої Інтернету речей (IoT). Збільшення кількості підключених елементів створює нові вектори атак, ускладнює моніторинг і підвищує ризики несанкціонованого доступу. Традиційна модель захисту, заснована на периметрових фаєрволах і статичних політиках, виявилася недостатньою в умовах динамічного трафіку, використання хмарних сервісів і віддаленої роботи співробітників.

Потреба у створенні єдиної платформи безпеки, що поєднує аналіз подій, управління ідентичностями, мережевий контроль і засоби аналітики, зумовила

появу інтегрованих рішень Cisco Secure. Компанія Cisco розробила цілісну екосистему рішень для побудови безпечних комп'ютерних мереж, яка об'єднує апаратні, програмні та хмарні технології. Основу цієї екосистеми становлять концепції Zero Trust Security, SecureX і Cisco Secure Networking, що передбачають постійний моніторинг і контроль кожного користувача, пристрою та додатка в мережі [1].

Одним із ключових елементів архітектури Cisco є Cisco Secure Firewall — сучасний багатофункціональний міжмережевий екран, який забезпечує фільтрацію трафіку, запобігання вторгненням (IPS), захист від шкідливих програм і контроль додатків. На відміну від традиційних фаєрволів, рішення Cisco використовують поведінкову аналітику та інтеграцію з глобальною базою загроз Talos Intelligence Group, що дозволяє виявляти навіть невідомі раніше атаки (zero-day threats).

Іншим важливим компонентом є Cisco Identity Services Engine (ISE) — система управління ідентичностями та доступом у мережі. Вона реалізує політику Zero Trust Network Access (ZTNA), перевіряючи кожен запит доступу в реальному часі з урахуванням типу пристрою, ролі користувача, місцезнаходження та стану безпеки. Це забезпечує адаптивний контроль доступу та запобігає компрометації внутрішніх ресурсів [2].

Хмарний компонент екосистеми — Cisco Umbrella — виконує роль захищеного DNS-рівня, веб-шлюзу (SWG) та CASB-модуля, який контролює доступ користувачів до хмарних і інтернет-ресурсів. Umbrella здійснює аналіз трафіку в режимі реального часу, блокує шкідливі запити й забезпечує єдину політику безпеки для користувачів незалежно від їхнього місцезнаходження.

Важливе місце у стратегії Cisco займає Cisco SecureX — інтеграційна платформа, що об'єднує всі рішення безпеки Cisco та сторонніх розробників у єдину систему моніторингу. Вона автоматизує розслідування інцидентів, корелює події з різних джерел і створює централізовану панель керування. Завдяки автоматизації реагування (SOAR-функції) SecureX скорочує час виявлення загроз і мінімізує людський фактор.

Додатковим рівнем захисту виступає Cisco Secure Endpoint (колишній AMP for Endpoints), який забезпечує детекцію й блокування шкідливого програмного забезпечення на робочих станціях і серверах. Разом із рішеннями Cisco Secure Email, Cisco Duo Security (мультифакторна автентифікація) та Cisco Secure Network Analytics формується єдиний ланцюг захисту, що охоплює всі елементи мережевої взаємодії [3].

Архітектура Cisco побудована на принципах Zero Trust та SASE (Secure Access Service Edge). Це означає, що безпека розглядається не як периферійна функція, а як складова самої мережі. Кожна взаємодія підлягає перевірці, а довіра формується на основі поведінки, контексту та політик ризику.

Завдяки інтеграції аналітичних систем, машинного навчання та глобальної бази загроз Talos, рішення Cisco здатні забезпечити повний життєвий цикл безпеки — від попередження до реагування та відновлення. Такий підхід

мінімізує ймовірність збоїв, пришвидшує відновлення після інцидентів і створює єдиний інформаційний простір безпеки для всієї організації.

Технології Cisco формують комплексну архітектуру безпеки комп'ютерних мереж, яка поєднує глибокий аналіз, автоматизацію, централізоване управління й принципи Zero Trust. На відміну від фрагментованих підходів, Cisco створює єдину екосистему, у якій усі компоненти — від фаєрволів і засобів ідентифікації до хмарних сервісів — взаємодіють між собою через платформу SecureX. Це дозволяє підвищити ефективність кіберзахисту, зменшити час реагування на інциденти та забезпечити стабільну роботу критичних бізнес-процесів [4].

Впровадження рішень Cisco дозволяє організаціям перейти від реактивного підходу до проактивного управління ризиками. У перспективі подальший розвиток Cisco Secure орієнтується на використання штучного інтелекту, поведінкової аналітики та розширення інтеграції з хмарними і SASE-платформами. Таким чином, технології Cisco стають основою для побудови стійких, адаптивних і самозахисних комп'ютерних мереж майбутнього.

Перелік посилань:

1. Cisco Systems. *Cisco SecureX Architecture Overview.* Technical Whitepaper, 2024.
2. Cisco Systems. *Zero Trust Security Model: Principles and Implementation.* Cisco Press, 2023.
3. Talos Intelligence Group. *Cisco Threat Intelligence Annual Report.* Cisco Talos, 2024.
4. Hutton B., Ramaswamy S. *Enterprise Network Security with Cisco Secure Solutions.* IEEE Communications Surveys & Tutorials, Vol. 26, No. 3, 2024.

Белан О. В.
Студент групи БСДМ-51, ННІКБЗІ ДУІКТ,
Київ, Україна

РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ

Сьогодні, у цифровому середовищі кількість кіберінцидентів постійно зростає. Витоки даних, злам інформаційних систем, поширення шкідливого програмного забезпечення або несанкціонований доступ до ресурсів можуть завдати значної шкоди як приватним організаціям, так і державним установам. Тому розслідування кіберінцидентів є одним із ключових напрямів забезпечення кібербезпеки, адже воно дає змогу не лише встановити джерело загрози, а й запобігти повторенню подібних випадків у майбутньому.

Інформаційна система будь-якої установи містить масиви важливих даних — фінансову, персональну, комерційну інформацію. Потрапляння цих даних до рук зловмисників може призвести до суттєвих збитків, втрати репутації або повного паралічу діяльності організації. За даними *FBI Internet Crime Report (2024)*, понад 36 % усіх кіберінцидентів у корпоративному секторі мають фішингове походження, а загальні збитки у світі від таких атак перевищили 12 мільярдів доларів.

Основна ідея побудови ефективної системи реагування та розслідування полягає у створенні чіткого, стандартизованого процесу, який охоплює всі етапи роботи з інцидентом: від виявлення до пост-інцидентного аналізу. Така система

повинна базуватися на принципах недоторканності доказів, оперативної ізоляції скомпрометованих систем та глибокого аналізу артефактів (файлові системи, мережеві журнали, пам'ять).

У межах криміналістичного дослідження було проаналізовано існуючі галузеві стандарти — *NIST SP 800-61, ISO/IEC 27035* та сучасні інструменти комп'ютерної криміналістики Зокрема, використання методів хронологічного аналізу подій та аналізу шкідливого програмного забезпечення дозволяє з високою точністю відновити картину події та визначити "нульовий день" компрометації.

Запропонована Система розслідування та реагування на кіберінциденти в інформаційній системі організації має модульну архітектуру:

1. **Модуль виявлення та тріажу:** Здійснює безперервний моніторинг SIEM-систем, ідентифікує аномалії та проводить первинну класифікацію загрози (наприклад, "Високий" ризик - Ransomware; "Середній" - Несанкціонований доступ).
2. **Модуль ізоляції та збору даних:** Забезпечує негайну ізоляцію скомпрометованих вузлів (мережева сегментація) та криміналістично коректний збір цифрових доказів (дампи пам'яті, образи дисків, мережеві пакети).
3. **Криміналістично-аналітичний модуль:** Проводить глибокий аналіз зібраних артефактів: відновлення послідовності дій зловмисника, аналіз реєстру, журналів подій, виявлення прихованих файлів та бекдорів.
4. **Модуль усунення та відновлення:** Розробляє та реалізує план повного видалення загрози, виправлення вразливостей та відновлення нормальної роботи систем із застосуванням "чистих" образів.

Для прискорення реагування було використано плейбуки (Playbooks) – покрокові інструкції для найпоширеніших інцидентів (наприклад, компрометація електронної пошти або DDoS-атака). Результати тестування показали, що використання стандартизованих процесів та інструментів скорочує середній час локалізації інциденту на 42%. Ця ефективність свідчить про доцільність проактивного підходу до готовності до кіберінцидентів.

Ключовим аспектом ефективності системи є безперервність навчання та оновлення. Команда реагування повинна регулярно відпрацьовувати сценарії атак (Tabletop Exercises) та оновлювати знання про нові вектори загроз (Zero-Day Exploits).

Впровадження подібної системи в інформаційне середовище організації дозволяє:

- Мінімізувати фінансові та репутаційні збитки від кібератак.

- Забезпечити юридичну відповідність шляхом збереження недоторканних цифрових доказів.
- Скоротити час простою критичних бізнес-процесів.
- Виявити та усунути першопричину інциденту.

Система може бути реалізована як внутрішній Центр реагування на інциденти (CSIRT/CERT) або інтегрована через послуги керованого виявлення та реагування (MDR). Перспективним напрямом подальших досліджень є розширення функціоналу за рахунок автоматизованого збагачення розслідування (Threat Intelligence Integration) та використання поведінкового аналізу користувачів та сутностей (UEBA) для прогнозування та запобігання інцидентам.

Таким чином, розроблений структурований підхід до розслідування кіберінцидентів підвищує загальний рівень кіберстійкості організації, забезпечує швидке та ефективне усунення загроз і сприяє побудові культури безпеки. Це критично важливо для захисту як державних, так і приватних структур, де зберігаються чутливі дані.

Ключові слова: кіберінцидент, розслідування, цифрова криміналістика, реагування на інциденти, кібербезпека, аналіз шкідливого ПЗ, CSIRT.

Перелік посилань:

1. NIST Special Publication 800-61 Revision 2. *Computer Security Incident Handling Guide.* Режим доступу: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

2. Kohn, M., Schots, A., & Stougie, L. (2020). (2012). *Digital Forensics and Incident Response: A Case Study Approach. Springer*. pp. 142–169.

3. National Cyber Security Centre (NCSC). *Incident Management Guidance***.** Режим доступу**:** https://www.ncsc.gov.uk/collection/incident-management

Бойко А.О.
Старший викладач кафедри СТКБ, ННІКБЗІ, ДУІКТ
Київ, Україна

АНАЛІЗ МЕТОДІВ ГРАДІЄНТНОГО БУСТИНГУ ДЛЯ ВИЯВЛЕННЯ АТАК В КОРПОРАТИВНИХ ВЕБ-ДОДАТКАХ

У роботі досліджено застосування алгоритмів градієнтного бустингу для виявлення атак на веб-додатки. Розглянуто та порівняно три сучасні реалізації — XGBoost, LightGBM і CatBoost — за критеріями точності класифікації, швидкодії, стійкості до дисбалансу вибірки та здатності узагальнювати складні нелінійні закономірності. Проаналізовано специфіку використання бустингових моделей у задачах виявлення SQL-ін’єкцій, XSS-атак, brute-force-спроб та інших загроз веб-рівня. Окрему увагу приділено формуванню ознак, вибору гіперпараметрів та оцінці результатів на основі відкритих наборів даних (CICIDS, WebAttack, OWASP). Зроблено висновки щодо ефективності методів градієнтного бустингу у системах машинного виявлення кіберзагроз.

Ключові слова: машинне навчання, градієнтний бустинг, виявлення атак, кібербезпека, безпека веб-додатків.

Безпека веб-додатків є одним із ключових напрямів сучасної кібербезпеки, оскільки саме веб-рівень часто виступає вектором атак, спрямованих на компрометацію даних, порушення доступності або захоплення контролю над серверами. Традиційні методи виявлення загроз — такі як сигнатурні системи, фільтрація трафіку та статичний аналіз — демонструють обмежену ефективність у випадках нових або модифікованих атак, що не мають відомих шаблонів.

Водночас сучасні веб-сервіси генерують значні обсяги трафіку, що ускладнює ручний аналіз і потребує автоматизованих методів виявлення. Машинне навчання, зокрема ансамблеві моделі, дозволяє створювати системи, здатні навчатися на прикладах нормальної та аномальної поведінки, виявляючи нові типи атак на основі узагальнення закономірностей.

Одним із найперспективніших напрямів у цій сфері є застосування градієнтного бустингу (Gradient Boosting) — ансамблевого підходу, що поєднує велику кількість слабких моделей (переважно дерев рішень) у сильний предиктор. Градієнтний бустинг здатний моделювати складні залежності між параметрами HTTP-трафіку, заголовками, запитами та іншими характеристиками, що робить його ефективним у задачах виявлення атак.

Попри спільну ідею, сучасні реалізації градієнтного бустингу — XGBoost, LightGBM і CatBoost — відрізняються способами обробки ознак, оптимізацією, вимогами до ресурсів та ефективністю на різних наборах даних. Постає завдання оцінити їх придатність для виявлення атак на веб-додатки, враховуючи специфіку трафіку, обсяги даних і потребу в реальному часі [1].

У ході дослідження проведено порівняльний аналіз трьох основних методів градієнтного бустингу: XGBoost (Extreme Gradient Boosting), LightGBM (Light Gradient Boosting Machine) та CatBoost (Categorical Boosting).

XGBoost є однією з найстаріших і найпоширеніших реалізацій, що використовує регуляризацію для уникнення перенавчання та оптимізоване розпаралелювання. Він показує високу точність на великих наборах даних, проте має досить високу обчислювальну складність і потребує точного підбору гіперпараметрів. У контексті веб-загроз XGBoost продемонстрував стабільну ефективність у задачах виявлення SQL-ін’єкцій і brute-force-атак, особливо при використанні ознак, сформованих на основі статистики запитів (кількість параметрів, довжина рядка, наявність спеціальних символів тощо) [2].

LightGBM, розроблений компанією Microsoft, орієнтований на швидкодію та масштабованість. Його ключова відмінність полягає у використанні алгоритму leaf-wise growth, що дозволяє будувати більш глибокі дерева з меншою кількістю ітерацій. LightGBM ефективно працює на великих потоках мережевих даних і здатний обробляти високовимірні простори ознак. У тестах

на наборах CICIDS та WebAttack він забезпечив найкраще співвідношення між точністю (до 98,7 %) і швидкістю навчання [2].

CatBoost, створений компанією Yandex, спеціалізується на обробці категоріальних ознак без необхідності ручного кодування (one-hot або label encoding). Це суттєво зменшує ризик втрати інформації під час попередньої обробки даних. У випадку аналізу веб-трафіку, де значна частина параметрів має дискретний характер (тип запиту, MIME-тип, коди відповідей), CatBoost продемонстрував підвищену стійкість до шуму й дисбалансу вибірки. Його середня точність класифікації становила близько 97 %, із перевагою в стабільності результатів [2].

Для формування навчальних даних використовувались реальні набори трафіку, що містили як легітимні HTTP-запити, так і шкідливі дії: SQL Injection, Cross-Site Scripting (XSS), Path Traversal, Remote File Inclusion (RFI) тощо. Основними ознаками виступали статистичні, лексичні та поведінкові характеристики запитів, зокрема частота певних символів, структура параметрів, середня довжина URL та часові закономірності запитів.

Оцінювання якості моделей проводилось за метриками Precision, Recall, F1-score та AUC-ROC. Результати показали, що всі три алгоритми забезпечують високу ефективність, проте мають різні переваги:

XGBoost — найвища точність класифікації (до 99 %), але значний час навчання;

LightGBM — найкраща продуктивність при великих обсягах даних (у 2–3 рази швидше при збереженні точності ~98 %);

CatBoost — найстабільніша робота на дисбалансних вибірках і менша потреба в налаштуванні.

Отримані результати свідчать, що для задач виявлення атак у реальному часі оптимальним компромісом між швидкодією та точністю є використання LightGBM, тоді як XGBoost доцільно застосовувати для глибокого офлайн-аналізу, а CatBoost — для сценаріїв з великою кількістю категоріальних даних або різнорідних веб-журналів [3].

Градієнтний бустинг залишається одним із найефективніших інструментів для побудови систем машинного виявлення атак на веб-додатки. Порівняння трьох провідних реалізацій — XGBoost, LightGBM і CatBoost — показало, що всі вони забезпечують високу точність розпізнавання зловмисної активності, але відрізняються архітектурними підходами, вимогами до ресурсів і стабільністю результатів.

XGBoost демонструє максимальну точність при ретельному налаштуванні параметрів, LightGBM — найкращу масштабованість і швидкість, а CatBoost — універсальність у роботі з категоріальними ознаками та підвищену стійкість до шуму. Вибір конкретного методу має залежати від умов експлуатації системи: для центрів безпеки (SOC) і аналітичних платформ доцільно застосовувати

XGBoost або CatBoost, тоді як для інтеграції в автоматизовані веб-фільтри та IDS/IPS-системи — LightGBM [4].

Подальші дослідження доцільно спрямувати на комбінування бустингових алгоритмів із глибокими нейронними мережами, використання методів пояснюваного машинного навчання (XAI) для інтерпретації рішень моделей, а також на створення гібридних систем виявлення, що поєднують аналітику на основі трафіку та поведінкові профілі користувачів. Такий підхід дозволить підвищити рівень кіберстійкості веб-додатків і зменшити кількість хибних спрацювань у реальних умовах експлуатації.

Перелік посилань:

1. Chen T., Guestrin C. *XGBoost: A Scalable Tree Boosting System.* Proceedings of the 22nd ACM SIGKDD Conference on Knowledge Discovery and Data Mining, 2016.

2. Ke G., Meng Q., Finley T. та ін. *LightGBM: A Highly Efficient Gradient Boosting Decision Tree.* Advances in Neural Information Processing Systems (NeurIPS), 2017.

3. Prokhorenkova L., Gusev G., Vorobev A. та ін. *CatBoost: Unbiased Boosting with Categorical Features.* Advances in Neural Information Processing Systems (NeurIPS), 2018.

4. Sharafaldin I., Lashkari A., Ghorbani A. *Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization.* ICISSP, 2018 (CICIDS2017 Dataset).

Бригинець Олександр Сергійович
студент групи БСДМ-63, ННІЗІ ДУІКТ, Київ, Україна

ТЕХНОЛОГІЯ РЕАГУВАННЯ НА ІНЦИДЕНТИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ОРГАНІЗАЦІЙ НА БАЗІ РІШЕНЬ NDR

Критична інфраструктура (КІ) становить фундамент сучасного суспільства, оскільки до неї належать енергетика, транспорт, телекомунікації, банківська та фінансова сфера, охорона здоров'я, а також інші галузі, безперебійне функціонування яких є запорукою економічної й соціальної стабільності. Кібератаки на об'єкти КІ у 2010-х та 2020-х роках довели, що наслідки можуть бути катастрофічними: зупинка енергопостачання цілих регіонів, блокування лікарень, паралізація транспортних систем або навіть вплив на національну безпеку. Тому питання побудови ефективної технології реагування на інциденти в КІ набуває особливої актуальності.

Традиційні засоби захисту, такі як міжмережеві екрани, IDS/IPS чи антивірусні рішення, в умовах розвитку сучасних загроз дедалі частіше виявляються недостатніми. Основною проблемою є те, що вони орієнтовані переважно на сигнатурний підхід, тобто виявлення відомих атак, тоді як нові форми загроз відзначаються складністю, багаторівневістю і часто залишаються «невидимими» для класичних систем. Крім того, середовище OT/ICS має специфіку: промислові протоколи (Modbus, DNP3, IEC-104, PROFINET) не розроблялися з урахуванням принципів безпеки, а тому є вразливими до маніпуляцій. В умовах таких викликів усе більшого поширення набувають технології NDR (Network Detection and Response), що забезпечують постійний моніторинг та аналіз мережевого трафіку. На відміну від класичних IDS, рішення NDR здатні поєднувати сигнатурний та поведінковий аналіз, виявляючи невідомі або «нульові» загрози. Вони будують профілі нормальної активності користувачів, пристроїв та сегментів мережі, що дозволяє виявляти відхилення в режимі реального часу. Це критично важливо для об'єктів КІ, де аномальна

поведінка може свідчити про спроби атак на контролери або несанкціоновані зміни в системах SCADA. Важливою перевагою NDR є інтеграція з системами SOAR та SIEM, що дозволяє не лише фіксувати загрозу, а й ініціювати автоматизовані сценарії реагування. У разі виявлення інциденту NDR може передати інформацію до оркестраційної платформи, яка запускає плейбук: ізоляція зараженого вузла, блокування трафіку, формування інциденту в системі Service Desk чи повідомлення відповідального аналітика SOC. Такий підхід значно скорочує час виявлення та усунення загроз (MTTD і MTTR), що у середовищі критичної інфраструктури має визначальне значення. Однак застосування NDR у промислових системах має свої виклики. По-перше, реагування повинно бути обережним: будь-яке необґрунтоване блокування може призвести до зупинки виробництва чи збоїв у роботі важливих сервісів. По-друге, специфіка промислових протоколів потребує високої експертизи у налаштуванні правил і алгоритмів, щоб зменшити кількість хибних спрацювань. По-третє, для максимальної ефективності NDR необхідно інтегрувати з іншими засобами захисту — EDR, SIEM, DLP, CASB, створюючи багаторівневу архітектуру безпеки. Таким чином, технології NDR можна розглядати як один із найперспективніших напрямів розвитку реагування на інциденти в критичній інфраструктурі. Вони дозволяють досягти комплексного моніторингу, значно підвищують прозорість і контроль над OT-середовищем, створюють умови для побудови адаптивної системи кіберзахисту. Подальші дослідження та практичні впровадження мають бути зосереджені на вдосконаленні поведінкових алгоритмів, підвищенні рівня автоматизації реагування та формуванні політик, які враховують баланс між безпекою й безперервністю бізнес-процесів. Подальші дослідження в цій сфері сприятимуть розвитку інтелектуальних засобів обробки подій, вдосконаленню механізмів захисту особистих даних та впровадженню адаптивних політик безпеки для динамічного середовища роботи.

Перелік посилань:

1. Gartner. *Market Guide for Network Detection and Response*. Gartner Research, 2023.

2. ENISA. *Cybersecurity of Critical Infrastructure: Threat Landscape 2023*. European Union Agency for Cybersecurity, 2023.

3. Check Point Research. *NDR for Critical Infrastructure: Capabilities and Challenges*, 2022.

4. Zetter K. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. Crown, 2014.

Василенко Я.О.
студент групи БСДМ-61, ННІКБЗІ ДУІКТ,
Київ, Україна

АВТОМАТИЗАЦІЯ ПРОЦЕСІВ РЕАГУВАННЯ НА ІНЦИДЕНТИ В SOC ЗА ДОПОМОГОЮ ТЕХНОЛОГІЙ SOAR

У тезі аналізується автоматизація процесів реагування на інциденти в Security Operations Center (SOC) за допомогою технологій SOAR. У сучасних умовах великого потоку кіберзагроз платформи

SOAR інтегрують різнорідні інструменти безпеки, автоматизують стандартні процедури (playbooks) і консолідують процеси обробки інцидентів. Це дозволяє значно прискорити реагування та знизити навантаження на аналітиків. Основна увага приділяється ключовим функціям SOAR (оркестрація, автоматизація, управління інцидентами, звітування) та їхнім перевагам для SOC.

Ключові слова: SOAR, SOC, автоматизація, реагування на інциденти, інформаційна безпека.

Сучасні центри моніторингу безпеки (SOC) обробляють величезну кількість сповіщень про потенційні загрози, що призводить до «alert fatigue» – перевантаження аналітиків хибними тривогами [1]. Такий стан ускладнює своєчасне реагування на реальні інциденти та потребує значних людських ресурсів для обробки сповіщень. Саме тому для підвищення ефективності SOC актуальним стає впровадження автоматизації. SOAR-платформи автоматизують та координують реагування на інциденти, знижуючи навантаження на операторів і дозволяючи фахівцям зосередитися на складніших загрозах [1, 2].

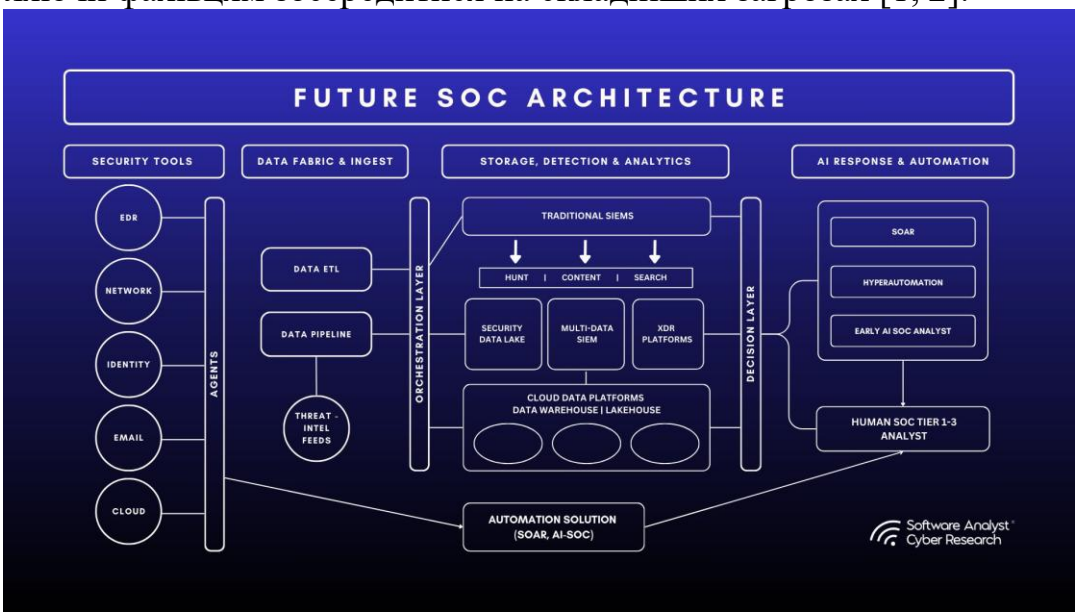

Рис. 1 – Архітектура SOC із впровадженням технології SOAR

Платформи SOAR поєднують функції оркестрації, автоматизації та реагування на інциденти. Вони фільтрують хибні тривоги, стандартизують процедури реагування та координують дії між різними інструментами безпеки [1]. SOAR дозволяє збирати інформацію про загрози з різних джерел, автоматично її аналізувати та виконувати передбачені сценарії (playbooks) для реагування[3, 4]. Це забезпечує єдиний огляд ситуації і оптимізує процеси аналізу інцидентів.

SOAR (Security Orchestration, Automation and Response) – це платформа кібербезпеки, що допомагає організаціям ефективніше управляти та реагувати на загрози [4]. Вона забезпечує узгоджене виконання повторюваних операцій та об’єднує розрізнені засоби захисту, що дозволяє централізовано обробляти інциденти [1, 4]. Основні функції SOAR-платформ:

- Оркестрація: інтеграція різних інструментів і технологій для узгодженого прийняття рішень на основі аналітики ризиків [3].
- Автоматизація: заміна ручних процедур автоматичними діями за заздалегідь прописаними сценаріями (playbooks) [3].

- Управління інцидентами: централізований контроль процесу реагування (пріоритезація, логування дій, ухвалення рішень) відповідно до внутрішніх політик організації [3].
- Звітування: генерація аналітичних звітів і візуалізація ключових показників (дашборди) для аналітиків, керівників SOC та CISO [3].

Переваги використання SOAR:

- Прискорене реагування та скорочення MTTR: автоматизовані сценарії реагування (playbooks) дозволяють негайно запускати контрзаходи при виявленні загрози, скорочуючи час вирішення інцидентів з годин до хвилин [1, 2].

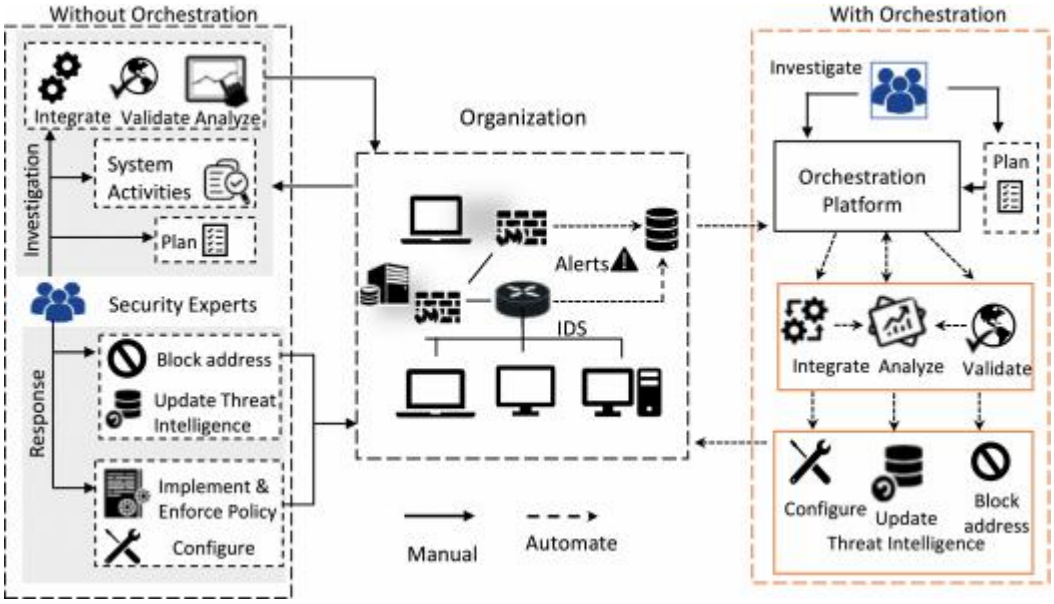

Рис. 2 – Порівняння ефективності SOC до та після впровадження SOAR

- Зменшення навантаження на аналітиків: SOAR-фільтрує хибні сповіщення та пріоритезує реальні загрози, виконуючи рутинні завдання автоматично. Це знижує «alert fatigue» і дає змогу фахівцям концентруватися на найскладніших загрозах [1, 2].
- Уніфікація та стандартизація процесів: уніфіковані playbooks гарантують послідовне виконання процедур реагування, що знижує ризик людських помилок і забезпечує однакове застосування політик безпеки [1].
- Цілісність моніторингу та звітності: SOAR-платформа консолідує дані з різних систем безпеки (SIEM, EDR, мережевий захист тощо) і надає єдину панель контролю. Це спрощує аналіз інцидентів і автоматичне формування звітів для всіх рівнів керівництва [3, 4].

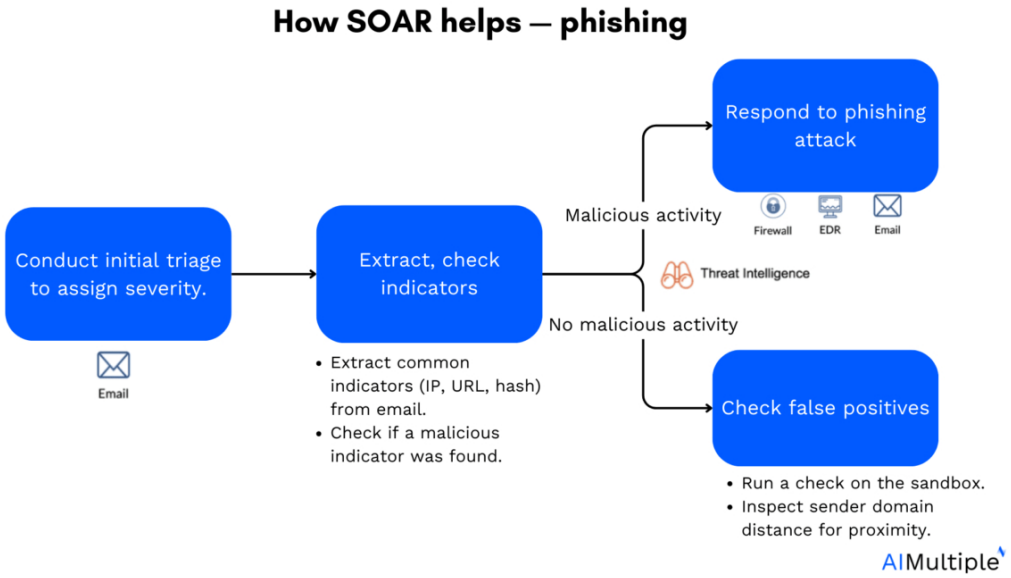

Рис. 3 – Приклад сценарію автоматизованого реагування (playbook) у SOAR-системі

Впровадження SOAR-платформ у SOC істотно підвищує ефективність реагування на кіберінциденти. Автоматизація та оркестрація дозволяють скоротити середній час розв'язання інцидентів, знизити людські помилки та забезпечити системний підхід до безпеки [2, 4]. Це зміцнює загальний кіберзахист організації і звільняє ресурси аналітиків для роботи з найважливішими загрозами [2, 4].

Перелік посилань:

1. Gurucul // *What Is SOC Automation?* [Електронний ресурс] — Режим доступу: https://gurucul.com/cybersecurity-101/what-is-soc-automation/
2. Palo Alto Networks // *SOAR vs. SIEM: What Is the Difference?* [Електронний ресурс] — Режим доступу: https://www.paloaltonetworks.com/cyberpedia/what-is-soar-vs-siem
3. Seeton Cyber Security Group // *Automated Incident Response (SOAR Solution)* [Електронний ресурс] — Режим доступу: https://www.seeton.pro/en/cybersecurity/soar/
4. One Identity // Security Orchestration, Automation and Response (SOAR) [Електронний ресурс] — Режим доступу: https://www.oneidentity.com/learn/what-is-soar.aspx/

Вербиненко В.О.
студент групи БСДМ-62, ННІКБЗІ ДУІКТ,
Київ, Україна

МОДЕЛЬ ВИЯВЛЕННЯ ІНСАЙДЕРСЬКИХ ЗАГРОЗ НА ОСНОВІ ГЕНЕРАТИВНО-ЗМАГАЛЬНИХ МЕРЕЖ

Завдання виявлення інсайдерських загроз є безперечно складним процесом, оскільки зловмисники діють з легітимними повноваженнями, що робить їхні дії важкопомітними для традиційних систем захисту. Їхня поведінка може лише незначно відхилятися від норми. У цьому контексті застосування генеративно-змагальних мереж (GAN) є активною та перспективною галуззю досліджень. Цей підхід є перспективним завдяки здатності GAN моделювати складні, нелінійні патерни нормальної поведінки, що теоретично дозволяє виявляти тонкі, але значущі відхилення, характерні для інсайдерських атак.

Ключові слова: генеративно-змагальні мережі, GAN, інсайдерські загрози, машинне навчання.

На думку багатьох фахівців, генеративно-змагальні мережі (GAN) є перспективним класом моделей для вирішення задач виявлення інсайдерських загроз, оскільки вони здатні вивчати розподіл нормальних даних. Парадигма виявлення аномалій на основі відтворення припускає, що модель, навчена на таких даних, може відтворити зразки наближені до нормальної поведінки, тоді як аномалії призведуть до високої помилки відтворення і будуть виділятись при аналізі [1,3].

Метою даної роботи була задача дослідити, чи можна використовувати модель GAN для виявлення зловмисної активності в системі, провести набір експериментів адаптуючи модель відповідно до отриманих результатів в пошуку робочої версії.

Основою для експериментів слугував набір даних CERT r4.2. Це набір даних, призначений для виявлення інсайдерських загроз. Він представляє собою агреговану поведінку користувачів у форматі "користувач-день": набір логів, що містять як нормальні, так і шкідливі сесії користувачів. Нашою метою було розробити модель на основі GAN, здатну виявляти ці шкідливі сесії з високою повнотою і достовірністю.

Для повноти результатів дослідження, логи користувачів були зібрані в один датасет, доповнений мітками (нормальна активність представлена 0, шкідлива активність як 1), а також структуровано кількома різними способами для навчання моделі:

A) Неструктурована серія даних, де модель тренується на поодиноких активностях;

B) 30-хвилинні вікна діяльності;

C) 24-годинний робочий день;

D) Розподілення по сесіям користувач:комп’ютер (де сесія - набір дій певного користувача на одному й тому ж самому комп’ютері між подіями входу і виходу в систему).

Слід зауважити, що класичні архітектури GAN характеризуються нестабільністю навчання через використання дивергенції Дженсена–Шеннона (JSD), що призводить до зникаючих градієнтів і колапсу мод. Ці обмеження роблять стандартні GAN непридатними для завдань з великою кількістю різнорідних даних, таких як поведінкові логи користувачів.

Зважаючи на це, було використано кілька відомих підходів до GAN, зокрема – Wasserstein GAN із градієнтним штрафом (WGAN-GP), що мало забезпечити стабільність навчання і покращити практичну ефективність у виявленні аномалій [2].

Дослідження пройшло кілька етапів:

1. AnoGAN (класична архітектура): модель навчалася на нормальних даних і оцінювала аномалії за помилкою реконструкції. Хоча метод демонстрував правильну логіку, він виявився надто повільним для практичного застосування – кожна оцінка вимагала сотень ітерацій оптимізації [3].
2. BiGAN (двонаправлений підхід): введення енкодера дозволило уникнути обчислювальних витрат, але призвело до колапсу навчання через дисбаланс між моделями.
3. WGAN: модель показала високий AUROC при роботі з даними, сортованими по сесіям, але інші показники досить низькі, як і в попередніх результатах.

Результати емпіричного тестування зведені у Таблиці 1. Для кожної конфігурації моделі було проведено повний цикл навчання (150 епох) на кожному з чотирьох визначених способів представлення вхідних даних, що дозволяє оцінити їх ефективність у різних умовах.

Таблиця 1. Результати тестування моделей

Модель	**Структура даних**	**Precision**	**Recall**	**AUROC**	**AUPRC**	**F1-Score**
Anogan	A	0.0435	0.0908	0.5056	0.0072	0.0589
	B	0.0754	0.0443	0.5075	0.0603	0.0558
	C	0.0493	0.0940	0.5049	0.0400	0.0647
	D	0.0479	0.0898	0.4003	0.0117	0.0625
BiGAN	A	0.0547	0.0258	0.5073	0.0296	0.0351

	B	0.0033	0.0985	0.4028	0.0919	0.0065
	C	0.0964	0.0396	0.5013	0.0863	0.0561
	D	0.0230	0.0108	0.4033	0.0338	0.0147
WGAN	A	0.0232	0.0951	0.6096	0.0002	0.0373
	B	0.0126	0.0759	0.6084	0.0872	0.0217
	C	0.0572	0.0142	0.8037	0.0311	0.0228
	D	0.0261	0.0398	0.9413	0.0270	0.0315

Проведений аналіз та серія експериментів із різними методами структурування даних призвели до однозначно негативних результатів. Хоча модель на базі WGAN, яка працювала з агрегованими по сесіям даними, показала порівняно високий AUROC, це свідчить про можливість з її допомогою аугментувати і доповнювати дані, але не відрізняти нормальну роботу користувача від дій потенційного зловмисника.

За результатами роботи можна зробити висновок, що генеративно-змагальні мережі не є самодостатнім інструментом для розв'язання задачі виявлення інсайдерських загроз.

Це вказує на те, що для досягнення практично значущих результатів, подальші дослідження мають бути зосереджені не на GAN як на окремому рішенні, а на гібридних підходах. Ефективність може бути досягнута шляхом поєднання GAN з більш потужними методами проектування ознак або шляхом їх інтеграції в ансамблі з іншими класами моделей, здатними краще обробляти таку складну природу даних.

Перелік посилань:

1. Arifin M.M., Ahmed M.S., Ghosh T.K., Zhuang J., Yeh J.-H. A Survey on the Application of Generative Adversarial Networks in Cybersecurity: Prospective, Direction and Open Research Scopes [Electronic resource] / arXiv preprint arXiv:2407.08839v1. – 2024. – Режим доступу: https://arxiv.org/html/2407.08839v1 (accessed: 24.10.2025).

2. Arjovsky M., Chintala S., Bottou L. Wasserstein GAN [Електронний ресурс] / arXiv preprint arXiv:1701.07875. – 2017. – Режим доступу: https://arxiv.org/abs/1701.07875 (дата звернення: 24.10.2025).

3. Bartoszewski F.W., Just M., Lones M.A., Mandrychenko O. Anomaly Detection for Insider Threats: An Objective Comparison of Machine Learning Models and Ensembles [Електронний ресурс] / в : A. Jøsang, L. Futcher, J. Hagen (ред.) *ICT Systems Security and Privacy Protection. SEC 2021. IFIP Advances in Information and Communication Technology, vol. 625*. Cham : Springer, 2021. – С. 367-381. – Режим доступу: https://doi.org/10.1007/978-3-030-78120-0_24 (дата звернення: 24.10.2025).

Гавриленко Д.П.
студент групи БСДМ-51, ННІКБЗІ ДУІКТ,
Київ, Україна

АКТУАЛЬНІ ПРОБЛЕМИ ТА НАПРЯМКИ УДОСКОНАЛЕННЯ МОДЕЛЕЙ БЕЗПЕКИ СУЧАСНИХ ОПЕРАЦІЙНИХ СИСТЕМ LINUX ТА ANDROID

Сучасні операційні системи Linux та Android, незважаючи на інтегровані механізми захисту, стикаються зі зростаючою кількістю складних кіберзагроз, що експлуатують як архітектурні особливості, так і людський фактор. Стандартні конфігурації безпеки часто виявляються недостатніми для протидії атакам з підвищенням привілеїв, експлуатації прихованих каналів та іншим векторам атак. У тезах аналізуються обмеження поширених моделей контролю доступу (DAC, MAC, RBAC) та ефективність вбудованих засобів захисту в контексті загроз, ідентифікованих за моделлю STRIDE. Обґрунтовується необхідність застосування комплексного, багатошарового підходу до посилення безпеки, що включає конфігураційне зміцнення (харденінг) ключових підсистем ОС та підвищення рівня кібергігієни користувачів.

Ключові слова: моделі безпеки ОС, Linux, Android, кібербезпека, контроль доступу, DAC, MAC, RBAC, STRIDE, DFD, підвищення привілеїв, харденінг, AppArmor, sysctl, auditd, кібергігієна.

Операційні системи Linux та Android є основою значної частини сучасної цифрової інфраструктури. Їхня поширеність робить їх пріоритетними цілями для дедалі витонченіших кібератак. Хоча розробники ОС впроваджують різноманітні механізми безпеки (мандатний контроль доступу, ізоляція процесів, криптографічний захист), стандартні конфігурації часто залишають простір для експлуатації вразливостей. Проблеми неправильної конфігурації, несвоєчасного оновлення, архітектурних обмежень та людських помилок створюють значні ризики. Необхідний аналіз ефективності існуючих моделей безпеки та обґрунтування шляхів їх удосконалення.

Ефективність захисту ОС залежить від застосованої моделі контролю доступу. Аналіз поширених моделей виявляє їхні обмеження:

- Дискреційна (DAC): Гнучка, але вразлива до помилок конфігурації та зловживань правами власника; root може обійти правила [1].
- Мандатна (MAC): Забезпечує сильний контроль (SELinux, AppArmor), ефективна проти підвищення привілеїв, але складна в адмініструванні. Обов'язкова в Android (SELinux), вибіркова в Linux.
- Рольова (RBAC): Спрощує керування у великих системах, але може призводити до "розповзання привілеїв".

Фундамент безпечної операційної системи закладається не стільки окремими механізмами, скільки набором архітектурних принципів, адже на відміну від прикладної або мережевої безпеки, де компрометація обмежується одним сервісом чи вузлом, порушення цілісності ядра або драйверів робить вразливими саму систему та всі розгорнуті на ній компоненти. Тому жодна модель не є ідеальною [1]. Linux вимагає експертних знань для налаштування гнучких комбінацій, тоді як Android обмежує кастомізацію [3].

Таблиця 1 - Порівняння моделей контролю доступу

Модель	Визначення	Переваги	Недоліки
DAC	Власник керує доступом	Проста	TOCTOU-ризики
MAC	Політика ядра	root ≠ повний доступ	Складність адміністрування
RBAC	Доступ через ролі	Мінімальні права	Необхідність оновлення ролей
Zero Trust	“Не довіряй нікому”	end-to-end контроль	Ресурсоємність та зручність

Моделювання загроз за методологією STRIDE у поєднанні з DFD-діаграмами дозволяє виявити найбільш значущі вектори атак [2].

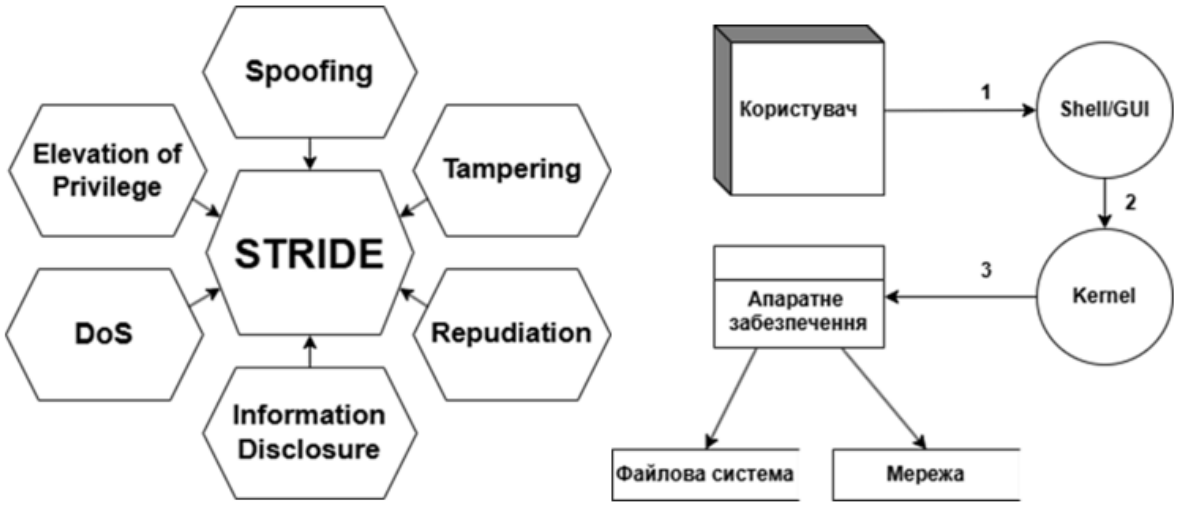

Рис. 1 - Модель загроз STRIDE та DFD

Найпріоритетними загрозами є: підвищення привілеїв (Elevation of Privilege)Фундаментальна загроза через уразливості ядра, служб або конфігурації. Приховані канали (Covert Channels): Дозволяють обходити ізоляцію для витоку даних. Складні для виявлення Атаки на продуктивність (DoS): Можуть призвести до недоступності сервісів через виснаження ресурсів

Сучасні Linux (Ubuntu 22.04) та Android (Android 14) мають значний набір вбудованих засобів: AppArmor/SELinux, автоматичні оновлення, Verified Boot, шифрування, ізоляція додатків.

Таблиця 2 - Порівняння базових механізмів безпеки Linux та Android

Критерій	Ubuntu 22.04	Android 14
MAC	AppArmor	SELinux
Verified Boot	UEFI SB	AVB + VBMeta
Sandbox	LXD / namespaces	UID + SELinux
Найпопулярніша загроза	Локальне EoP	Ланцюг RCE→EoP

Однак ці механізми мають обмеження від конфігурації, оновлень, людський фактор та атак нульового дня. Виявлені проблеми обґрунтовують необхідність багатошарового, проактивного підходу:

1. Харденінг ядра та системних параметрів (sysctl): Тонке налаштування параметрів ядра Linux превентивно блокує вектори атак на рівні ОС.
2. Ефективне застосування MAC (AppArmor/SELinux): Створення гранулярних політик для критичних сервісів є ключовим для реалізації принципу найменших привілеїв.
3. Мережева фільтрація (UFW/nftables): Політика "заборонити за замовчуванням" на брандмауері зменшує поверхню атаки з мережі.
4. Проактивний аудит (auditd): Детальне логування критичних подій дозволяє виявляти аномалії та атаки в реальному часі.
5. Підвищення кібергігієни користувачів: Людський фактор залишається вирішальним. Необхідне постійне навчання користувачів [3].

Отже, стандартні механізми безпеки ОС Linux та Android не є достатні проти сучасних кіберзагроз. Ефективна безпека вимагає багатошарового, проактивного підходу, що поєднує теоретично обґрунтований харденінг системи (ядро, мережа, контроль доступу, аудит) та підвищення обізнаності користувачів. Інструменти sysctl, гранулярні політики MAC, мережева фільтрація та детальний аудит суттєво підвищують стійкість систем. Кібергігієна користувачів залишається критично важливим елементом. Лише комплексне застосування цих заходів забезпечує адекватний рівень захисту.

Перелік посилань:

1. Saltzer J. H., Schroeder M. D. The Protection of Information in Computer Systems // Proceedings of the IEEE. 1975. Vol. 63, No. 9. P. 1278–1308. URL: https://web.mit.edu/6.857/OldStuff/Fall03/ref/saltzer-schroeder.pdf
2. Threat Modeling Process // OWASP. [Електронний ресурс]. Режим доступу: https://owasp.org/www-community/Threat_Modeling_Process
3. Android security architecture and features // Source.android.com Docs. [Електронний ресурс]. Режим доступу: https://source.android.com/docs/security/features

Гайдур Г.І., завідувач кафедри СТКБ, ННІКБЗІ
ДУІКТ, Київ, Україна
Московка С.М., студент групи БСДМ-62,
ННІКБЗІ ДУІКТ, Київ, Україна

ЗАХИСТ КІНЦЕВИХ ТОЧОК ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ ВІД СУЧАСНИХ ЗАГРОЗ

Сьогодні захист кінцевих точок інформаційної системи організації є надзвичайно актуальним питанням. Адже загрози значно ускладнилися і стали більш витонченими. Зловмисники використовують штучний інтелект для створення переконливих фішингових повідомлень та задля маскування шкідливого програмного забезпечення. З поширенням віддаленої роботи та використанням особистих пристроїв в офісних мережах, кількість вразливих точок в інформаційній системі організації компаній різко зростає. Тому захист кінцевих точок інформаційної системи організації є актуальним питанням.

Ключові слова: загрози, кінцева точка, кібербезпека, шкідливе програмне забезпечення.

Захист кінцевих точок інформаційної системи організації– це підхід до кібербезпеки, який захищає пристрої кінцевих користувачів, такі як ноутбуки, настільні комп'ютери, мобільні телефони та сервери, від кіберзагроз. Захист гарантує безпеку цих точок доступу до мережі організації, запобігаючи несанкціонованому доступу зловмисників або компрометації даних [1].

Безпека кінцевих точок розширює периметр безпеки організації на кожен окремий пристрій, який підключається до її мережі (рис.1). Ці пристрої, або «кінцеві точки», є потенційними точками входу для кібератак , що робить їх комплексний захист першочерговим завданням [2].

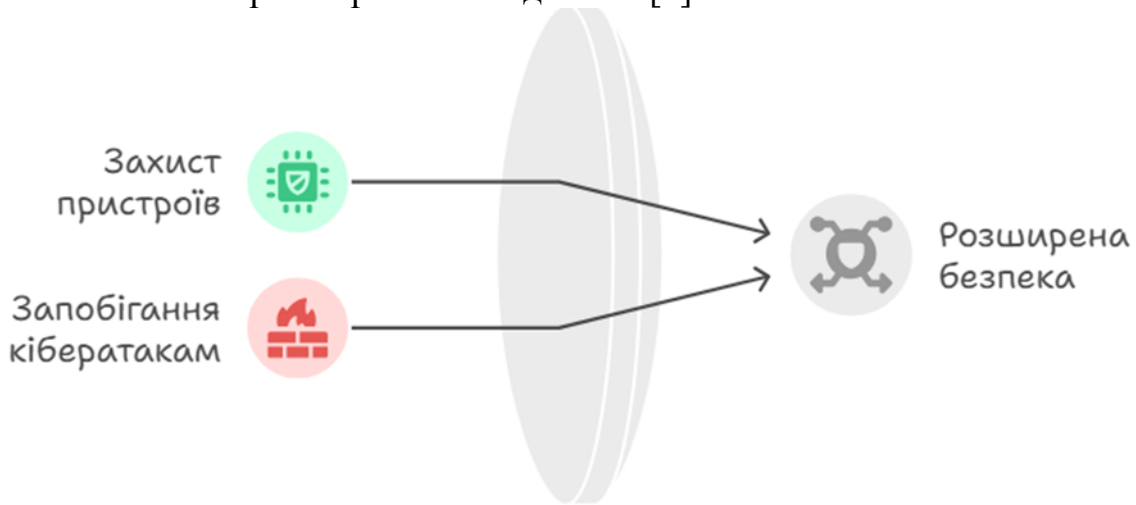

Рис.1. Безпека кінцевих пристроїв

Традиційні антивіруси вже не можуть ефективно протистояти цим **новим загрозам**, таким як програми-вимагачі (ransomware) та цілеспрямованим атакам. Кінцеві точки є дверима до найцінніших **корпоративних даних** та інтелектуальної власності. Якщо ці пристрої будуть скомпрометовані, це призведе до **витоку даних**, значних фінансових втрат та шкоди репутації

компанії. Тому захист кінцевих точок вимагає **комплексних рішень** з функціями виявлення та реагування (EDR), які постійно моніторять і захищають пристрої в режимі реального часу.

Розглянемо щодо роботи технології захисту від шкідливого програмного забезпечення на основі використання Cortex XDR.

Cortex XDR руйнує ізольовані рішення безпеки, пропонуючи агента кінцевих точок, механізм аналітики виявлення загроз, автоматизацію для кінцевих точок та сповіщень, виявлення загроз ідентифікації, можливості криміналістики та підтримку отримання даних третіх сторін.

Агент Cortex XDR використовує передові багаторівневі методи захисту та запобігання для захисту ваших кінцевих точок від відомих та невідомих шкідливих програм та програмних експлойтів.

Агент Cortex XDR забезпечує захист від шкідливого програмного забезпечення в серії з чотирьох фаз оцінювання, як це показано на рис.2.

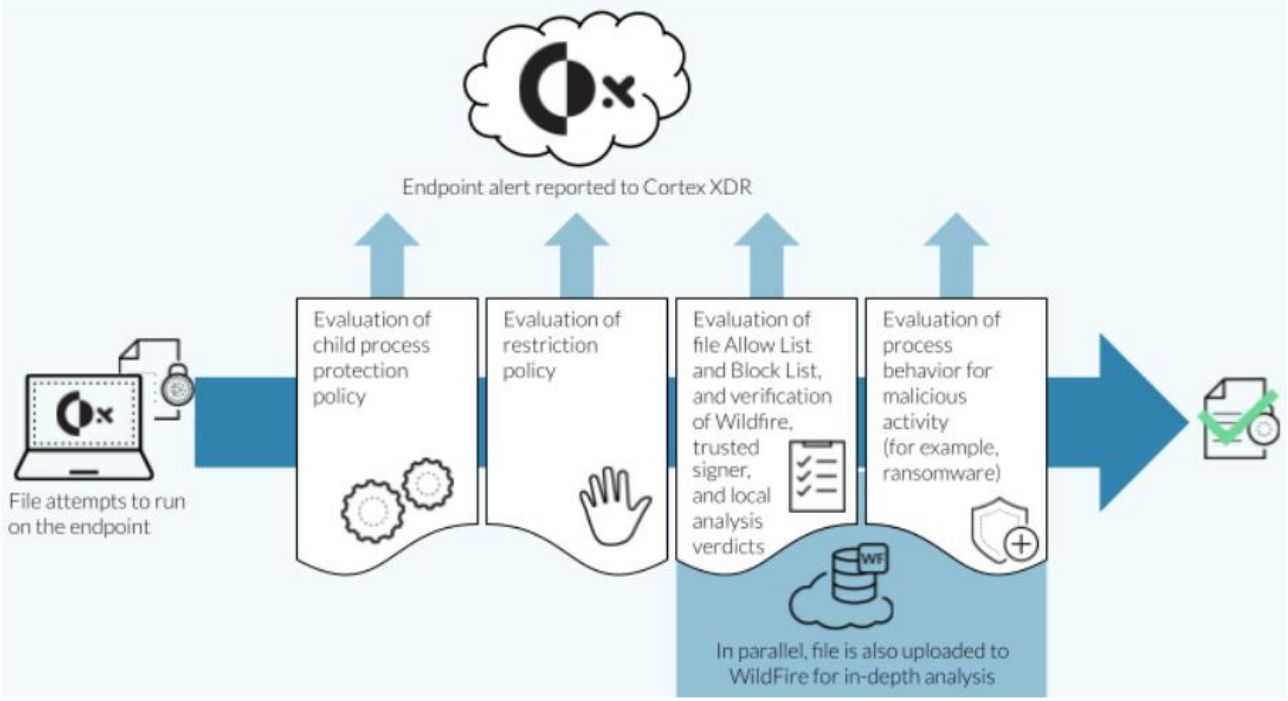

Рис. 2. Фази оцінювання захисту від шкідливого програмного забезпечення

Фаза 1: Оцінка політики захисту процесуальних питань дочірних процесів.

Фаза 2: Оцінка політики обмежень.

Фаза 3: Визначення вердикту хешу.

Фаза 4: Оцінка політики захисту від шкідливого програмного забезпечення.

Перелік посилань:

1. Cortex-XDR. URL: https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-4.x-Documentation/Learn-about-Cortex-XDR /

2. Захист кінцевих точок. UR: https://docs-cortex.paloaltonetworks.com/r/Cortex-CLOUD/Cortex-Cloud-Runtime-Security-Documentation/Endpoint-protection .

Гуляєв А.В.
студент групи БСДМ-62, ННІКБЗІ ДУІКТ,
Київ, Україна

ІНТЕЛЕКТУАЛЬНІ СИСТЕМИ ПРОТИДІЇ СОЦІАЛЬНІЙ ІНЖЕНЕРІЇ В КОРПОРАТИВНИХ МЕРЕЖАХ

Фішинг як інструмент соціальної інженерії залишається однією з найпоширеніших загроз для користувачів і організацій. У цій тезі розглянуто проблематику протидії методам соціальної інженерії в корпоративному середовищі, що набуває особливої актуальності в умовах зростання кількості кібератак, спрямованих на людський фактор. Запропоновано підхід до створення інтелектуальної системи захисту, заснованої на алгоритмах штучного інтелекту, яка дозволяє автоматизувати виявлення спроб маніпуляцій, фішингових атак та несанкціонованих дій користувачів.

Ключові слова: фішинг, соціальна інженерія, штучний інтелект, NLP, адаптивне навчання, корпоративна безпека.

Соціальна інженерія залишається одним із найефективніших інструментів зловмисників, спрямованим на отримання конфіденційних даних шляхом психологічного впливу на користувачів [1]. Традиційні методи кіберзахисту зосереджені переважно на технічних аспектах — шифруванні, автентифікації, контролі доступу, — однак не враховують поведінкові чинники, пов’язані з діяльністю персоналу [2].

Інтелектуальні системи, побудовані на основі алгоритмів машинного навчання, відкривають нові можливості для протидії таким загрозам. Вони здатні аналізувати поведінкові моделі користувачів, контент електронних листів та повідомлень, а також виявляти відхилення від звичної активності. Застосування методів обробки природної мови (NLP) дає змогу ідентифікувати ознаки маніпулятивних чи фішингових повідомлень у реальному часі [3].

Практична реалізація таких систем у корпоративних мережах передбачає інтеграцію аналітичного модуля ШІ з існуючими системами моніторингу безпеки (SIEM) та управління доступом (IAM). Це дозволяє не лише виявляти потенційні загрози, а й формувати адаптивні політики безпеки залежно від рівня ризику користувача чи підрозділу.

У практичному застосуванні інтелектуальні системи протидії соціальній інженерії часто поєднують кілька рівнів контролю. Наприклад, у корпоративних мережах застосовують одночасно:

Аналіз електронної пошти: автоматична перевірка вхідних повідомлень на ознаки фішингу — підозрілі посилання, невідповідні домени, термінові запити про передачу даних.

Моніторинг поведінки користувачів: виявлення нетипових дій, таких як повторне введення паролів, швидке відкриття вкладень або пересилання повідомлень стороннім особам.

Динамічне навчання персоналу: після виявлення потенційно ризикових дій система негайно надає короткі навчальні матеріали, пояснює ризик і дає рекомендації щодо безпечної поведінки [1,3].

Реальні кейси показують ефективність такого підходу. Наприклад, у пілотному впровадженні системи на базі NLP та адаптивного навчання для середньої IT-компанії вдалося:

зменшити кількість успішних фішингових атак на 35 % за перші три місяці;

підвищити швидкість реагування співробітників на підозрілі повідомлення майже вдвічі;

знизити навантаження на службу безпеки за рахунок автоматизації первинного аналізу листів [2].

Таким чином, поєднання алгоритмів штучного інтелекту з практичним навчанням користувачів забезпечує системний захист, який охоплює як технічні, так і поведінкові аспекти кібербезпеки. Такий комплексний підхід дозволяє організаціям значно підвищити стійкість до сучасних методів соціальної інженерії та зменшити вплив людського фактора на рівень інформаційної безпеки.

Перелік посилань:

1. Mitnick K., Simon W. The Art of Deception: Controlling the Human Element of Security. Wiley, 2021.
2. Maimon D., Alper M. Social Engineering: Nontechnical Threats to Information Security. CRC Press, 2019.
3. Almomani A. et al. Phishing Detection Based on Machine Learning Algorithms. Security and Communication Networks, 2022.

Жакомін Дмитро Юрійович
студентка групи БСДМ-62, ННІКЗБІ ДУІКТ,
Київ, Україна

СИСТЕМА ЗАХИСТУ REST API ВІД МЕРЕЖЕВИХ АТАК

У сучасному цифровому середовищі кіберзагрози стають дедалі складнішими. Щоб забезпечити безпеку та надійність веб-систем, ми повинні постійно оцінювати та вдосконалювати методи виявлення їхніх вразливостей.

У сучасному світі обмін даними між клієнтськими застосунками та серверами виконується через REST API, який забезпечує стандартний та простий спосіб взаємодії веб-сервісів за допомогою HTTP-запитів. Ця універсальність є їхньою найбільшою силою — вона дозволяє різним платформам та системам швидко інтегруватися, забезпечуючи масштабування інфраструктури та гнучкість в обробці інформації, незалежно від операційної системи чи мови програмування. Однак саме ця відкритість та широке поширення також роблять REST API головною мішенню для кібератак [1].

Згідно зі звітом про тенденції безпеки API за 2023 рік, значна частина організацій використовує понад 2500 API, створюючи величезну поверхню для атак зловмисників. За останні 2 роки 60% організацій повідомили про витік даних, при цьому ці інциденти були системними що в подальшому впливає на фінансові збитки, крадіжку інтелектуальної власності та втрату репутації бренду [2].

До поширених вразливостей API часто належать [3]:

- Відсутність обмеження швидкості, що дозволяє системам бути перевантаженими.
- Недоліки в автентифікації та авторизації, що дозволяють зловмисникам видавати себе за законних користувачів.
- Недостатня перевірка даних на стороні сервера, що відкриває двері для зловмисного введення даних.

Наслідки цих атак можуть бути серйозними, починаючи від компрометації конфіденційних даних та перебоїв у роботі сервісів і закінчуючи крадіжкою облікових даних користувачів. З усіх цих причин розробка ефективніших рішень безпеки для REST API — це не просто технічна мета, а нагальна та критична необхідність [2].

Проведені дослідження демонструють нам що більшість сучасних API залишаються вразливими через недостатню перевірку структури даних. Недоліками існуючих підходів є використання окремих методі захисту ізольовано, без інтеграції їх в єдину систему, що створює сліпі зони в безпеці та послаблює загальний захист. Існуючі рішення покривають лише окремі типи загроз, залишаючи інші вразливості поза увагою. З появою нових видів атак або зі зміною поведінки користувачів системи є недостатньо адаптивними, щоб ефективно запобігти загрозам [1, 4].

Щоб підвищити рівень безпеки пропонується створити систему захисту REST API, яка поєднує кілька методів у єдиний комплекс.

Це включає:

- Автентифікація та авторизація: Використання надійних стандартів, таких як JWT та OAuth2.
- Обмеження швидкості: Контроль кількості запитів, які може зробити користувач.
- Перевірка вхідних даних: Забезпечення правильності та безпеки всіх вхідних даних.
- Моніторинг та ведення журналу: Спостереження за підозрілою активністю.

На відміну від стандартних рішень, де ці механізми працюють окремо, у даній системі вони взаємодіють між собою. Наприклад, можливість відстежувати аномальні дії користувачів, як-от часті спроби доступу до ресурсів чи підозріло велику кількість запитів за короткий проміжок часу.

З часом REST API збереже свою актуальність та продовжить відігравати ключову роль у світі розробки, тому важливо впроваджувати комплексі системи захисту для ефективної протидії загрозам.

Перелік посилань:

1. Tanveer M. et al. Towards Secure APIs: A Survey on RESTful API Vulnerability Detection: Computers, Materials & Continua, 2025, Vol. 84, No. 3, P. 4223-4257. DOI:10.32604/cmc.2025.067536.
2. Traceable - Blog: 2023 API Security Trends: Insights, Risks, and Strategies. Traceable: Intelligent Application and API Security at Enterprise Scale. URL: https://www.traceable.ai/blog-post/2023-state-of-api-security-trends (date of access: 23.10.2025).
3. OWASP Top 10 API Security Risks – 2023 - OWASP API Security Top 10. OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation. URL: https://owasp.org/API-Security/editions/2023/en/0x11-t10/ (date of access: 23.10.2025).
4. Jang S.-W., Lee S.-H. Vulnerabilities and Encryption Applications of JWT-Based Authentication Methods // Journal of Information Systems Engineering & Management. – 2025.

Жилін М.І.
студент групи ІСДМ-61 ННІІТ ДУІКТ,
Київ, Україна

ОПТИМІЗОВАНИЙ КОМП'ЮТЕРНИЙ ЗІР ДЛЯ ІДЕНТИФІКАЦІЇ ТРАНСПОРТУ В ІТС

Що ми розуміємо під ІТС? Інтелектуальні транспортні системи (ІТС) є основою для "розумних міст", і їхня ефективність критично залежить від здатності автоматичної ідентифікації та категоризації транспортних засобів (АІТЗ). Сучасні вимоги до АІТЗ включають не лише розпізнавання номерних знаків, але й точну класифікацію ТЗ за типом, маркою та моделлю у складних експлуатаційних умовах. Традиційні алгоритми комп'ютерного зору (КЗ) часто не можуть забезпечити необхідну швидкість та стійкість до факторів навколишнього середовища (погана погода, динамічні зміни освітлення, висока швидкість руху).

Ключові слова: комп'ютерний зір, глибоке навчання, ІТС, CNN, ідентифікація транспортних засобів, категоризація, обробка в реальному часі.

1. Актуальність та Методологічний Виклик

Основний виклик для ІТС полягає у необхідності одночасного досягнення двох цілей: максимальної точності (для надійної класифікації) та мінімальної затримки (latency) (для обробки даних у реальному часі, критичної для безпеки та управління трафіком). Для вирішення цієї проблеми пропонується оптимізація глибоких конволюційних нейронних мереж (CNN), які здатні автоматично витягувати складні ознаки, але вимагають адаптації для периферійних обчислень (Edge Computing). [3]

У рамках даного дослідження було розроблено та проаналізовано методологію оптимізації CNN-архітектур для швидкого та точного розпізнавання та категоризації ТЗ. Дослідження зосереджується на:

- Порівнянні архітектур: Оцінка ефективності легкозважених CNN-архітектур (наприклад, MobileNet, EfficientNet) порівняно з громіздкими, але високоточними моделями (наприклад, VGG, ResNet).

- Техніках оптимізації: Застосування методів квантування та прунінгу для зменшення розміру моделі та прискорення висновку без критичної втрати точності.
- Стійкості до умов: Оптимізація навчання на датасетах з високою варіативністю для підвищення стійкості системи до типових експлуатаційних викликів ІТС.

2. Архітектура Системи та Технологічна Інтеграція

Пропонована концептуальна модель АІТЗ розділена на модулі, що функціонують послідовно. [1]

Етапи роботи системи:

1. Захоплення даних: Високошвидкісне захоплення зображень із дорожніх камер.
2. Обробка на периферії: Використання оптимізованої CNN-моделі для швидкої детекції та виділення ТЗ.
3. Багаторівневий аналіз: Рівень 1 (Категоризація): Визначення типу ТЗ (вантажівка, легковик, автобус). Рівень 2 (Ідентифікація): Розпізнавання номерного знаку (ANPR) та/або розпізнавання марки/моделі.
4. Вивід: Передача категоризованих даних до центральної системи ІТС.

Таблиця 1. Порівняння CNN-Архітектур для Впровадження в ІТС

Параметр	VGG16 (Традиційна)	MobileNetV2 (Легкозважена)	Результат Оптимізації (Пропонована)
Кількість параметрів	≈138 млн (Висока)	≈3.5 млн (Низька)	<3.0 млн (Мінімальна)
Обчислювальна складність	Висока (GFLOPS)	Низька (MFLOPS)	Ультра-низька
Швидкість Inference	Повільна	Висока	Реальний час (на периферії)
Типова Точність	Дуже висока (98%)	Середня (90-95%)	Висока (95-97%)
Сфера застосування	Хмарні обчислення	Мобільні пристрої	Edge-пристрої, Дорожні контролери

3. Висновки та Перспективи

Проведене дослідження підтверджує, що застосування оптимізованих легкозважених CNN-архітектур у поєднанні з ефективними техніками квантування дозволяє створити систему АІТЗ, яка забезпечує високий рівень точності категоризації при швидкості обробки, достатній для функціонування в динамічному середовищі ІТС. Досягнення цього балансу є критично важливим для підвищення ефективності автоматизованого контролю трафіку, безпеки та керування міською інфраструктурою. [2]

Подальші дослідження будуть спрямовані на впровадження методів федеративного навчання для постійного оновлення моделі на основі даних з різних дорожніх ділянок без компрометації конфіденційності. [4]

Перелік посилань:

1. Azhad Zuraimi, Fadhlan Hafizhelmi Kamaru Zaman, "Vehicle Detection and Tracking using YOLO and DeepSORT", in 2021 IEEE 11th IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE) DOI:10.1109/ISCAIE51753.2021.9431784
2. M. Ravichandran, K. Laxmikant and A. Muthu, "Efficient Vehicle Detection and Classification using YOLO v8 for Real-Time Applications," 2023 Global Conference on Information Technologies and Communications (GCITC), Bangalore, India, 2023, pp. 1-5, doi: 10.1109/GCITC60406.2023.10426587.
3. J. Karangwa, J. Liu and Z. Zeng, "Vehicle Detection for Autonomous Driving: A Review of Algorithms and Datasets," in IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 11, pp. 11568-11594, Nov. 2023, doi: 10.1109/TITS.2023.3292278.
4. Michael Abebe Berwo, Asad Khan, Yong Fang, Hamza Fahim, Shumaila Javaid, Jabar Mahmood, Zain Ul Abideen, Syam M.S. «Deep Learning Techniques for Vehicle Detection and Classification from Images/Videos: A Survey», in Sensors 2023, 23(10), 4832; https://doi.org/10.3390/s23104832

Земляков Сергій Олексійович
студент групи БСДМ-51, ННІКБЗІ ДУІКТ, Київ, Україна

ПРОБЛЕМИ ТА СТРАТЕГІЇ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОНТЕЙНЕРИЗОВАНИХ ДОДАТКІВ У ХМАРНИХ СЕРЕДОВИЩАХ

У тезі проаналізовано ключові виклики безпеки, що виникають при використанні технологій контейнеризації, зокрема Docker та Kubernetes, у хмарних інфраструктурах. Розглянуто основні вектори атак, такі як вразливості базових образів, ризики середовища виконання, включаючи "втечу з контейнера", та проблеми невірної конфігурації оркестраторів. Запропоновано багаторівневу стратегію захисту, що ґрунтується на принципах DevSecOps, та охоплює сканування вразливостей на етапі CI/CD, впровадження політик безпеки на рівні кластера та моніторинг поведінки під час виконання для виявлення аномалій.

Вступ. Перехід до хмарно-нативної (cloud-native) архітектури став де-факто стандартом для розробки сучасних корпоративних інформаційних систем. Технології контейнеризації, такі як Docker, та системи оркестрації, як Kubernetes, забезпечують безпрецедентну гнучкість, масштабованість та швидкість розгортання додатків [1]. Однак ця динамічність та ефемерність інфраструктури породжують новий, складний ландшафт загроз, до якого традиційні моделі безпеки, орієнтовані на периметр, не пристосовані. Метою даної роботи є аналіз специфічних вразливостей контейнеризованих середовищ та формування комплексної стратегії мінімізації ризиків.

Аналіз основних загроз безпеці контейнерів. Проблеми безпеки у хмарно-нативних системах існують на кожному етапі життєвого циклу додатка та інфраструктури. Їх можна класифікувати за кількома ключовими напрямками.

1) **Вразливості ланцюга постачання (Supply Chain Vulnerabilities).** Контейнери будуються на основі "образів" (images), які, в свою чергу, складаються з шарів. Базові образи, що часто завантажуються з публічних репозиторіїв (напр., Docker Hub), можуть містити застарілі бібліотеки з відомими вразливостями (CVE). Дослідження показують, що значний відсоток офіційних образів містить критичні вразливості

[2]. Компрометація будь-якого шару в образі автоматично компрометує кожен контейнер, запущений на його основі.

2) **Безпека середовища виконання (Runtime Security).** Найбільш критичною загрозою під час виконання є "втеча з контейнера" (container escape). Це атака, при якій процес всередині контейнера отримує несанкціонований доступ до базової хост-системи. Зазвичай це стається через вразливості ядра Linux або, що частіше, через надмірні привілеї, надані контейнеру (наприклад, запуск від імені 'root' або у привілейованому режимі --privileged). Отримавши доступ до хоста, зловмисник може контролювати всі інші контейнери на даній ноді.
3) **Помилки конфігурації оркестратора та мережі. Системи** оркестрації, як Kubernetes, є складними системами з сотнями параметрів конфігурації. Помилки, залишені за замовчуванням (наприклад, відкритий доступ до API-сервера або Kubelet), створюють величезні прогалини в безпеці. Окремою проблемою є мережева безпека. У Kubernetes за замовчуванням реалізована "пласка" мережа, де кожен "под" (pod) може вільно спілкуватися з кожним іншим. Це ідеальне середовище для латерального (горизонтального) переміщення зловмисника після компрометації одного сервісу [3].
4) **Стратегії захисту та модель "4C".** Ефективний захист хмарно-нативних додатків вимагає інтегрованого підходу, відомого як DevSecOps – інтеграції безпеки на кожен етап життєвого циклу. Цей підхід зручно описується моделлю "4C" (Cloud, Cluster, Container, Code), яка передбачає ешелонований захист [4].

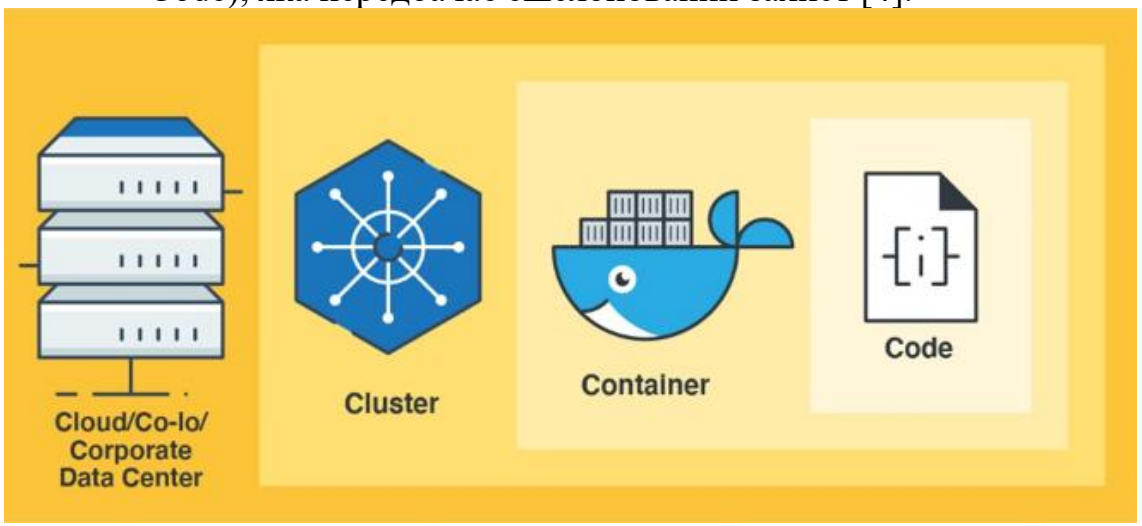

Рис. 1. Модель 4C безпеки хмарно-нативних додатків [4]

- **Cloud/Corporate (Хмара/Інфраструктура**): Це базовий рівень інфраструктури (IaaS або фізичні сервери). Безпека тут забезпечується захистом хост-ОС, налаштуванням фаєрволів хмарного провайдера (Security Groups) та суворим управлінням доступом (IAM).
- **Cluster (Кластер):** Це рівень оркестратора (Kubernetes). Захист включає аудит конфігурації кластера (наприклад, за стандартами CIS Kubernetes

Benchmark), використання аутентифікації та авторизації (RBAC) та, що найважливіше, впровадження мережевих політик (Network Policies). Мережеві політики дозволяють реалізувати мікросегментацію, обмежуючи трафік між подами за принципом нульової довіри (Zero Trust).

- **Container (Контейнер):** На цьому етапі ключовим є сканування образів контейнерів на наявність CVE. Цей процес має бути інтегрований у CI/CD-пайплайн, блокуючи розгортання образів, що не відповідають політикам безпеки. Також сюди входить "зміцнення" (hardening) образів – мінімізація їх вмісту (distroless images) та запуск процесів від імені непривілейованого користувача.
- **Code (Код):** Захист починається на рівні коду. Включає статичний аналіз коду (SAST), аналіз залежностей (SCA) для виявлення вразливих бібліотек та управління секретами (уникнення "hard-code" паролів).

Для захисту середовища виконання (Runtime) необхідно використовувати спеціалізовані інструменти, які відстежують поведінку контейнерів у реальному часі. Такі системи (напр., Falco, Aqua Security) використовують правила або машинне навчання для виявлення аномальної активності, такої як запуск неавторизованих процесів, спроби зміни файлової системи або підозрілі мережеві з'єднання, що можуть свідчити про спробу "втечі з контейнера".

Висновки. Контейнеризація та оркестрація кардинально змінили підходи до розробки та експлуатації корпоративних систем, але водночас створили нові, складні виклики у сфері кібербезпеки. Забезпечення захисту у таких динамічних середовищах неможливе без комплексного, багаторівневого підходу. Стратегія повинна поєднувати "shift-left" практики (сканування коду та образів на ранніх етапах), суворе налаштування конфігурації кластера та мережеву мікросегментацію, а також постійний моніторинг поведінки під час виконання для виявлення та реагування на атаки в реальному часі.

Перелік посилань:

1. Alexis Richardson. CNCF TOC Chair & CEO Weaveworks. What is Cloud Native and why should I care? URL: https://www.cncf.io/wp-content/uploads/2020/08/What-is-Cloud-Native-CNCF-Webinar-23-Feb-2017-1.pdf
2. Liran Tal. Snyk Blog. Top 5 Docker Security Vulnerabilities. URL: https://snyk.io/blog/top-5-docker-security-vulnerabilities/
3. Kubernetes Documentation. Security Checklist. URL: https://kubernetes.io/docs/concepts/security/security-checklist/
4. Magno Logan. Trend Micro. Securing the 4 Cs of Cloud-Native Systems: Cloud, Cluster, Container, and Code. URL: https://www.trendmicro.com/vinfo/gb/security/news/virtualization-and-cloud/securing-the-4-cs-of-cloud-native-systems-cloud-cluster-container-and-code

Ісаєнко І.І., студент групи БСДМ-62,
ННКБЗІ ДУІКТ, Київ, Україна

УПРАВЛІННЯ МОБІЛЬНИМИ ПРИСТРОЯМИ В СУЧАСНОМУ КОРПОРАТИВНОМУ СЕРЕДОВИЩІ: ВИКЛИКИ СЬОГОДЕННЯ ТА СТРАТЕГІЇ ПОДОЛАННЯ

Широке використання мобільних пристроїв в організаціях дозволяє працівникам бути більш продуктивними, дозволяючи їх залишатися на зв'язку та працювати з корпоративними даними з будь-якої точки світу. Проте, ця революція мобільності породила комплексні та багатогранні виклики у сфері управління та кібербезпеки. Сучасна організація стоїть перед дилемою: як максимально використати переваги мобільності, не скомпрометувавши при цьому цілісність, конфіденційність та доступність критично важливих корпоративних даних.

Ключові слова: кібербезпека, управління, мобільні пристрої, BYOD

Стрімкий розвиток інформаційних технологій і тотальна мобільність робочої сили перетворили мобільні пристрої — смартфони, планшети, ноутбуки — на невід'ємний інструмент ведення бізнесу. Ключова проблема в управління мобільними пристроями полягає у необхідності встановити єдиний, надійний та гнучкий механізм контролю над усім різноманіттям мобільних кінцевих точок, що функціонують у мережі. Цей виклик посилюється явищем BYOD (Bring Your Own Device – використовуй власний пристрій), коли особисті гаджети співробітників отримують доступ до корпоративних ресурсів. У таких умовах розмивається межа між особистим та робочим простором, що створює значний ризик витоку даних, несанкціонованого доступу та інфікування корпоративної мережі шкідливим програмним забезпеченням. Традиційні методи захисту периметра стають неефективними перед такою децентралізації.

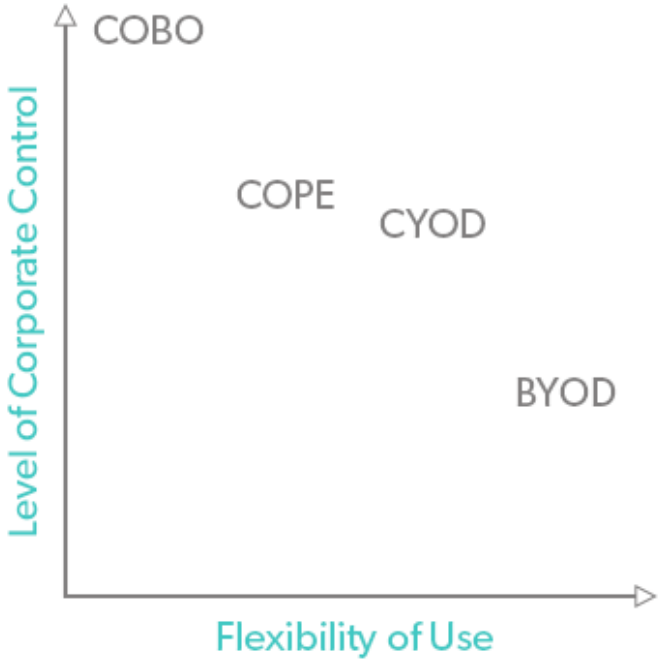

Рис. 1. Концепції використання мобільних пристроїв

Навіть у випадку використання корпоративних пристроїв (COPE – Corporate-Owned, Personally-Enabled) виникає потреба в балансі між безпекою та

зручністю користувача. Занадто суворі політики можуть викликати незадоволення персоналу та знизити продуктивність, тоді як послаблення контролю прямо веде до зростання вразливостей. Серед конкретних технічних та організаційних проблем слід виділити:

– забезпечення актуальності оновлень операційних систем та додатків; керування різними операційними системами (iOS, Android, Windows) з їх унікальними вимогами до безпеки;

– забезпечення відповідності нормативним вимогам, таким як GDPR чи HIPAA;

– необхідність віддаленого стирання даних у разі втрати або крадіжки пристрою.

– навчання персоналу основам кібергігієни, оскільки людський фактор часто є найслабшою ланкою в системі захисту.

Шляхи вирішення цієї комплексної проблеми лежать у площині стратегічного впровадження інтегрованих систем управління та багаторівневого підходу до безпеки. Фундаментом є впровадження спеціалізованих рішень для управління мобільними пристроями (Mobile Device Management, MDM) або, що більш прогресивно, уніфікованого управління кінцевими точками (Unified Endpoint Management, UEM).

Рішення UEM/MDM дозволяє централізовано застосовувати політики безпеки, незалежно від типу пристрою чи операційної системи. Це включає: примусове встановлення складних паролів та шифрування даних на пристрої; контроль над встановленням додатків та доступом до корпоративних ресурсів; віддалену конфігурацію параметрів мережі та пошти; а також функцію геозонування та віддаленого блокування або повного очищення даних у критичних ситуаціях.

Особлива увага має бути приділена методології управління, яка враховує специфіку використання. У сценаріях BYOD ключовим є концепція контейнеризації або розділення даних. Це означає створення захищеного, ізольованого робочого простору на особистому пристрої, який містить лише корпоративні дані та програми. Це дозволяє IT-відділу керувати та захищати виключно корпоративний сегмент, не втручаючись в особисте життя співробітника та не порушуючи його конфіденційності.

Перелік посилань:

5. Коцепції використання мобільних пристроїв – URL: https://www.datalinknetworks.net/dln_blog/barracudas-email-security-gateway-your-first-line-of-defense (дата звернення: 13.10.2025).

6. What is mobile device management (MDM)? – URL: https://www.techtarget.com/searchmobilecomputing/definition/mobile-device-management (дата звернення: 13.10.2025).

Карапиш Богдан Олегович
студент групи БСДМ-51, ННІКБЗІ ДУІКТ, Київ, Україна

БІЗНЕС-ЛОГІКА ЯК СЛІПА ЗОНА АВТОМАТИЗОВАНОГО АНАЛІЗУ: ПРАКТИЧНИЙ ПІДХІД ДО ТЕСТУВАННЯ ВЕБЗАСТОСУНКІВ

Що таке вразливості бізнес-логіки? Вразливості бізнес-логіки – це помилки в проєктуванні або реалізації прикладних систем, що дають змогу атакуючому експлуатувати штатну функціональність для досягнення небажаних результатів. Такі дефекти зазвичай виникають через хибні або неповні припущення про поведінку користувачів, про властивості бізнес-процесів чи про можливі проміжні стани додатку, а також через відсутність адекватних механізмів обробки нетипових ситуацій.

Ключові слова: бізнес-логіка, вразливості вебзастосунків, автоматизоване тестування, ручний пентестинг, моделювання загроз, логічні помилки.

Автоматизовані сканери покривають лише очікувані успішні сценарії, тому не виявляють бізнес-логічних вразливостей.

Атаки, спрямовані на бізнес-логіку API, становили 27% від загальної кількості атак у 2023 році, що на 10% більше, ніж у попередньому році [1]. Такі дефекти не є низькорівневими, як SQL-ін’єкції чи XSS, а виникають у моделі робочих процесів, зокрема через некоректні переходи між станами, відсутність перевірок ролей і транзакцій, можливість маніпуляцій параметрами, примусового обходу та перелічення ресурсів, змін на клієнтській стороні і ланцюгових ескалацій привілеїв [2]. Їхнє виявлення вимагає аналізу з урахуванням станів, декомпозиції робочих потоків і цілеспрямованого ручного пентестингу, що поєднує мислення атаки, моделювання загроз і тестування нетипових сценаріїв, а не лише запуск автоматичного інструменту.

Універсальної методології для тестування бізнес-логіки не існує, ефективність виявлення залежить від досвіду, технічної глибини та креативності пентестера.

Цей тип вразливості, як правило, один з найбільш важко виявлених, як правило, специфічний для конкретного додатка, але в той же час, як правило, один з найбільш руйнівних для цього додатку у разі його експлуатації. Класифікація недоліків бізнес-логіки вивчена недостатньо, хоча експлуатація бізнес-вразливостей часто зустрічається в реальних системах, і багато дослідників прикладних вразливостей займаються їх вивченням [3]. Тестування помилок бізнес-логіки схоже на тести, які використовуються функціональними тестувальниками, які фокусуються на логічному або кінцевому цільовому тестуванні. Ці типи тестів вимагають від фахівців безпеки дещо іншого мислення, розробки сценаріїв зловживань і нецільового використання, а також використання багатьох методів тестування. Автоматизація випадків зловживань

бізнес-логікою неможлива і залишається ручною працею, яка потребує навичок тестувальника та його знання всього бізнес-процесу та його правил.

Перелік посилань:

1. Imperva: State of API Security in 2024
[Електронний ресурс] – Режим доступу: https://www.imperva.com/blog/state-of-api-security-in-2024 (дата звернення: 21.10.202).

2. PortSwigger Web Security Academy: Вразливості бізнес-логіки
[Електронний ресурс] – Режим доступу: https://portswigger.net/web-security/logic-flaws (дата звернення: 22.10.2025).

3. OWASP WSTG: Вступ до тестування бізнес-логіки
[Електронний ресурс] – Режим доступу: https:/owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/10-Business_Logic_Testing/00-Introduction_to_Business_Logic (дата звернення: 22.10.2025).

Киркач М.Ю.
студент групи БСДМ-61, ННІКБЗІ ДУІКТ,
Київ, Україна

ТЕХНОЛОГІЇ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ НА БАЗІ РІШЕННЯ FORTIGATE

Сучасна корпоративна мережева інфраструктура стикається зі зростаючим обсягом цілеспрямова- них та складних кібератак. Використання застарілих рішень для захисту периметра більше не є достатнім. Ефективний захист вимагає впровадження інтегрованих, високоефективних технологій, здатних проводити аналіз трафіку на всіх рівнях, включаючи зашифрований. Рішення **FortiGate** представляє собою інноваційну платформу, яка поєднує функції міжмережевого екрана та розши- рені можливості безпеки.

FortiGate як ядро захисту: Маршрутизатор нового покоління:

FortiGate — це маршрутизатор нового покоління (NGFW), який кардинально відрізняє- ться від традиційних міжмережевих екранів. Він забезпечує не лише фільтрацію за портами та IP-адресами, але й глибоку інспекцію вмісту пакетів (Deep Packet Inspection, DPI) з високою про- дуктивністю завдяки використанню спеціалізованих процесорів (SPU).

Ключові технології FortiGate для захисту інфраструктури охоплюють кілька критично важли- вих областей. До них відноситься **Система запобігання вторгненням (IPS)**, яка запобігає екс- плуатації відомих вразливостей і блокує мережеві атаки в реальному часі, використовуючи актуаль- ні бази даних від FortiGuard Labs. Також важливим є **Контроль додатків (Application Control)**, що дає змогу ідентифікувати та керувати тисячами додатків на рівні L7, незалежно від використо- вуваного порту. Для боротьби зі шкідливим програмним забезпеченням реалізовано **Антивірус та Advanced Malware Protection**, а для виявлення прихованих загроз у шифрованому трафіку використовується функціонал **SSL Inspection** без

суттєвого падіння продуктивності.

Архітектурні рішення та інтеграція в Security Fabric

Ефективний захист досягається не лише через окремий пристрій, а через інтеграцію. FortiGate слу- гує центральним елементом концепції Fortinet Security Fabric, яка об’єднує всі рішення безпеки в єдину, автоматизовану систему.

Основою захисту є **внутрішня сегментація мережі (ISFW)**, де FortiGate використовується для створення мікросегментів усередині корпоративної мережі, що обмежує горизонтальне поши- рення (lateral movement) атаки. Це створює необхідну базу для реалізації політики **Zero Trust Network Access (ZTNA)**, де доступ надається лише після строгої перевірки. Крім того, FortiGate виступає як рішення **Secure SD-WAN**, що інтегрує мережеві функції та функції безпеки в єдину платформу. Це дозволяє компаніям захищати трафік філій та віддалених офісів, оптимізуючи при цьому використання смуги пропускання та підвищуючи стійкість з’єднанн

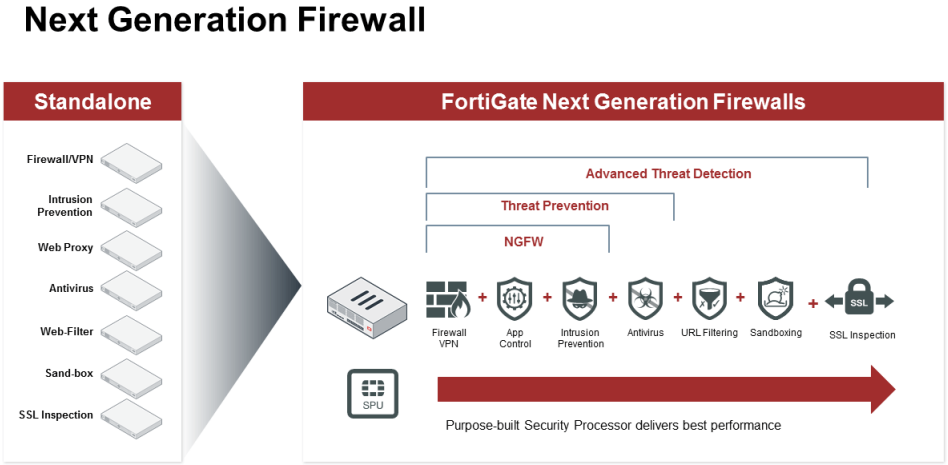

Рис. 1: Fortinet-NGF.

Автоматизація, моніторинг та реагування

Технології захисту FortiGate підтримуються механізмами автоматизації, необхідними для протидії сучасним швидким загрозам. Завдяки постійному оновленню інформації про загрози від Forti- Guard Labs Intelligence та інтеграції з FortiManager і FortiAnalyzer, система забезпечує централі- зоване управління та автоматизоване реагування на інциденти. Це включає автоматичну зміну політик безпеки у відповідь на виявлені загрози, що значно підвищує загальну швидкість протидії та ефективність кіберзахисту.

Перелік посилань:

[1] Fortinet, "FortiGate Next-Generation Firewall Capabilities, https://www.fortinet.com/products/next-generation-firewall

[2] Davies, R., "Implementing Zero Trust with Next-Generation Firewalls,"*International Journal of Network Security*, 2024.

[3] Fortinet, "Secure SD-WAN Solutions: Architecture and Implementation Guide,"2023.

Коврига Максим, студент УБДМ-61,
Легомінова С.В., Мужанова Т.М.
ННІКБЗІ, ДУІКТ, м. Київ, Україна

СТРАТЕГІЇ ЗАХИСТУ ВІД КІБЕРАТАК, ЩО СПОНСОРУЮТЬСЯ ДЕРЖАВАМИ

В умовах постійного зростання кількості і складності кіберзагроз з боку держав нагальною стає потреба забезпечення належного захисту державних установ і організацій, об’єктів критичної інфраструктури, бізнес-суб’єктів держав, які є потенційними мішенями зловмисників. Встановлено, що основні стратегії захисту охоплюють програмно-технічну сферу (впровадження архітектури поглибленого захисту, сегментація мереж, моніторинг загроз); організаційні заходи (проактивна оцінка ризиків і загроз, реагування на інциденти); нормативно-правові дії (унормування процесів виявлення і притягнення до відповідальності держав-агресорів); міжнародна співпраця й дипломатичні зусилля.

Кібератаки за підтримки держав стали серйозною проблемою для установ і організацій, особливо в урядовому секторі та секторі критичної інфраструктури. За останні роки національні держави розширили свої деструктивні кібероперації й постійно удосконалюють тактику, що робить їх щораз більш небезпечними.

Держави-кіберагресори тісно співпрацюють з фінансово мотивованими хакерами, проявляють зростаючий інтерес до проведення деструктивних атак і використання інструментів штучного інтелекту. Як свідчить статистика, у 2024 році 36% кібератак було організовано або здійснено державними суб’єктами, що може бути пов'язано з активними регіональними і глобальними конфліктами, а також із застосуванням кібератак для підтримки різних сторін конфліктів [1].

З огляду на обсяги і складність кібератак, що спонсоруються державами, а також їх серйозні наслідки для національної безпеки держав-мішеней основним завданням є забезпечення належного і всеохоплюючого захисту державних установ і організацій, об’єктів критичної інфраструктури, бізнес-суб’єктів тощо.

Огляд досліджень щодо протидії кібератакам за підтримки держав дозволив виділити ключові стратегії захисту, які поєднують зусилля як у галузі кібербезпеки, так і в правовому полі окремих держав, міждержавних об’єднань і міжнародного масштабу [2-4] (Рис. 1).

Для ефективного захисту від кібератак, що спонсоруються державами, необхідно проводити проактивну оцінку ризиків, на основі якої визначати пріоритетні заходи безпеки. Використовуючи можливості розвідки загроз, зокрема платформи обміну розвідувальними даними і обміну передовими практиками «полювання» на загрози, можна отримати уявлення про тактику, методи та процедури (TTP) організаторів кібернападів, а також зрозуміти їх поведінку й адаптувати оборонні стратегії для зменшення конкретних ризиків.

Основою ефективного кіберзахисту від кібератак, що спонсоруються державами, слугують надійні практики кібергігієни. Організації повинні регулярно впроваджувати оновлення програмного забезпечення, сегментацію мережі, засоби контролю доступу та безпечні конфігурації, щоб мінімізувати

поверхню атаки й мінімізувати вразливості. Навчання персоналу навичкам виявлення і протидії методам соціальної інженерії має вирішальне значення для зниження ризику людських помилок та зміцнення загальної кіберстійкості.

Рис. 1. Основні стратегії протидії кібератакам за підтримки держав

Впровадження архітектури поглибленого захисту, яка передбачає розгортання кількох рівнів забезпечення безпеки (фаєрволи, системи виявлення і запобігання вторгненням IDS/IPS, засоби антивірусного захисту, виявлення та реагування на загрози кінцевим точкам EDR, системи управління інформацією та подіями безпеки SIEM тощо), сприяє виявленню кіберзагроз і зменшенню їхніх негативних впливів на різних етапах життєвого циклу атаки.

Сегментація мережі є важливою для обмеження горизонтального руху зловмисника і стримування впливу потенційних порушень внаслідок кібератак, що спонсоруються державами. Сегментуючи мережі та забезпечуючи дотримання принципу найменших привілеїв, можна зменшити площу атаки й мінімізувати потенціал несанкціонованого доступу до критично важливих систем і конфіденційних даних.

Розробка і регулярне тестування планів реагування на інциденти є важливим для надання ефективної відповіді на кібератаки, ініційовані державами. Важливо встановити чіткі ролі й обов'язки, протоколи зв'язку та процедури ескалації, щоб забезпечити скоординоване та своєчасне реагування на кіберінциденти. Готуючись до різних сценаріїв, можна значно підвищити стійкість до кібератак.

Технології безперервного моніторингу і виявлення загроз, такі як системи IDS, EDR і платформи аналітики безпеки, мають вирішальне значення для виявлення ознак компрометації або зловмисної діяльності. Відстеження мережевого трафіку, активності кінцевих точок і поведінки користувачів у режимі реального часу дозволяє виявляти й реагувати на кіберзагрози за підтримки держав, перш ніж вони переростуть у серйозні інциденти безпеки.

Посилення безпеки ланцюга поставок є важливим для зменшення ризиків кібератак з ініціативи держав, спрямованих на сторонніх постачальників і підрядників. Організації повинні перевіряти й контролювати партнерів і сторонні організації щодо їхньої діяльності у сфері кібербезпеки та наявності вразливостей, впроваджувати заходи для перевірки цілісності й автентичності програмних та апаратних компонентів, а також встановлювати вимоги щодо дотримання вимог безпеки та готовності до реагування на інциденти в угодах.

Сьогодні в умовах глобального характеру кіберпростору безпрецедентно важливою є міжнародна співпраця та обмін інформацією за участі державних установ, підприємств, міжнародних організацій. Постійне партнерство в галузі кібербезпеки сприяє підвищенню ситуаційної обізнаності про загрози і координації зусиль щодо реагування на кібернапади, організовані державами. На міжнародному рівні основними напрямами протидії державам-кібератресорам є розробка міжнародних норм щодо взаємодії в кіберпросторі для сприяння відповідальній поведінці та стримування ворожих дій; дипломатичні зусилля для протидії кіберагресії, зниження напруженості та зміцнення довіри [4].

Розроблення чіткої політики кіберстримування та інформування про її положення всіх залучених сторін є важливим чинником перешкоджання зловмисній діяльності держав у кіберпросторі. Водночас, особливого значення набуває організація ефективних процесів атрибуції, тобто встановлення суб’єкта, який стоїть за кібератакою, та судово-медичного аналізу.

Забезпечення стійкості критичної інфраструктури та бізнес-операцій є важливим для пом'якшення впливу кібератак з боку держав і забезпечення безперервності операцій. Організації повинні розробляти надійні плани забезпечення безперервності бізнесу та відновлення після аварій, впроваджувати резервні системи і копії, механізми відновлення після збоїв, а також проводити регулярні навчання для перевірки готовності реагувати на кіберінциденти.

Готуючись до різних сценаріїв та пом'якшуючи потенційні збої, можна мінімізувати вплив кібератак, що спонсоруються державами, на свою діяльність і репутацію, тим самим підтримуючи безперервність бізнесу та зберігаючи довіру клієнтів перед обличчям динамічних кіберзагроз.

Отже, з огляду на масштабність і складність кібератак, що спонсоруються державами, захист від них вимагає комплексного та багаторівневого підходу, який поєднує технічні, організаційні, стратегічні заходи і є важливою передумовою посилення кіберстійкості установ, підприємств та організацій, захисту критичної інфраструктури і в підсумку - зменшення ризиків для кібербезпеки держави.

Перелік посилань:

1. 2025 Threat Landscape Report. *Cognyte.* 2025. URL: https://engage.cognyte.com/s/c8036aeb/?page=2
2. State-Backed Cyber Attacks: Insights and Solutions. *Searchinform* URL: https://searchinform.com/articles/cybersecurity/cyber-threats/cyber-attacks/state-sponsored-cyber-attacks/
3. Defending Against State-Sponsored Cyberattacks in 2025 *ISA Global Security Alliance.* 2025. URL: https://gca.isa.org/blog/defending-against-state-sponsored-cyberattacks-in-2025.
4. Decoding State-Sponsored Cyber Attacks. How Nation-States Wage War in the Digital Age. *Configr Technologies*. 2024. URL: https://configr.medium.com/decoding-state-sponsored-cyber-attacks-2f23f64ee439

Котецька В. І.
студентка групи УБДМ-61, ННІКБЗІ ДУІКТ,
Київ, Україна

СИСТЕМНИЙ ПІДХІД ДО ПОБУДОВИ SOC ДЛЯ МОНІТОРИНГУ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Системний підхід до побудови Security Operations Center (SOC) дозволяє ефективно моніторити ризики інформаційної безпеки на об'єктах критичної інфраструктури. Він включає моделювання загроз, проектування архітектури, впровадження технологій та організацію роботи аналітичної команди. Інтеграція IT та операційних технологій, застосування стандартів ISA/IEC 62443 та сучасних методів аналізу загроз забезпечує активне управління ризиками і підвищує стійкість критичних систем.

Ключові слова: критична інфраструктура, SOC, системний підхід, ризик.

Об'єкти критичної інфраструктури - це системи та активи, порушення або руйнування яких матиме катастрофічний вплив на національну безпеку, економіку та суспільство. В умовах зростання кіберзагроз, спрямованих на промислові системи управління (OT/ICS/SCADA), створення ефективного Security Operations Center (SOC), заснованого на системному підході, стає невід'ємною умовою забезпечення стійкості критичної інфраструктури та безперервності надання критичних послуг [1].

Системний підхід передбачає розгляд SOC як складної, адаптивної системи, що складається з взаємопов'язаних елементів між людиною, процесами та технологіями. Його головна перевага полягає у забезпеченні цілісного моніторингу ризиків, який охоплює IT-середовище та операційні технології.

Основним завданням SOC є не лише захист інформації, а передусім забезпечення безпеки виробничих процесів і запобігання можливій фізичній шкоді на об'єктах критичної інфраструктури. Важливою умовою ефективної роботи є інтеграція IT та OT систем, що дозволяє здійснювати комплексний аналіз загроз і потребує ретельної сегментації мереж та дотримання міжнародних стандартів безпеки, зокрема ISA/IEC 62443. Крім того, SOC повинен функціонувати у відповідності до національних та галузевих вимог щодо захисту критичної інфраструктури, дотримуючись всіх чинних регуляторних стандартів і правил [2].

Побудова та функціонування SOC для критичної інфраструктури здійснюється через взаємопов'язані етапи, що формують єдиний цикл управління ризиками. На початковому етапі, присвяченому стратегічному плануванню та моделюванню ризиків, визначається основа роботи SOC. Цей процес включає детальне моделювання загроз, характерних для конкретної галузі критичної інфраструктури. Особливу увагу приділяють ідентифікації всіх

активів, зокрема контролерів, інженерних станцій та мережевого обладнання, від яких залежить безперервність роботи систем. На підставі отриманих даних формуються сценарії виявлення загроз, орієнтовані на найбільш критичні ризики ОТ, такі як порушення цілісності команд або несанкціоновані зміни у конфігурації обладнання.

Наступний етап пов'язаний із проектуванням архітектури та розробкою процесів, де формується структура SOC, здатна забезпечувати високий рівень стійкості критичної інфраструктури. Впроваджується технологічний стек, що дозволяє ефективно обробляти великі обсяги даних з IT та ОТ. Основними компонентами є SIEM для централізованої кореляції подій, ОТ-спеціалізовані засоби пасивного моніторингу трафіку та SOAR для автоматизації процесів реагування на інциденти. Одночасно розробляються детальні плани реагування, які включають специфічні процедури стримування та відновлення ОТ-систем, що дозволяє мінімізувати вплив інцидентів на виробничі процеси.

На етапі впровадження, формування команди та постійного моніторингу відбувається технічна реалізація SOC. Встановлюються сенсори з мінімальним впливом на ОТ-системи та налаштовуються правила кореляції, що дозволяють пріоритезувати інциденти, які можуть загрожувати фізичній безпеці.

Паралельно формується та навчається команда аналітиків різних рівнів (Tier 1–3), які мають глибоке розуміння специфіки ОТ-протоколів. Після запуску SOC працює у режимі безперервного та проактивного управління ризиками, що включає реагування на інциденти, активне виявлення загроз, а також використання основних метрик часу виявлення та усунення загроз (MTTD/MTTR). Регулярні тренування сприяють постійному вдосконаленню процесів і підвищенню професійного рівня команди [3].

Системний підхід дозволяє SOC для критичної інфраструктури функціонувати як цілісна, послідовна система захисту, що ефективно інтегрує IT та ОТ-безпеку. Він переводить діяльність з оперативного усунення наслідків на завчасне управління ризиками, гарантуючи стійкість критично важливих національних систем. Успіх такого SOC вимірюється не лише кількістю виявлених інцидентів, але й збереженням безперервності, надійності та безпеки критичних операцій.

Перелік посилань:

1. Вимоги до управління ризиками безпеки критичної інфраструктури і категорії. URL: https://bdf.gov.ua/vymohy-do-upravlinnia-ryzykamy-bezpeky-krytychnoi-infrastruktury-i-katehorii/
2. Як побудувати та запустити центр безпеки (SOC). URL: https://oleg-dubetsky.medium.com/як-побудувати-та-запустити-центр-безпеки-soc-50f42b66cfa5f
3. SOC Frameworks: Principles, Comparison with Security Policies, Steps in Development, and Types. URL: https://eventussecurity.com/cybersecurity/soc/framework/

Кравцов С. С.
студент групи БСДМ-51, ННІЗІ ДУІКТ,
Київ, Україна

УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ ДЛЯ ЇХ ВИЯВЛЕННЯ ТА УСУНЕННЯ

Ефективне управління вразливостями є критично важливим з низки причин**.** Багато електронних пристроїв зберігають конфіденційну інформацію та мають доступ до неї. Їхній захист є ключовим для недопущення витоку, втрати або несанкціонованого доступу до даних. Платформа Tenable.SC у процеси інформаційної безпеки відкриває можливості для повноцінного безперервного моніторингу стану активів, контролю відповідності політикам безпеки та формування стратегій виправлення. **Ключові слова:** Управління вразливостями, сканування, виявлення, усунення, аналізування, моніторинг.

Для запобігання вразливості систем ефективним шляхом є використання сканеру вразливостей. Коли впроваджено сканер вразливостей, це означає, що в організації або системі налаштовано спеціальний інструмент, який автоматично перевіряє комп’ютери, сервери, мережеві пристрої, вебдодатки чи хмарні середовища на наявність вразливостей — тобто слабких місць, які можуть бути використані зловмисниками. (рис. 1). Такий підхід надає контроль та підвищує безпеку систем, де конфіденційність має критичне значення.

Рис. 1 – Порядок дій управління вразливостями

Попри стрімкий розвиток систем автоматизації безпеки, процес управління вразливостями залишається складним і ресурсоємним завданням. Виявлення та усунення вразливостей у великих інформаційних інфраструктурах потребує постійного моніторингу, аналізу ризиків і координації між підрозділами. На практиці навіть після первинного сканування часто залишається значна кількість неусунутих або невірно класифікованих вразливостей, що створює потенційні точки доступу для зловмисників. Додатковою проблемою є необхідність своєчасного оновлення баз знань про уразливості (наприклад, CVE, NVD), адже нові загрози з'являються щодня.

Проаналізувавши сучасні системи управління вразливостями, такі як Tenable.SC, Qualys VMDR та Rapid7 InsightVM, можна зробити висновок, що вони відрізняються глибиною аналітики, рівнем автоматизації та можливостями інтеграції з іншими інструментами кіберзахисту. Рішення Tenable.SC забезпечує централізований збір і кореляцію даних із різних джерел, дозволяє створювати гнучкі політики сканування й відстеження усунення вразливостей у динаміці. Натомість Qualys VMDR робить акцент на автоматичному пріоритезуванні ризиків, що дає змогу ефективніше розподіляти ресурси між критичними та низькорівневими загрозами.

У результаті аналізу запропоновано гібридний підхід до управління вразливостями, який поєднує регулярне автоматизоване сканування з аналітичною оцінкою ризиків на основі контексту середовища. Такий підхід дозволяє зменшити кількість хибнопозитивних результатів, прискорити процес усунення вразливостей і підвищити загальний рівень кіберстійкості організації. Найважливіші активи (сервери з критичними даними, облікові записи адміністраторів) перевіряються з максимальною частотою, тоді як менш критичні елементи інфраструктури проходять планові сканування відповідно до політик безпеки (рис. 1). Це забезпечує баланс між точністю, продуктивністю та безпекою.

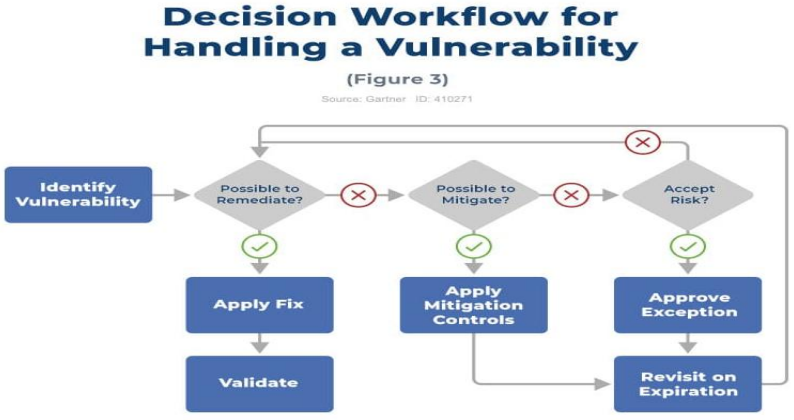

Рис. 2 – Процес управління вразливостями(виявлення, оцінка, усунення або пом’якшення ризику.)

Результати практичного застосування гібридного підходу до управління вразливостями показали, що завдяки автоматизації процесів виявлення та пріоритезації ризиків загальний час реагування скорочується у 2–3 рази порівняно з ручними методами. При цьому рівень захищеності системи суттєво підвищується, а кількість критичних невиправлених вразливостей зменшується до мінімуму. Для більшості корпоративних мереж така оптимізація є прийнятним компромісом між швидкістю та якістю безпекових процесів. Особливо це актуально для фінансових організацій, державних установ та медичних закладів, де час реагування має вирішальне значення.

Таким чином, впровадження систем управління вразливостями (зокрема на базі Tenable.SC) є одним із найбільш ефективних напрямів розвитку кіберзахисту сучасних підприємств. Такі рішення дають змогу забезпечити повний цикл управління вразливостями — від автоматичного сканування до контролю усунення знайдених ризиків. Це знижує імовірність несанкціонованого доступу до критичних ресурсів і дозволяє створити проактивну модель кіберзахисту, яка здатна адаптуватися до нових загроз у режимі реального часу.

Подальші дослідження мають бути спрямовані на підвищення точності виявлення та зменшення кількості хибнопозитивних результатів, а також на інтеграцію сканерів у комплексні системи моніторингу безпеки (SIEM, SOAR). Це дозволить підвищити рівень автоматизації реагування на інциденти та знизити навантаження на аналітиків з інформаційної безпеки.

Перелік посилань:

3. Vulnerability Management with Tenable.sc / Tenable, Inc. [Електронний ресурс] – Режим доступу: https://www.tenable.com/products/tenable-sc
4. Rapid7 InsightVM – Advanced Vulnerability Management Platform / Rapid7. [Електронний ресурс] – Режим доступу: https://www.rapid7.com/products/insightvm
5. Qualys VMDR: Continuous Vulnerability Detection / Qualys. [Електронний ресурс] – Режим доступу: https://www.qualys.com/vmdr

Крикун Ю.В.
студентка групи ТСДМ-62 ННІТ ДУІКТ,
Київ, Україна

КРИПТО-БІОМЕТРИЧНА МОДЕЛЬ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ: БАЛАНС АНОНІМНОСТІ ТА АВТЕНТИЧНОСТІ

Що ми розуміємо під безпекою виборчого процесу в цифрову епоху? В умовах інформатизації суспільства та постійного розвитку інформаційних технологій, питання забезпечення довіри, безпеки та конфіденційності в електронному голосуванні (ЕГ) стали надзвичайно актуальними. ЕГ має

потенціал суттєво спростити процес участі громадян, проте його впровадження пов'язане з ризиками, які загрожують як коректності голосування (фальсифікація), так і захисту особистих даних виборців. Основною вимогою до демократичного ЕГ є одночасне гарантування автентичності (голосує лише уповноважений виборець) та анонімності (неможливо зв'язати голос із виборцем).

Ключові слова: електронне голосування, сліпий підпис, біометрична автентифікація, анонімність, криптографія, безпека, довіра.

Основна складність для сучасних систем електронного волевиявлення полягає у необхідності збалансувати ідентифікацію виборця (для запобігання множинному голосуванню) та його конфіденційність (для збереження свободи волевиявлення). Традиційні системи, які поєднують ідентифікаційні дані та голос у централізованій базі, є вразливими до компрометації.

Для вирішення проблеми конфлікту між автентичністю та анонімністю, пропонується концептуальна модель системи електронного голосування (ЕГ). Ця модель використовує гібридну архітектуру, що розмежовує процеси ідентифікації та волевиявлення шляхом інтеграції двох ключових технологій.

На етапі допуску до голосування використовується біометрична автентифікація (відбитки пальців, обличчя) для високоточного встановлення особи виборця. Це не лише підвищує рівень безпеки у порівнянні з традиційними паролями, але й гарантує, що участь у виборах беруть лише авторизовані користувачі, підтримуючи принцип "один виборець – один голос".[1]

Після успішної автентифікації, для анонімізації самого голосу застосовується схема «Сліпого підпису» (Blind Signature). Виборець «засліплює» свій бюлетень (шифрує його унікальним фактором) перед тим, як надсилає його до виборчого органу для підписання. Орган підтверджує, що бюлетень є дійсним, але не бачить його змісту і, що найважливіше, не може відстежити унікальний фактор засліплення. Це виключає можливість прив'язки біометричних даних, використаних для входу, до кінцевого анонімного голосу.

Технологія	Основна Функція у Системі	Забезпечуваний Принцип	Механізм Захисту
Біометрична Автентифікація	Контроль доступу та ідентифікація виборця.	Автентичність (Хто голосує).	Запобігання множинному/неавторизованому голосуванню.
Криптографічний «Сліпий Підпис»	Анонімізація та завірення бюлетеня.	Анонімність (За що проголосовано).	Виключення зв'язку між ідентифікатором виборця та його вибором.
AES/RSA	Шифрування даних.	Цілісність та Конфіденційність.	Захист даних від перехоплення та несанкціонованої зміни.

Робота демонструє, що інтеграція цих методів дозволяє ефективно вирішити проблему анонімності, зберігаючи при цьому автентичність.

Розмежування процесів: Система забезпечує суворе розмежування між модулем автентифікації (який обробляє біометричні дані) та модулем голосування (який обробляє сліпі підписи). Цей архітектурний поділ запобігає створенню єдиного журналу, що містить ідентифікатор виборця та його вибір.

Криптографічна Стійкість: Для забезпечення цілісності та конфіденційності даних голосування використовуються сучасні криптографічні алгоритми (RSA для «сліпого підпису» та AES для шифрування даних). Дані голосування зберігаються у зашифрованому вигляді, що гарантує їхню цілісність та захист від несанкціонованого доступу.[3]

Проведене моделювання та тестування ключових компонентів підтвердило, що система здатна стабільно функціонувати навіть за високих навантажень, забезпечуючи коректну обробку голосів та їх захист від фальсифікації.

Результати дослідження підтверджують, що гібридна крипто-біометрична модель є ефективним і надійним рішенням для модернізації виборчих процесів. Анонімність, прозорість і захист даних є ключовими аспектами, які підсилюють довіру виборців до чесності та неупередженості виборів.

Система також демонструє потенціал для адаптації в різних сферах, де необхідні безпечні та анонімні опитування чи голосування (корпоративні вибори, громадські організації). [2]

Подальші дослідження можуть бути спрямовані на оптимізацію продуктивності системи, удосконалення алгоритмів захисту від нових типів кібератак та аналіз етичних і правових викликів, пов’язаних із впровадженням біометрії у національних масштабах. [4]

Перелік посилань:

1. Election Cybersecurity: Emerging Trends / Lisa D. Nelson / 2019 р. (дата звернення: 08.10.2024)
2. Blind Signatures for Untraceable Payments / David Chaum / Advances in Cryptology / 2017 р. (дата звернення: 01.11.2024)
3. Introduction to Electronic Voting / David Chaum, Ronald Rivest / 2018 р. (дата звернення: 10.11.2024)
4. Security of Electronic Voting Systems / Aggelos Kiayias, Moti Yung / 2020 р. (дата звернення: 11.11.2024)

Литвинюк Владислав Вадимович
Студент групи БСДМ-52, ННІКБЗІ ДУІКТ, Київ, Україна

АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ. ЗАГРОЗИ В ХМАРНИХ СЕРЕДОВИЩАХ

Масовий перехід бізнесу та державних установ на використання хмарних технологій зумовив появу нових комплексних загроз кібербезпеці. Хмарні середовища, пропонуючи масштабованість, гнучкість та економічність, одночасно стають привабливою мішенню для кіберзлочинців через централізацію даних та ускладненість архітектури. Основними ризиками є несанкціонований доступ до даних, втрата контролю над інформацією, атаки на віртуальну інфраструктуру та наслідки неправильної конфігурації безпеки. Протидія цим загрозам вимагає комплексного підходу, що поєднує передові технології захисту, чіткі протоколи безпеки та підвищення кваліфікації фахівців.

Ключові слова: хмарна безпека, кіберзагрози, конфігурація, несанкціонований доступ, модель спільної відповідальності.

Хмарні обчислення стали фундаментом цифрової трансформації, однак їх динамічна та розподілена природа відкриває нові вектори для атак. За даними компанії SentinelOne (2024), близько 82 % інцидентів у хмарних середовищах пов’язані з людським фактором, зокрема помилками конфігурації та управління доступом, а не з вразливістю самих платформ [1].

Це підкреслює критичну важливість людського фактору та управління конфігурацією. Модель спільної відповідальності, де провайдер хмарних послуг забезпечує безпеку самої хмари, а клієнт відповідає за безпеку у хмарі — тобто за налаштування правил доступу, захист даних і контроль користувачів — є ключовою для розуміння розподілу ризиків [2, с. 15–18].

Однією з найпоширеніших загроз залишається неправильна конфігурація безпеки. Ненавмисне відкриття публічного доступу до сховищ даних, таких як S3-бакети в AWS або Blob-контейнери в Azure, регулярно призводить до масштабних витоків конфіденційної інформації. Дослідження компанії Palo Alto Networks (Unit 42) (2024) показало, що 65 % досліджених хмарних сховищ були сконфігуровані з порушенням базових принципів безпеки [3].

Для боротьби з такими ризиками застосовуються інструменти автоматизованого сканування конфігурацій (CSPM), які безперервно моніторять середовище на відповідність політикам безпеки та своєчасно сигналізують про виявлені проблеми.

Складність становлять і атаки на віртуальну інфраструктуру, зокрема side-channel attacks, коли зловмисник, розміщуючи свій віртуальний сервер на тому ж фізичному хості, що й жертва, намагається отримати несанкціонований доступ до даних. Хоча провідні провайдери впроваджують ізоляційні механізми, зокрема AWS Nitro System, загроза залишається актуальною для менш захищених середовищ.

Крім того, поширеним явищем є атаки на інтерфейси управління хмарою. Через слабкі облікові дані або відсутність багатофакторної автентифікації (MFA) зловмисники можуть отримати повний контроль над інфраструктурою клієнта. Тому необхідно неухильно дотримуватися принципу найменших привілеїв (PoLP) та впроваджувати MFA для всіх облікових записів, особливо адміністративних [4, с. 92].

Інсайдерські загрози в хмарних середовищах мають особливо високий потенційний збиток. Колишні співробітники або зловмисні адміністратори, які зберігають доступ до облікових записів, можуть експортувати або пошкодити критичні дані. Для запобігання таким інцидентам необхідно впроваджувати сувору політику найму та звільнення, застосовувати принцип найменших привілеїв (PoLP) для користувачів і сервісів, а також забезпечувати ретельне логування та моніторинг усіх дій за допомогою SIEM-систем.

Регулярні аудити доступу дозволяють своєчасно виявляти зайві або неактивні облікові записи. Важливо розуміти, що в хмарному середовищі логування є не просто рекомендацією, а критичною необхідністю. Без повного

аудиту-трейлу визначити джерело атаки або масштаби порушення стає практично неможливо.

Зростання популярності контейнеризації (Docker, Kubernetes) та serverless-архітектур породжує новий клас вразливостей. Загрози, пов’язані з використанням небезпечних образів контейнерів, вразливими налаштуваннями оркестрації Kubernetes або сервісами типу Function-as-a-Service (FaaS), вимагають застосування спеціалізованих інструментів безпеки — SAST, DAST та сканерів контейнерів. Дослідження показують, що понад 50 % образів у публічних репозиторіях містять критичні вразливості [4].

У результаті безпека сучасного хмарного середовища має починатися ще на етапі розробки застосунків (DevSec) і потребує інтеграції контролю безпеки в процес розгортання та супроводу програмного забезпечення — підхід DevSecOps.

Враховуючи складність і динамічність загроз, стає очевидним, що безпека хмарних середовищ — це безперервний і багаторівневий процес, а не разовий захід. Ефективний захист не може ґрунтуватися на одному рішенні; він базується на поєднанні технічних засобів (CSPM, CWPP, MFA, шифрування), чітких організаційних процедур і постійного навчання персоналу. Міжнародні стандарти, зокрема ISO/IEC 27017, надають практичні рекомендації щодо впровадження заходів безпеки, допомагаючи організаціям створювати довірене хмарне середовище.

Розвиток хмарної безпеки в майбутньому буде тісно пов’язаний із впровадженням штучного інтелекту та машинного навчання для проактивного виявлення аномалій, аналізу поведінки користувачів і сервісів (UEBA) та автоматизації реагування на інциденти.

Перелік посилань:

1. SentinelOne. *Cloud Security Statistics — 82 % of cloud misconfigurations stem from human error.* 2024. URL: (https://www.sentinelone.com/cybersecurity-101/cloud-security/cloud-security-statistics/)

2. Mather T., Kumaraswamy S., Latif S. Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. O'Reilly Media, 2009.

3. Unit 42. Cloud Threat Report, 2H 2024. Palo Alto Networks. URL: (https://start.paloaltonetworks.com/rs/531-OCS-018/images/4.13PM_unit42-cloud-threat-report-volume7-final.pdf)

4. Rhoton J., Haukioja R. Cloud Security Auditing: A Handbook for Auditing Cybersecurity in the Modern Enterprise. Springer, 2023.

Ломовацький О.В
студент групи БСДМ-61, ННІКБЗІ ДУІКТ,
Київ, Україна

ТЕХНОЛОГІЯ ТЕХНІЧНОГО АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СЕРВЕРІВ ТА РОБОЧИХ СТАНЦІЙ КОРИСТУВАЧІВ В СЕРЕДОВИЩІ WINDOWS

У тезі розглядається методологічна основа для проведення технічного аудиту безпеки в корпоративних середовищах Windows. Наголошено на недостатності реактивних заходів та важливості переходу до проактивного управління ризиками. Запропоновано структурований життєвий цикл

аудиту, що охоплює планування, технічну оцінку, аналіз ризиків та звітування. Проаналізовано ключові стандарти, такі як CIS Benchmarks та NIST CSF, як об'єктивні критерії оцінки [1, 2]. Описано критичні зони фокусування, зокрема Active Directory та GPO, та підкреслено необхідність переходу до моделі безперервного моніторингу [3, 4].

Ключові слова: аудит безпеки, Windows, Active Directory, CIS Benchmarks, NIST CSF, GPO.

У сучасному ландшафті кіберзагроз корпоративні інфраструктури на базі Microsoft Windows є постійною мішенню [3]. Реактивних заходів стає недостатньо, тому систематичний технічний аудит безпеки є фундаментальною опорою кіберзахисту. Його мета – не лише виявлення вразливостей, але й перевірка відповідності стандартам та формування дорожньої карти для переходу до проактивного управління ризиками.

Ефективний аудит – це структурований життєвий цикл, що починається з Планування (визначення цілей та обсягу) та Збору інформації (аналіз документації, інтерв'ю). Ядром є Технічна оцінка (сканування на вразливості, тестування на проникнення, аналіз конфігурацій) та Аналіз ризиків, що надає бізнес-контекст виявленим вразливостям. Процес завершується Звітуванням (пріоритезовані рекомендації) та Подальшим контролем для перевірки впровадження виправлень.

Для об'єктивності, оцінка повинна проводитися не на основі суб'єктивних уявлень, а відповідно до загальновизнаних стандартів та кращих практик[1, 2]. CIS Benchmarks виступають де-факто кращими практиками для технічного "гарденінгу" (посилення захисту) конфігурацій, надаючи детальні профілі налаштувань (наприклад, вимоги до паролів) [1]. У свою чергу, NIST Cybersecurity Framework (CSF) надає високорівневу стратегічну рамку, яка структурує зусилля з кібербезпеки за п'ятьма функціями: Ідентифікація, Захист, Виявлення, Реагування та Відновлення [2]. Ці фреймворки синергетичні: NIST CSF визначає "Що робити?", а CIS – "Як саме налаштувати?" [1, 2].

Інструментарій аудитора поєднує вбудовані засоби (журналювання подій Windows), комерційні та відкриті сканери (наприклад, Nessus, OpenVAS) та PowerShell. Останній є найпотужнішим інструментом для глибокого, кастомізованого та масштабованого аудиту, дозволяючи автоматизувати перевірки конфігурацій, аналізувати журнали та опитувати Active Directory.

Аудит має пріоритетно фокусуватися на критичних зонах та векторах високого ризику.

1. Active Directory (AD). Як "ключі від королівства", AD є головною ціллю [3]. Аудит повинен цілеспрямовано шукати вразливості, що уможливлюють поширені атаки, такі як Kerberoasting, Password Spraying та Pass-the-Hash [3].

2. Об'єкти групової політики (GPO). GPO є двосічним мечем: це потужний інструмент управління, але й небезпечний вектор атаки [4]. Зловмисник, який отримав права на редагування GPO, може одночасно скомпрометувати тисячі

систем. Тому аудит дозволів на GPO є настільки ж критичним, як і безпека контролерів домену [4].

Кінцевий звіт з аудиту має перетворювати технічні дані на дієву інформацію, з чітким резюме для керівництва та пріоритезованими, ризик-орієнтованими рекомендаціями. Роль аудитора – бути "перекладачем" технічного ризику на мову бізнесу, щоб забезпечити ресурси для виправлення.

Таким чином, комплексний аудит є незамінним стратегічним процесом. Кінцевою метою зрілої програми безпеки є перехід від моделі періодичних перевірок до культури безперервного моніторингу та автоматизованої валідації стану безпеки.

Перелік посилань:

1. CIS Benchmarks. Center for Internet Security (CIS). URL: https://www.cisecurity.org/cis-benchmarks (дата звернення: 21.10.2025).

2. NIST Cybersecurity Framework (CSF). National Institute of Standards and Technology. URL: https://csrc.nist.gov/projects/cybersecurity-framework (дата звернення: 21.10.2025).

3. Active Directory Attack Methods. Lepide. URL: https://www.lepide.com/blog/top-10-active-directory-attack-methods/ (дата звернення: 21.10.2025).

4. Group Policy as an Attack Pathway. Practical 365. URL: https://practical365.com/group-policy-as-an-attack-pathway/ (дата звернення: 21.10.2025).

Мельниченко Н. М.
Студента групи УБДМ-61, ННІКБЗІ ДУІКТ,
Київ, Україна

Методика перевірки ефективності засобів протидії інсайдерським загрозам під час внутрішнього аудиту інформаційної безпеки

У тезі розглянуто методику перевірки ефективності засобів протидії інсайдерським загрозам під час проведення внутрішнього аудиту інформаційної безпеки в організаціях. Визначено сутність інсайдерських ризиків, їх вплив на інформаційні ресурси та значення системного підходу до оцінювання рівня захисту. Описано основні етапи методики, що включають аналіз політик доступу, аудит технічних і організаційних заходів, перевірку систем моніторингу та навчання персоналу. Наголошено на необхідності комплексного оцінювання ефективності впроваджених заходів, формування обґрунтованих рекомендацій та підвищення рівня зрілості системи інформаційної безпеки. Застосування методики дозволяє підвищити надійність корпоративного захисту, мінімізувати вплив людського фактору та забезпечити стабільність функціонування інформаційного середовища підприємства.

Ключові слова: інсайдерські загрози, внутрішній аудит, інформаційна безпека.

На теперішній час, загрози з боку внутрішніх осіб (інсайдерів) є однією з критичних проблем, що постають перед захистом інформаційних активів підприємств. Ситуація ускладнюється тим, що дії цих осіб — працівників, консультантів чи контрагентів, які мають легітимний доступ до внутрішніх IT-систем, — складніше виявити та попередити, аніж зовнішні кібератаки. Інсайдерські дії можуть бути як свідомими (саботаж, розкрадання інформації, промислове шпигунство), так і ненавмисними (нехтування правилами, помилки

у роботі) [1, с. 177]. З огляду на це, при проведенні внутрішньої ревізії інформаційного захисту необхідно приділяти особливе значення оцінці того, наскільки ефективно функціонують механізми попередження інсайдерських ризиків.

Системний підхід є основою методології оцінки ефективності таких механізмів, охоплюючи аналіз адміністративних, технологічних та людських факторів безпеки. Першим кроком є детальна перевірка існуючих політик ІБ: правил контролю доступу, процедур реєстрації облікових записів, розподілу повноважень і ролей, а також регламенту дій при звільненні співробітників чи зміні їхніх функціональних обов'язків. Чітко визначена та актуальна політика доступу є базисом для успішної протидії зловживанням інсайдерів. Під час ревізії обов'язково встановлюється, чи виконуються ці положення на практиці, як часто проводиться інвентаризація прав доступу, і чи існують оперативні процедури анулювання доступу для осіб, які змінюють посаду чи припиняють роботу в організації.

Другим важливим кроком аудиту полягає у вивченні систем реєстрації подій та моніторингу активності користувачів. Інструменти нагляду (зокрема, DLP-рішення, SIEM-системи, платформи для аналізу поведінки) повинні забезпечувати консолідацію та кореляцію інформації з різних джерел. Це дозволяє вчасно ідентифікувати підозрілі дії. Аудиторська перевірка повинна визначити, наскільки повноцінно охоплені найкритичніші інформаційні потоки, чи налаштовано системи на виявлення аномалій у звичній поведінці персоналу, і чи регулярно відбувається аналіз накопичених журналів безпеки. Не менш важливо перевірити наявність задокументованих інструкцій щодо реагування на інциденти, виявлені даними системами, та фіксацію дій відповідального персоналу [2, с. 56].

Оцінка функціональності технологічних засобів, що протидіють інсайдерським загрозам є третім кроком. До нього належать засоби обмеження використання зовнішніх накопичувачів, шифрування даних, системи контролю доступу до файлових ресурсів, інструменти мережевого моніторингу та механізми автентифікації. В процесі аудиту перевіряється узгодженість роботи цих засобів, відсутність «сліпих зон» у захисному контурі та їх відповідність галузевим стандартам (NIST SP 800-53, ISO/IEC 27001 тощо). Також аудиту підлягає якість управління оновленнями програмного забезпечення та патч-менеджмент, оскільки застаріле ПЗ може стати прогалиною в захисті навіть за наявності сучасних контролів.

Особлива увага в рамках аудиторської методики приділяється фактору людської поведінки. Навіть найдосконаліші технології безсилі, якщо співробітники не бажають або не здатні дотримуватися правил безпеки. Тому аудит передбачає оцінку рівня обізнаності персоналу у питаннях ІБ, аналіз результатів навчальних курсів та тестувань, а також вивчення наявності програм підвищення загальної культури безпеки. Ключовим індикатором успішності є не

лише сам факт проведення таких заходів, але й їх систематичність та орієнтація на практичні навички. Формування рекомендацій та узагальнення знахідок є фінальною частиною методології. Аудитор готує звіт, де деталізуються слабкі та сильні сторони системи захисту від інсайдерів, оцінюється рівень зрілості системи безпеки та встановлюються пріоритети вдосконалення. Рекомендації мають бути прагматичними, конкретними та реалістичними, враховуючи наявні ресурси підприємства. Важливо, щоб висновки аудиту слугували не просто документуванням поточного стану, а стали основою для постійного розвитку системи управління ІБ [3, с. 87].

Враховуючи все вище сказане, методологія перевірки ефективності інструментів протидії інсайдерським загрозам є критично важливим елементом внутрішнього аудиту та системи управління інформаційною безпекою загалом. Її всебічний характер дозволяє виявити не тільки технічні вразливості, але й прогалини в організаційних процедурах та людські ризики. Впровадження цієї методики підвищує довіру до внутрішньої інфраструктури, допомагає мінімізувати потенційні збитки від інцидентів з інсайдерами, та сприяє становленню міцної корпоративної культури безпеки. Застосування системного підходу забезпечує неупередженість оцінки, підтримку управлінського процесу та здатність організації адекватно реагувати на актуальні виклики у сфері захисту даних.

Перелік посилань:

1. INSIDERS AND INSIDER INFORMATION: ESSENCE, THREATS, ACTIVITIES AND LEGAL RESPONSIBILITY / S. Shevchenko et al. Cybersecurity: Education, Science, Technique. 2022. Vol. 3, no. 15. P. 175–185. URL: https://doi.org/10.28925/2663-4023.2022.15.175185
2. TECHNOLOGIES OF USER ACTIVITIES MONITORING AND ANALYSIS IN PREVENTING INSIDER THREATS OF INFORMATION SECURITY OF AN ORGANIZATION / T. Muzhanova et al. Cybersecurity: Education, Science, Technique. 2021. Vol. 1, no. 13. P. 50–62. URL: https://doi.org/10.28925/2663-4023.2021.13.5062
3. Єршова Н., ЖЕНЬ В. Оцінювання ефективності персоналу: методичний підхід та практична реалізація. Acta Academiae Beregsasiensis. Economics. 2025. № 10. С. 84–96. URL: https://doi.org/10.58423/2786-6742/2025-10-84-96

Опалько І.Б.
Студент групи БСДМ-62, ННІКБЗІ, ДУІКТ
Київ, Україна

ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНИХ РЕСУРСІВ ОРГАНІЗАЦІЇ НА ОСНОВІ РІШЕНЬ SASE

У роботі розглянуто сучасні підходи до забезпечення безпеки інформаційних ресурсів організації на основі архітектури Secure Access Service Edge (SASE). Проаналізовано передумови виникнення цієї технології, її ключові компоненти — SD-WAN, SWG, CASB, ZTNA, FWaaS — та принципи інтеграції в єдину хмарно орієнтовану платформу. Визначено основні переваги застосування SASE для корпоративного середовища, зокрема підвищення рівня безпеки при віддаленому доступі, уніфікацію політик безпеки та оптимізацію мережевих процесів. Окрему увагу приділено проблемам впровадження, викликам масштабування й перспективам розвитку архітектури SASE у контексті концепції Zero Trust.

Ключові слова: кібербезпека, Zero Trust, SASE, безпека мереж.

Традиційні моделі побудови корпоративної безпеки ґрунтувалися на принципі периметрового захисту: основна увага приділялася контролю доступу всередині локальної мережі підприємства, тоді як зовнішні з'єднання вважалися менш довіреними. Проте з поширенням віддаленої роботи, використанням хмарних сервісів і мобільних пристроїв та активним переходом бізнесу до моделей "anywhere workforce" ця парадигма перестала бути ефективною. Інформаційні ресурси організацій дедалі частіше розміщуються за межами корпоративного центру обробки даних, а користувачі отримують доступ до них з різних географічних точок і з різним рівнем довіри.

Така розподіленість створює нові виклики: традиційні VPN-з'єднання перевантажують інфраструктуру, ускладнюють моніторинг трафіку та не відповідають вимогам гнучкості, які диктує сучасний бізнес. Крім того, класичні міжмережеві екрани та шлюзи безпеки не здатні ефективно контролювати доступ до SaaS-додатків, хмарних платформ і віддалених користувачів.

У відповідь на ці виклики у 2019 році аналітична компанія Gartner сформулювала концепцію SASE (Secure Access Service Edge) як нову модель конвергенції мережевих та безпекових функцій. Її мета — забезпечити безпечний, уніфікований і масштабований доступ до корпоративних ресурсів незалежно від місцезнаходження користувача або пристрою. Технологія SASE поєднує в собі функції маршрутизації, фільтрації, контролю доступу та моніторингу в єдиній хмарній інфраструктурі. Її архітектура базується на п'яти основних компонентах, які інтегруються в рамках одного сервісу [1].

Першим компонентом є SD-WAN (Software-Defined Wide Area Network) — технологія віртуального мережевого з'єднання, що забезпечує інтелектуальне маршрутування трафіку між користувачами, філіями та центрами обробки даних. Завдяки SD-WAN можна зменшити затримки, підвищити стабільність з'єднання та оптимізувати пропускну здатність без необхідності у складних VPN-тунелях.

Другим елементом є SWG (Secure Web Gateway) — безпечний веб-шлюз, який забезпечує фільтрацію HTTP/HTTPS-трафіку, виявлення шкідливого програмного забезпечення, контроль доступу до веб-ресурсів і запобігання витоку даних. SWG дозволяє централізовано реалізовувати політики веб-безпеки для всіх користувачів незалежно від їхнього місцезнаходження.

Третім компонентом виступає CASB (Cloud Access Security Broker) — брокер безпеки для хмарних сервісів. Він здійснює контроль за використанням SaaS-додатків (наприклад, Microsoft 365, Salesforce, Google Workspace), відстежує передачу даних і блокує підозрілі дії. CASB також допомагає забезпечити відповідність нормативним вимогам і політикам конфіденційності.

Четвертим елементом є ZTNA (Zero Trust Network Access) — механізм доступу на основі принципу "нікому не довіряй за замовчуванням". Замість того, щоб надавати користувачеві повний доступ після автентифікації, ZTNA перевіряє кожну сесію окремо, враховуючи контекст — пристрій, місцезнаходження, час і рівень ризику. Це дозволяє мінімізувати наслідки компрометації облікових даних і забезпечити динамічне застосування політик.

П’ятий компонент — FWaaS (Firewall as a Service) — хмарний міжмережевий екран, який забезпечує фільтрацію трафіку, виявлення вторгнень і моніторинг подій безпеки на рівні мережі. На відміну від класичних фаєрволів, FWaaS не потребує апаратного забезпечення й забезпечує масштабування під навантаження організації [2].

Переваги архітектури SASE полягають у гнучкості, масштабованості та уніфікації процесів безпеки. Вона знижує кількість розрізнених пристроїв безпеки, зменшує складність підтримки та дозволяє швидко впроваджувати оновлення. Крім того, використання хмарних рішень SASE забезпечує високу доступність і глобальне покриття, що особливо важливо для міжнародних компаній із розподіленими командами [3].

Архітектура SASE є одним із найперспективніших напрямів розвитку корпоративної кібербезпеки, що поєднує мережеві та захисні функції в єдиному хмарному середовищі. Вона дозволяє організаціям створити універсальну модель захисту, здатну масштабуватися разом із бізнесом і підтримувати концепцію безпечного доступу з будь-якої точки. Завдяки централізованому керуванню, автоматизації політик і глибокій інтеграції з Zero Trust Architecture рішення SASE створюють новий стандарт корпоративної безпеки. Отже, впровадження технології SASE дає змогу організаціям перейти від фрагментованих засобів захисту до цілісної, керованої платформної екосистеми, де безпека стає невід’ємною частиною самої мережевої інфраструктури [4].

Перелік посилань:

1. Gartner, Inc. *The Future of Network Security Is in the Cloud.* Gartner Report, 2019.
2. Bhardwaj A., Kumar P. *Secure Access Service Edge (SASE): Architecture, Components, and Security Capabilities.* IEEE Access, Vol. 11, 2023, pp. 10574–10589.
3. Palo Alto Networks. *The Ultimate Guide to SASE.* Technical Whitepaper, 2024.
4. Cisco Systems. *Integrating Zero Trust and SASE for Modern Enterprise Security.* Cisco Press, 2024.

Педосенко Богдан Володимирович
студент групи БСДМ-62, ННІКБЗІ, Київ, Україна

ТЕХНІЧНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

У сучасному цифровому суспільстві інформація стала одним із найцінніших ресурсів. Вона визначає конкурентоспроможність компаній, ефективність управління державою, безпеку критичної інфраструктури та навіть політичну стабільність. Водночас інформаційні ресурси стають об’єктом постійних кібератак, спроб несанкціонованого доступу, маніпулювання або знищення. Саме тому створення ефективних **технічних систем захисту інформації (ТСЗІ)** є фундаментом інформаційної безпеки сучасних організацій.

ТСЗІ являють собою сукупність технічних, програмних та організаційних засобів, спрямованих на забезпечення цілісності, конфіденційності та доступності інформації. Їхнє завдання — запобігти порушенню безпеки даних як унаслідок цілеспрямованих атак, так і через випадкові або технічні збої. У загальному випадку технічна система захисту складається з підсистем **криптографічного захисту**, **контролю доступу**, **мережевого захисту**, **захисту від побічних каналів витоку** та **систем моніторингу безпеки** [1].

1. Призначення та основні завдання технічних систем захисту

Основне призначення ТСЗІ полягає у **виявленні, запобіганні та локалізації** спроб порушення безпеки інформації. До головних завдань таких систем належать:

- захист інформаційних ресурсів від несанкціонованого доступу;
- запобігання витоку інформації технічними каналами (електромагнітними, акустичними, оптичними);
- забезпечення контролю за цілісністю програмного та інформаційного забезпечення;
- виявлення атак і несанкціонованих змін у системах;
- формування єдиної політики безпеки в межах підприємства.

Згідно з підходами міжнародних стандартів ISO/IEC 27001 та 15408, ТСЗІ повинні бути побудовані на принципах **багаторівневості**, **резервування**, **керованості ризиками** та **адаптивності**. Це означає, що компрометація одного рівня системи не повинна призводити до повного зниження безпеки, а система має здатність оновлювати свої політики відповідно до нових загроз.

2. Компоненти технічних систем захисту

ТСЗІ охоплюють широкий набір засобів різного рівня:

1. **Криптографічні системи захисту інформації (КЗІ).** Вони забезпечують шифрування даних при передаванні або зберіганні, створення електронного підпису, аутентифікацію та захист каналів зв’язку. Сучасні криптографічні протоколи, такі як TLS 1.3 або IPsec, використовують алгоритми AES, RSA, ECC, а також хеш-функції SHA-2 та SHA-3. З огляду на розвиток квантових обчислень активно досліджуються постквантові алгоритми, зокрема CRYSTALS-Kyber та Dilithium [2].
2. **Мережеві засоби захисту.** До них належать міжмережеві екрани, маршрутизатори з політиками безпеки, системи виявлення і запобігання вторгненням (IDS/IPS), системи аналізу трафіку (NTA) та DLP-платформи, що контролюють передачу конфіденційних даних. Сучасні рішення реалізують принципи сегментації мережі, Zero Trust та багатофакторної автентифікації користувачів.
3. **Системи контролю доступу (СКД).** Вони відповідають за ідентифікацію, автентифікацію і авторизацію користувачів. Залежно від рівня безпеки застосовуються паролі, токени, смарт-картки, біометричні параметри (відбитки пальців, розпізнавання обличчя, сітківки ока тощо).
4. **Захист від технічних каналів витоку інформації.** Це один із найбільш специфічних аспектів ТСЗІ. До нього належать заходи екранізації приміщень, фільтрації електроживлення, захисту від ПЕМВ, акустичного випромінювання, лазерного підслуховування тощо. Для виявлення потенційних каналів витоку застосовують спеціальні прилади

контролю електромагнітного випромінювання, генератори шумів і системи технічного моніторингу [3].

5. **Системи моніторингу та управління безпекою.** До них належать SIEM (Security Information and Event Management), SOAR (Security Orchestration, Automation and Response), UEBA (User and Entity Behavior Analytics) та інші. Вони збирають журнали подій з усього IT-ландшафту організації, аналізують їх та автоматично реагують на потенційні інциденти [4].

3. Інтелектуалізація та автоматизація ТСЗІ

Класичні методи захисту, засновані на сигнатурному підході, стають дедалі менш ефективними через зростання складності атак. Сучасні кібератаки часто використовують невідомі вразливості, соціальну інженерію, обфускацію коду та багатоетапні сценарії (APT). Тому в нових поколіннях ТСЗІ активно застосовуються технології **машинного навчання та штучного інтелекту (AI/ML)**.

Такі системи здатні навчатися на основі історичних даних, автоматично виявляти аномалії, аналізувати поведінку користувачів та пристроїв, прогнозувати можливі вектори атак. Прикладом є **інтелектуальні системи раннього виявлення загроз**, які аналізують мережеві потоки, журнали подій і дії користувачів для виявлення прихованих вторгнень ще до того, як вони завдадуть шкоди [5].

4. Інтеграція фізичної та кібербезпеки

Сучасні ТСЗІ розвиваються у напрямі інтеграції фізичного та цифрового рівнів. До технічних засобів фізичного захисту належать системи контролю та управління доступом (СКУД), сигналізація, системи відеоспостереження, біометричні комплекси і датчики вторгнення. Інтеграція цих засобів із IT-системами дозволяє створювати **єдині платформи управління безпекою**, де дані з різних джерел (мережевих журналів, камер, сенсорів) аналізуються централізовано.

Таким чином, фізична та кібербезпека більше не існують окремо — вони стають частинами єдиної екосистеми захисту. Особливо це важливо для критичних інфраструктур: енергетики, транспорту, фінансів, державного сектору, де компрометація фізичних пристроїв може призвести до кіберінцидентів, і навпаки.

5. Перспективи розвитку технічних систем захисту

Майбутнє технічних систем захисту визначається такими ключовими тенденціями:

- **Архітектура Zero Trust.** Усі користувачі, пристрої та сервіси вважаються потенційно небезпечними, поки не доведено протилежне. Це вимагає постійної автентифікації, шифрування всіх з’єднань і мінімізації довірених зон.

- **Інтернет речей (IoT) і кіберфізичні системи.** Вони потребують нових методів захисту на рівні сенсорів і контролерів, оскільки традиційні засоби не підходять для малопотужних пристроїв.
- **Квантові технології.** Квантовий розподіл ключів (QKD) та постквантова криптографія відкривають новий рівень стійкості до зламів.
- **Автоматизоване управління інцидентами.** Використання SOAR-систем, що здатні реагувати на інциденти без участі людини, скорочує час реакції та мінімізує людський фактор.
- **Інтерпретація моделей безпеки.** Системи пояснюваного штучного інтелекту (XAI) дозволяють розуміти причини прийняття рішень AI-моделями, що підвищує довіру до автоматизованого захисту [6].

6. Висновки

Технічні системи захисту інформації є базовим елементом кібербезпеки сучасного світу. Вони забезпечують комплексний захист даних на всіх рівнях — від фізичних пристроїв до хмарних сервісів. Сучасні ТСЗІ розвиваються у напрямі інтелектуалізації, автоматизації та інтеграції різних підсистем безпеки. Їхня ефективність визначається не лише потужністю технічних засобів, а й здатністю до самонавчання, адаптації та взаємодії з іншими компонентами інформаційної інфраструктури.

У перспективі технічні системи захисту інформації стануть повністю автономними, здатними виявляти, прогнозувати та блокувати атаки без участі людини. Поєднання класичних принципів безпеки, штучного інтелекту та квантових технологій створить нову парадигму цифрового захисту, де інформація залишатиметься безпечною навіть у найскладніших умовах кіберпростору.

Перелік посилань:

1. Грищук Р., Гуменюк В. *Технічний захист інформації: системи, методи, технології.* – Київ: НАУ, 2022. – 212 с.
2. Bernstein D. J. *Post-Quantum Cryptography*. – Springer, 2023. – 384 p.
3. НД ТЗІ 2.5-004-99. *Захист інформації від витоку технічними каналами. Загальні положення.* – Київ: ДСТСЗІ, 2011.
4. Khanna A., Gaur M. *AI-driven threat detection systems: architecture and applications* // *Computers & Security.* – 2023. – Vol. 127. – P. 103205.
5. Liu Y., Zhang Q. *Machine learning in cybersecurity: recent advances and applications* // *IEEE Transactions on Information Forensics and Security.* – 2024. – Vol. 19, No. 4. – P. 1715–1732.
6. Xu F., Ma L., Zhang Y. *Quantum key distribution in modern communication networks* // *IEEE Communications Surveys & Tutorials.* – 2024. – Vol. 26, No. 2. – P. 88–110.

Романов О. А.
студент групи УБДМ-61, ННІКБЗІ ДУІКТ,
Київ, Україна

МЕТОДИ ТА ІНСТРУМЕНТИ ОЦІНКИ ЗАХИЩЕНОСТІ МОБІЛЬНИХ ЗАСТОСУНКІВ ФІНАНСОВОГО СЕКТОРУ

У роботі розглянуто основні методи та інструменти оцінки захищеності мобільних застосунків фінансового сектору. Проаналізовано підходи статичного й динамічного аналізу безпеки, тестування на проникнення, а також використання автоматизованих платформ для моніторингу вразливостей. Показано значення інструментів MobSF, Burp Suite, Frida, SonarQube та рекомендацій OWASP MSTG для забезпечення комплексного захисту мобільних фінансових сервісів. Наголошено на важливості системного підходу, що поєднує технічні та організаційні заходи, з метою підвищення довіри користувачів і стабільності фінансових операцій.

Сучасний фінансовий сектор є одним із найбільш вразливих до кіберзагроз, адже він оперує значними обсягами конфіденційної інформації, персональних даних користувачів та фінансовими транзакціями. З розвитком цифрових технологій мобільні застосунки банків, платіжних сервісів і страхових компаній стали основним інструментом взаємодії клієнтів із фінансовими установами. Проте зростання популярності мобільних фінансових сервісів неминуче супроводжується підвищенням ризиків несанкціонованого доступу, шахрайських дій, витоків даних і маніпуляцій із платіжною інформацією. Саме тому питання оцінки захищеності таких застосунків набуває особливої актуальності та потребує системного підходу, що поєднує сучасні методи аналізу, тестування та моніторингу безпеки [1].

Оцінка захищеності мобільних застосунків фінансового сектору передбачає комплекс дій, спрямованих на виявлення вразливостей, аналіз рівня ризиків та визначення ефективності існуючих заходів безпеки. Основними методами оцінки є статичний та динамічний аналіз безпеки, тестування на проникнення, реверс-інжиніринг, а також аудит конфігурацій і політик доступу. Статичний аналіз (SAST) полягає у дослідженні вихідного коду або бінарних файлів застосунку без його виконання. Такий метод дозволяє виявляти потенційно небезпечні конструкції, невірне використання бібліотек, уразливості до ін’єкцій та проблеми з управлінням пам’яттю. Наприклад, за допомогою інструментів MobSF, QARK або SonarQube можна автоматично аналізувати код на наявність відомих патернів вразливостей [2].

Динамічний аналіз (DAST), навпаки, здійснюється під час роботи застосунку в реальному середовищі. Цей метод дозволяє перевірити, як програма поводиться під час виконання певних дій користувача або при обміні даними з сервером. Для цього використовуються інструменти, такі як OWASP ZAP, Burp Suite або Drozer, що імітують атаки та фіксують реакцію системи. Важливо, що динамічний аналіз дозволяє виявити ті вразливості, які не завжди можливо знайти під час статичного аналізу, зокрема, проблеми з автентифікацією, сесійним управлінням, передачою даних по незашифрованих каналах або некоректною обробкою помилок [3].

Окреме місце серед методів оцінки займає тестування на проникнення (penetration testing), яке імітує дії реального зловмисника з метою визначення реальної стійкості мобільного застосунку до атак. Пентестери використовують різні техніки — від соціальної інженерії до експлуатації вразливостей у

програмному коді або серверній інфраструктурі. У фінансових мобільних застосунках основну увагу під час такого тестування приділяють перевірці механізмів шифрування даних, захисту токенів автентифікації, безпеки комунікації між клієнтом і сервером, а також ізоляції даних у файловій системі пристрою. У цьому контексті ефективними є інструменти, описані в OWASP Mobile Security Testing Guide (MSTG), які забезпечують поетапну перевірку всіх критичних компонентів системи [4].

Важливим напрямом є також використання мобільних емуляторів і фреймворків для дослідження поведінки застосунку в різних умовах. Наприклад, за допомогою Frida або Objection можна виконувати динамічний аналіз, модифікувати виконання коду, відстежувати виклики до API, що дозволяє зрозуміти логіку функціонування програми та можливі слабкі місця. У свою чергу, такі інструменти, як AppCritique чи NowSecure, надають автоматизовану оцінку рівня безпеки застосунку з урахуванням політик корпоративних систем управління мобільними пристроями (MDM).

Особливої уваги заслуговує перевірка безпеки зберігання та обробки даних у мобільних фінансових застосунках. Часто вразливості виникають внаслідок недбалого зберігання конфіденційної інформації у відкритому вигляді — у кеші, журналах або базах даних SQLite. Для виявлення таких ризиків застосовують інструменти для аналізу файлової системи мобільного пристрою, а також методи реверс-інжинірингу APK або IPA файлів, які дозволяють дослідити структуру застосунку, сертифікати, ключі шифрування та конфігураційні файли.

Серед важливих критеріїв оцінки безпеки мобільних застосунків фінансового сектору варто виділити: надійність аутентифікації та авторизації користувачів, захист комунікаційного каналу (TLS/SSL), коректне керування сесіями, шифрування локальних даних, безпечну інтеграцію з API, а також відповідність вимогам стандартів PCI DSS, GDPR та ISO/IEC 27001. Під час оцінки доцільно застосовувати ризик-орієнтований підхід, який враховує потенційний вплив кожної вразливості на бізнес-процеси фінансової установи.

У сучасних умовах автоматизовані платформи для безпеки мобільних застосунків набувають дедалі більшої популярності. Вони дозволяють проводити безперервний моніторинг безпеки, інтегрувати перевірки у CI/CD процес розробки та отримувати аналітику щодо рівня відповідності стандартам. Серед таких платформ можна виділити Mobile Security Framework (MobSF), ImmuniWeb, та AppScan, які забезпечують повноцінний цикл оцінки — від первинного аналізу до формування звіту з рекомендаціями щодо усунення вразливостей.

Таким чином, ефективна оцінка захищеності мобільних застосунків фінансового сектору передбачає поєднання кількох методів — статичного, динамічного, інтегрованого тестування та пентесту. Застосування інструментів з відкритим кодом разом із комерційними рішеннями дає змогу досягти високого рівня точності та глибини аналізу. Проте жоден із технічних методів не буде ефективним без впровадження організаційних заходів: політик безпеки, навчання персоналу, контролю за змінами у вихідному коді та постійного

моніторингу подій безпеки. Системний підхід до оцінки захищеності дозволяє не лише виявляти вразливості, а й запобігати інцидентам, що мають потенціал фінансових або репутаційних втрат. У контексті постійного розвитку фінтеху та цифрових банків саме якісна оцінка захищеності мобільних застосунків є запорукою довіри користувачів і стабільності фінансових послуг [1; 3].

Перелік посилань:

1. OWASP Foundation. *OWASP Mobile Security Testing Guide (MSTG)*. – 2023. – Режим доступу: https://owasp.org/www-project-mobile-security-testing-guide/
2. QARK – *Quick Android Review Kit*. – 2022. – Режим доступу: https://github.com/linkedin/qark
3. NowSecure. *Mobile App Security Testing Overview*. – 2024. – Режим доступу: https://www.nowsecure.com/resources
4. SonarSource. *SonarQube Documentation*. – 2023. – Режим доступу: https://docs.sonarsource.com/sonarqube/latest/

Савченко Вадим Володимирович,
студент групи БСДМ-51, ННІКБЗІ ДУІКТ, Київ, Україна
Стожок Максим Романович,
студент групи БСДМ-51, ННІКБЗІ ДУІКТ, Київ, Україна

МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК ОСНОВА СТІЙКОСТІ ОРГАНІЗАЦІЇ В УМОВАХ КІБЕРЗАГРОЗ

Стійкість організації в умовах сучасних кіберзагроз неможлива без побудови системного менеджменту інформаційної безпеки. Такі компоненти, як оцінка ризиків, розробка політик, впровадження заходів захисту та постійний моніторинг, формують основу ефективної системи безпеки. Вони дозволяють не лише мінімізувати ймовірність реалізації загроз, а й забезпечити відповідність міжнародним стандартам, інтегрувати безпеку в бізнес-процеси та формувати культуру обізнаності серед персоналу, створюючи комплексний захист інформаційних активів організації.

Ключові слова: менеджмент інформаційної безпеки, СМІБ, ISO/IEC 27001, управління ризиками, кібербезпека.

Сучасні підприємства працюють в уомовах безпрецендентних кіберзагроз, тому системний підхід до інформаційної безпеки є не просто бажанням, а необхідністю. Управління інформаційною безпекою (ІБ) – це копмплексний процес, спрямований на забезпечення конфіденційності, цілісності та доступності інформаційних активів організації. Він виходить за межі простої технічної реалізації заходів безпеки і охоплює упаравління ризиками, політики, процедури та людський фактор, тим самим створюючи міцну основу для досягнення бізнес-цілей.

Управління ризиками інформаційної безпеки: від оцінки до прийняття рішень

Ефективне управління ризиками ІБ є фундаментом для прийняття обґрунтованих рішень щодо захисту інформаційних активів організації. Цей

процес починається з комплексної ідентифікації інформаційних активів, оцінки їх критичності для бізнесу, аналізу потенційних загроз та вразливостей систем захисту. Кількісна та якісна оцінка ризиків дозволяє не лише визначити пріоритетність заходів захисту, але й оптимізувати розподіл ресурсів на їх впровадження. Кінцевим результатом цього процесу є формування єдиного реєстру ризиків, який слугує основою для розробки стратегії інформаційної безпеки та прийняття управлінських рішень щодо впровадження контрзаходів [1].

Рис. 1 – Процес управління ризиками інформаційної безпеки

Міжнародні стандарти ISO/IEC 2700X: основа побудови СМІБ

Серія міжнародних стандартів ISO/IEC 2700X становить методологічну основу для побудови ефективної системи менеджменту інформаційної безпеки. ISO/IEC 27001 визначає чіткі вимоги до СМІБ, тоді як ISO/IEC 27002 містить детальні практичні рекомендації щодо імплементації заходів безпеки. Ключовою перевагою цих стандартів є реалізація циклу PDCA (Plan-Do-Check-Act), що забезпечує постійне вдосконалення системи безпеки організації. Впровадження СМІБ відповідно до вимог ISO/IEC 27001 дозволяє не лише ефективно керувати ризиками інформаційної безпеки, але й демонструвати зацікавленим сторонам дотримання міжнародно визнаних практик у сфері захисту інформації [2].

Кадрова безпека: формування культури обізнаності в умовах кіберзагроз

Людський фактор продовжує залишатися одним з найкритичніших елементів у системі безпеки будь-якої організації. Ефективний менеджмент інформаційної безпеки вимагає комплексного підходу до управління кадровою безпекою, який включає: ретельну перевірку співробітників при наймі, підписання угод про конфіденційність, регулярне навчання та системне підвищення обізнаності з питань безпеки. Сучасні дослідження підтверджують, що організації з налагодженими програмами security awareness мають на 70%

менший ризик успішних кібератак. Формування сталої культури безпеки серед співробітників є критично важливим елементом для забезпечення стійкості організації до сучасних кіберзагроз [2].

Рис. 2 – Вплив програм security awareness на рівень безпеки організації

Інтеграція СМІБ з бізнес-процесами: баланс між безпекою та ефективністю

Сучасний менеджмент інформаційної безпеки не може функціонувати як ізольований від бізнесу напрям. Ефективна СМІБ має бути органічно інтегрованою в усі бізнес-процеси організації - від стратегічного планування та розробки продуктів до обслуговування клієнтів. Це передбачає активну участь керівника з інформаційної безпеки в прийнятті стратегічних рішень, проведення обов'язкової оцінки впливу на безпеку при впровадженні нових технологій та послуг, а також включення вимог безпеки в усі внутрішні регламенти та процедури. Така інтеграція дозволяє забезпечити оптимальний баланс між рівнем безпеки та операційними потребами бізнесу [1].

Синергія процесів у межах системи менеджменту інформаційної безпеки

Взаємозв’язок між управлінням ризиками, дотриманням стандартів, кадровою безпекою та інтеграцією СМІБ у бізнес-процеси створює єдиний механізм забезпечення стійкості організації. У такій системі кожен елемент підтримує інший: стандарти задають методологію, управління ризиками забезпечує пріоритети, навчання персоналу мінімізує людські помилки, а інтеграція в бізнес-процеси гарантує практичну ефективність усіх заходів. Саме узгодженість цих компонентів дозволяє перетворити інформаційну безпеку з окремої функції на стратегічну складову корпоративного управління, що забезпечує безперервність діяльності та довіру до організації в цифровому середовищі.

Перелік посилань:

1. ISO. Information Security Risk Management: Principles and Guidelines. — ISO/IEC 27005:2022 Overview. URL: https://www.iso.org/standard/80585.html (дата звернення: 20.10.2025).

2. IBM Security. The Human Factor in Cybersecurity: Building Awareness and Resilience. — IBM Security Intelligence. URL: https://securityintelligence.com/posts/building-cybersecurity-awareness/ (дата звернення: 20.10.2025

Сайніді М.С.,
студент УБДМ-61, ННІКБЗІ, ДУІКТ,
м. Київ, Україна

ПЕРЕВАГИ І НЕДОЛІКИ СИСТЕМ UEBA

В умовах динамічного розвитку кіберзагроз і технологій зловмисного кібервпливу системи поведінкової аналітики UEBA з їх проактивним і адаптивним підходом дозволяють забезпечити вчасне й ефективне виявлення й аналіз загроз, протидію деструктивному людському чиннику та нормативну відповідність. Встановлено, що незважаючи на низку недоліків, зокрема наявність хибнопозитивних результатів, складність розгортання й інтеграції, а також проблеми з конфіденційністю даних, UEBA мають чіткі перспективи використання як важливого інструменту забезпечення кібербезпеки.

У сучасному швидкозмінному цифровому світі кіберзагрози стають дедалі складнішими. Традиційні системи безпеки, що спираються на статичні правила, часто не справляються з динамічними та непередбачуваними атаками. Саме тут на допомогу приходить аналітика поведінки користувачів та ІТ-об’єктів (UEBA), яка, як пильний охоронець організації, постійно спостерігає й аналізує діяльність користувачів, щоб виявити спроби деструктивного впливу.

Сучасні UEBA використовують машинне навчання (ML) та поведінкову аналітику для встановлення базової лінії нормальної поведінки користувачів та ІТ-об’єктів в організації; виявлення відхилень від цього шаблону і сповіщення про потенційні загрози безпеці.

Кібербезпека пройшла довгий шлях від базових брандмауерів і антивірусних програм, які переважно зосереджуються на виявленні відомих загроз на основі правил. Однак сучасні зловмисники навчилися вміло обходити ці системи за допомогою таких методів як крадіжка облікових даних, внутрішні загрози й атаки без використання шкідливого ПЗ.

Саме тут UEBA реалізують свої переваги, аналізуючи поведінку, а не покладаючись на заздалегідь визначені правила, і маючи змогу виявляти загрози, які традиційні інструменти можуть пропустити. Системи поведінкової аналітики є особливо ефективними у протидії:

– внутрішнім загрозам, тобто зловмисним або випадковим діям працівників, які ставлять під загрозу безпеку;

– крадіжкам облікових даних, коли зловмисники використовують вкрадені облікові дані для отримання доступу до конфіденційних активів;

– автоматизованим атакам, які охоплюють аномальну поведінку ботів, скомпрометованих пристроїв або серверів.

Крім цього UEBA роблять свій внесок у посилення мережевої безпеки, відстежуючи, як користувачі та ІТ-об'єкти взаємодіють з мережевими ресурсами, а також хмарної безпеки, виявляючи сумнівну поведінку користувачів та ІТ-об'єктів у хмарних середовищах [1].

UEBA притаманні декілька суттєвих переваг [2, 3], які роблять ці системи важливим компонентом сучасних стратегій кібербезпеки.

Насамперед, UEBA здійснюють проактивне виявлення загроз безпеці. На відміну від традиційних інструментів, які реагують на відомі загрози, UEBA виявляють аномалії в режимі реального часу, що дозволяє вирішувати проблеми до їх загострення.

Також системи поведінкової аналітики дозволяють організації забезпечити відповідність вимогам законодавства і регуляторним нормам, ведучи детальні журнали та проводячи регулярний аналіз поведінки користувачів та IT-об’єктів.

Завдяки впровадженню рішень UEBA організації зменшують відсоток людських помилок, адже засоби автоматизації та штучний інтелект мінімізують ризик пропуску критичних загроз.

Водночас впровадження систем поведінкової аналітики не позбавлене низки проблем [2, 3]. Найбільш поширеною є наявність хибнопозитивних результатів - позначення звичайних дій як підозрілих, що призводить до втрати часу і ресурсів.

Налаштування UEBA, а також інтеграція з іншими корпоративними системами вимагає досвіду в машинному навчанні та поведінковій аналітиці, що може бути складним для невеликих організацій.

З огляду на те, що UEBA у процесі свого функціонування збирають великі обсяги даних, можуть виникати проблеми з їх конфіденційністю, що робить критично важливим збалансування вимог безпеки і етичних принципів.

Основні переваги і виклики впровадження UEBA показані на рисунку 1.

Рис. 1. Переваги і проблеми впровадження UEBA

Незважаючи на наявність переваг і недоліків, безсумнівним є значні перспективи використання UEBA як важливого інструменту впровадження

проактивного й адаптивного підходів до виявлення та пом'якшення сучасних кіберзагроз.

Перелік посилань:

5. UEBA An In-depth Exploration of User and Entity Behavior Analytics. April 2024. URL: https://informatics.nic.in/uploads/pdfs/f0e84d03_37_38_tup_ueba.pdf

6. Iyer, Kumrashan Indranil. Behavioral Intelligence at Scale: Implementing UEBA for Enhanced Security Posture. *International Journal of Science and Research (IJSR).* 2022. 11. P. 1971-1977. 10.21275/SR22074090532.

7. Making Sense of UEBA: A Practical Guide to Modern Cybersecurity January 2025. URL: https://hacklido.com/blog/984-making-sense-of-ueba-a-practical-guide-to-modern-cybersecurity

Скибицький Вадим Олександрович

студент групи БСДМ-61, ННІКБЗІ, Київ, Україна

СПОСТЕРЕЖУВАНІСТЬ ЯК КОНЦЕПТ ВИЯВЛЕННЯ АНОМАЛІЙ У СУЧАСНИХ РОЗПОДІЛЕНИХ ІТ-СЕРЕДОВИЩАХ

Сьогоднішня арена інформаційних технологій має значний пласт складностей через ускладнення систем. Міграція до так хмарних рішень та гібридних оперативних середовищ, поряд із стрімким розповсюдженням мікросервісних схем побудови програм, сформувала цілий пласт розподілених, вкрай динамічних і за своєю суттю короткочасних системних конгломератів. Синхронно з цими змінами, ризики та загрози модифікувалися і розвинулися з ідентичною швидкістю. Зловмисні суб'єкти вже не обмежують себе лише використанням примітивних файлів зі шкідливим кодом. Вони активно запроваджують програмне забезпечення, що працює без фізичного файлу, здійснюють напади на мережі постачальників послуг, використовують вдосконалені методи постійного вторгнення (Advanced Persistent Threats) та розгортають заплутані, багатовекторні кампанії вторгнення.

У результаті, стандартні засоби кіберзахисту виявились недостатніми. Їхня принципова проблема криється у тому, що ці інструменти функціонують на основі застарілих методологій, котрі спираються на бази даних ідентифікаторів та набір чітко визначених, статичних правил. Сучасні агресори активно експлуатують абсолютно легітимні системні утиліти та операційні техніки, які за своїми характеристиками апріорі не мають унікальних сигнатур. Відповідно, будь-яка захисна стратегія, що ґрунтується виключно на пошуку та виявленні вже відомих "поганих" елементів, приречена на провал. Новий, дієвий підхід мусить базуватися на глибокому знанні загальноприйнятої, "нормальної" поведінки системи для ефективного виявлення "поганого", яке ще не було ідентифіковане.

Застарілий підхід до кіберзахисту, що діяв за принципом "фортеці" і концентрувався на обороні зовнішніх кордонів, більше не відповідає реаліям сучасності. Периметр став віртуальним і нечітким, що зумовлено широким використанням хмарних рішень та віддаленим режимом роботи. Фундаментальні завдання кібербезпеки – Конфіденційність, Цілісність та Доступність (відомі як тріада CIA) тепер доповнюються новою, головною метою: Стійкістю (Resilience) [1].

Стійкість системи окреслюється як її спроможність успішно протистояти актуальним та новим кіберзагрозам, зберігати працездатність критичних функцій безпосередньо в процесі відбиття атаки та демонструвати високу швидкість повернення до нормального режиму після інциденту. Досягнення стійкості вимагає

не просто поверхневого, а глибокого, безперервного аналізу внутрішнього стану системи у реальному часі. Багаторівнева структура сьогоднішніх IT-інфраструктур (куди входять мікросервісна архітектура та хмарні середовища) виступає не лише як розширена площина для потенційних атак, але й як серйозна перешкода для ефективного захисту. Зловмисні дії часто відбуваються у проміжках між окремими компонентами, де класичні засоби безпеки, такі як EDR (Endpoint Detection and Response), які моніторять виключно кінцеві пристрої, нездатні охопити та візуалізувати увесь комплексний ланцюг розвитку кібератаки.

Звичний моніторинг був створений для систем, які є відносно нерухомими та нескладними. Його увага концентрувалася на виявленні вже відомих небезпек. За своєю природою, він завжди діє реактивно. Натомість, спостережуваність – це наступний етап розвитку, який став необхідним через заплутаність сучасних, географічно рознесених систем. Це не просто вдосконалення моніторингу, це активна характеристика системи, що дозволяє вивчати ще невідомі ризики та знаходити відповідь на запитання «через що щось відбувається».

Замість реакції на сповіщення про відомі загрози, спостережуваність дозволяє командам безпеки проактивно виявляти аномалії та незвичайні патерни. Платформи спостережуваності використовують машинне навчання (ML) та штучний інтелект (AI) для аналізу всієї телеметрії, створення "бейзлайну" нормальної поведінки та виявлення відхилень від неї. Це дозволяє прогнозувати проблеми до того, як вони вплинуть на користувачів або перетворяться на повноцінний інцидент безпеки. Таким чином, захист переходить від реактивного до проактивного і навіть предиктивного [2].

Спостережуваність надає єдине джерело для різних команд. Команди SecOps, Ops та Dev можуть використовувати ту саму платформу та ті самі дані (логи, метрики, трейси) для розслідування проблем. Це усуває ізольованість і дозволяє набагато ефективніше співпрацювати [3].

Ця можливість є критично важливою. Проблема продуктивності та проблема безпеки можуть виглядати однаково на рівні метрик. Традиційний, ізольований SOC не може їх розрізнити. Об'єднана команда, що використовує платформу спостережуваності, може миттєво скорелювати логи мережевого трафіку з метриками сервера та трейсами додатків, щоб відрізнити законний сплеск трафіку від зловмисної атаки.

Більше того, це дозволяє будувати більш стійкі системи. Завдяки глибокому аналізу першопричин, спостережуваність дозволяє командам не просто заблокувати IP зловмисника (підхід моніторингу), а виправити вразливість у коді або перепроектувати архітектуру, яка дозволила атаку.

Отже, такий підхід до кібербезпеки, що базується на спостережуваності та глибокому аналізі поведінки системи, дозволяє радикально змінити спосіб протидії загрозам у сучасних IT-інфраструктурах. Замість того, щоб лише реагувати на відомі атаки та блокувати відомі загрози, організації отримують змогу проактивно виявляти

аномалії, передбачати потенційні проблеми та усувати першопричини вразливостей ще до того, як вони стануть критичними.

Це відкриває нові горизонти для побудови стійких систем, які здатні не лише витримувати атаки, а й швидко відновлювати свою працездатність, зберігаючи ключові сервіси для користувачів. Крім того, інтеграція даних і єдине джерело телеметрії для команди забезпечує ефективну взаємодію, усуває «сліпі зони» в безпеці та дозволяє приймати обґрунтовані рішення на основі повного розуміння подій у системі.

Таким чином, перехід від традиційного, реактивного захисту до сучасної спостережуваності та аналітики є не лише технологічною необхідністю, а й ключовою стратегією забезпечення кіберстійкості. Він формує основу для безперервного розвитку IT-інфраструктур, здатних протистояти новим, складним та непередбачуваним загрозам, забезпечуючи надійність, безпеку та стабільність цифрового середовища.

Перелік посилань:

1. Understanding Modern Observability [Електронний ресурс] // National Center for Biotechnology Information (NCBI). – Режим доступу: https://pmc.ncbi.nlm.nih.gov/articles/PMC7122347/ (дата звернення: 24.10.2025).
2. Reactive and Proactive Observability in the Modern Monitoring Landscape [Електронний ресурс] // *DZone*. – Режим доступу: https://dzone.com/articles/reactive-and-proactive-observability-in-the-modern-monitoring-landscape (дата звернення: 24.10.2025).
3. 5 Reasons Why Observability and Security Work Well Together [Електронний ресурс] // *Elastic Blog*. – Режим доступу: https://www.elastic.co/blog/5-reasons-why-observability-and-security-work-well-together (дата звернення: 24.10.2025).

Слободська Л. О.
студентка групи УБДМ-61, ННІКБЗІ ДУІКТ,
Київ, Україна

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ АВТОМАТИЗАЦІЇ ПРОЦЕСІВ ПЕНТЕСТУ

У даній тезі розглядаються сучасні тенденції використання штучного інтелекту (ШІ) для автоматизації процесів тестування на проникнення (пентесту). Особливу увагу приділено впливу інтелектуальних алгоритмів на ефективність і точність виявлення вразливостей, можливостям застосування машинного навчання та обробки природної мови у сфері кібербезпеки, а також викликам, що постають перед фахівцями при інтеграції ШІ у процеси безпеки. У роботі розкрито переваги, ризики та перспективи розвитку таких систем у контексті забезпечення надійності сучасних інформаційних технологій.

Штучний інтелект поступово змінює підходи до забезпечення інформаційної безпеки, зокрема до тестування на проникнення — процесу, спрямованого на виявлення вразливостей у програмному забезпеченні та інфраструктурі до того, як ними скористаються зловмисники. Традиційні методи пентесту вимагають значних людських і часових ресурсів, адже фахівці повинні вручну аналізувати складні

системи, проводити атаки та документувати результати. Завдяки застосуванню штучного інтелекту ці процеси можна частково або повністю автоматизувати, підвищивши ефективність і зменшивши ймовірність людських помилок [1].

Основна роль ШІ у пентесті полягає у здатності аналізувати великі обсяги даних та виявляти закономірності, які можуть свідчити про потенційні уразливості. Наприклад, системи машинного навчання можуть бути навчені на основі попередніх атак, шаблонів поведінки користувачів або мережевого трафіку, що дозволяє їм автоматично визначати підозрілі дії або конфігурації [2]. Такі алгоритми можуть швидко аналізувати результати сканування, проводити класифікацію виявлених проблем за рівнем критичності та пропонувати способи їх усунення.

Важливим напрямом є застосування обробки природної мови (NLP) у пентесті. Завдяки цій технології інструменти штучного інтелекту здатні обробляти текстову інформацію з технічної документації, журналів подій або звітів і на основі цього формувати гіпотези щодо потенційних векторів атак. Наприклад, ШІ може проаналізувати опис API або політику безпеки й виявити невідповідності, які можуть бути використані для експлуатації системи. Це дозволяє автоматизувати етапи підготовки до тестування, зменшуючи обсяг ручної роботи спеціалістів [3, с. 42].

Іншим напрямом розвитку є використання генеративних моделей для створення сценаріїв атак. Такі системи можуть автоматично генерувати запити, експлойти або фішингові повідомлення, які імітують реальні дії зловмисників. Це допомагає тестувальникам оцінити стійкість системи до соціальної інженерії або спроб отримання несанкціонованого доступу. Штучний інтелект також може виконувати автоматизоване моделювання загроз, використовуючи аналітичні дані про відомі уразливості, що значно прискорює процес оцінки ризиків [4].

Застосування ШІ у пентесті відкриває нові можливості для прогнозування атак. Завдяки аналізу історичних даних і поведінкових моделей системи можуть передбачати, які саме частини інфраструктури можуть бути найбільш вразливими у майбутньому. Це дає змогу організаціям переходити від реактивного до проактивного підходу у сфері безпеки, коли потенційні ризики усуваються ще до того, як вони стають реальною загрозою [2].

Разом з тим, використання штучного інтелекту у процесах пентесту має і свої виклики. Однією з головних проблем є якість навчальних даних. Якщо модель навчається на неповних або упереджених даних, це може призвести до помилкових висновків і пропуску критичних вразливостей. Крім того, автоматизовані системи можуть бути самі об’єктом атак, коли зловмисники намагаються маніпулювати вхідними даними, щоб обійти перевірки або викликати хибні результати [1].

Іншою складністю є питання етичності та відповідальності. Автоматизовані системи можуть використовуватись не лише для тестування безпеки, але й для створення більш складних атак. Тому важливо визначити межі застосування ШІ у кібербезпеці та встановити контроль за його використанням. Людський фактор залишається ключовим у процесі пентесту, адже навіть найрозвиненіші алгоритми

потребують нагляду з боку експертів, здатних інтерпретувати результати та приймати рішення у складних ситуаціях [3].

У майбутньому розвиток штучного інтелекту може призвести до появи повністю автономних систем пентесту, здатних самостійно виконувати комплекс перевірок без участі людини. Проте сьогодні найефективнішими залишаються гібридні моделі, у яких поєднується інтелект людини та машинний аналіз. Такий підхід забезпечує баланс між автоматизацією, точністю та контролем, дозволяючи досягати високої ефективності при збереженні гнучкості під час проведення перевірок [4].

Отже, застосування штучного інтелекту у сфері тестування на проникнення є перспективним напрямом, що має потенціал значно підвищити рівень кіберзахищеності організацій. Використання інтелектуальних алгоритмів дозволяє не лише зменшити навантаження на фахівців, але й підвищити якість аналізу, точність прогнозування та швидкість реагування на нові загрози. Водночас важливо забезпечити належний контроль і розвиток етичних стандартів, аби ШІ залишався інструментом захисту, а не ризиком для інформаційної безпеки.

Перелік посилань:

1. Brundage M. et al. *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation.* – 2023.
2. IBM Security. *AI-Powered Penetration Testing Solutions.* – 2024. – Режим доступу: https://www.ibm.com/security/ai
3. Mitre Corporation. *Artificial Intelligence for Cybersecurity Operations.* – 2023. – Режим доступу: https://www.mitre.org
OWASP Foundation. *AI in Security Testing: Practical Guidelines.* – 2024. – Режим доступу: https://owasp.org

Теремко Микита Олександрович
Студент групи КНДм-61, ННІІТ ДУІКТ, Київ, Україна

АРХІТЕКТУРА КІБЕРМОНІТОРИНГУ НА БАЗІ OSINT ДЛЯ ВИЯВЛЕННЯ ТА ПРІОРИТИЗАЦІЇ КІБЕРРИЗИКІВ

Подано архітектуру кібермоніторингу на базі OSINT для виявлення та пріоритизації кіберризиків. Описано конвеєр: збір, нормалізація, збагачення, кореляція. Запропоновано ризик-скоринг із CVSS, EPSS, експозицією та критичністю активів. Показано інтеграцію з ISMS і SOC-процесами та метрики ефективності (MTTD, MTTR, покриття ATT&CK) для управлінських рішень. Підхід зменшує залишковий ризик, підвищує прозорість та швидкодію.

У цій роботі, котра описує архітектуру, джерела OSINT стають інформаційним об’єктом, котрий складається з чотирьох пов’язаних між собою пластів. До джерел були віднесені: технічні фіди, тактична розвідка загроз, стратегічні джерела, медійні майданчики. Технічні фіди це IP-адреси, домени та хеші з репутаційних списків на кшталт CERT[1]. Тактична розвідка загроз описує як саме діє нападник, які інструменти застосовує і які сліди лишає. Тут важливі мапінг на MITRE ATT&CK, звіти про кампанії, а також правила виявлення у форматах Sigma та YARA, що перетворюють аналітику на конкретні сигнали для моніторингу. Стратегічні джерела дають ширший контекст і пріоритети робіт: огляди галузі, реєстри вразливостей на зразок CVE та CPE, бюлетені виробників і офіційні попередження. Медійні майданчики забезпечують ранні індикатори з форумів, професійних спільнот і тематичних каналів, але з ними потрібна обережність в межах права. У підсумку ці чотири пласти зливаються в керований інформаційний об’єкт, який легко нормалізувати, збагатити контекстом активів і пріоритизувати для дій.

Конвеєр обробки та інтеграції будується як послідовність кроків: спочатку збираємо дані через колектори та підписки на стрічки даних загроз, додаємо вебскрапінг з обмеженням частоти й дедуплікацією, а також приймаємо події з систем керування інформацією та подіями безпеки і з платформ оркестрації, автоматизації та реагування. Далі нормалізуємо все до узгоджених форматів, зокрема до формату обміну структурованою інформацією про загрози та до протоколу автоматизованого надійного обміну індикаторами, перевіряємо цілісність і відсіюємо джерела з низьким рівнем довіри. На етапі збагачення додаємо довідкові атрибути з реєстрів власників доменів, виконуємо географічне визначення за адресою інтернет-протоколу, використовуємо пасивні дані системи доменних імен та відкриті платформи обміну інформацією про загрози; зіставляємо техніки з базою знань тактик, технік і процедур від організації MITRE і пов’язуємо сигнали з активами з конфігураційної бази даних та з відомими вразливостями з реєстру загальновідомих вразливостей разом із їх оцінкою за системою загальної оцінки небезпеки. Після цього виконуємо кореляцію за правилами виявлення, евристиками та часовими вікнами, відшуковуємо ланцюжки атаки й тенденції. Завершальним кроком є оцінювання ризику, рахуємо інтегральний бал як поєднання ймовірності та впливу, де ймовірність спирається на систему прогнозної ймовірності експлуатації,

а вплив визначається критичністю активу, наявними компенсуючими контролями та рівнем зовнішньої доступності сервісу.

Пріоритизацію кіберризиків будуємо як зважене поєднання трьох вимірів. Першим є технічна суворість вразливості за системою CVSS версії 4.0 [2]. Другий є прогностична ймовірність її реальної експлуатації за методикою EPSS [4]. Третім є індикатор актуальності у вигляді частоти згадувань у публічних потоках даних про загрози. Сам по собі бал CVSS описує лише технічну небезпеку, тому його доповнюємо факторами середовища і загрози. Додаємо контекст активів: значущість сервісу для бізнес процесу, цільовий час відновлення та цільову точку відновлення, зовнішню доступність у мережі, залежності з переліку програмних компонентів і з ланцюга постачання. Окремо оцінюємо готовність до виявлення та захисту на практиці, зокрема наявність офіційного виправного пакета, покриття засобами виявлення і реагування на кінцевих точках та системами керування інформацією і подіями безпеки, наявні правила виявлення і діючі компенсаційні заходи. Щоб отримати один пріоритет для черги робіт, обчислюємо інтегральний бал ризику як зважену суму компонентів ймовірності і впливу з урахуванням прогностичної оцінки експлуатації [4], технічної суворості [2], експозиції, критичності активу та покриття контролями. Коефіцієнти ваг налаштовуємо під профіль ризику організації. Такий підхід відповідає класичній моделі управління ризиками, де ризик розглядається як поєднання ймовірності настання події та величини впливу на активи і бізнес цілі [3]. Нарешті, використання прогностичної оцінки експлуатації дає обґрунтований сигнал щодо того, які вразливості з реєстру загальновідомих вразливостей з більшою імовірністю будуть атаковані протягом найближчих тридцяти днів, що безпосередньо допомагає у впорядкуванні виправлень [4].

Місце цієї архітектури в системі менеджменту інформаційної безпеки визначається через щоденну роботу процесів. У керуванні ризиками дані з кібермоніторингу потрапляють до реєстру ризиків, порівнюються з критеріями прийнятності та одразу пов’язуються з відповідальними власниками бізнес активів, щоб рішення про обробку ризику ухвалювалися не формально, а з урахуванням впливу на процеси компанії. В менеджменті інцидентами, згенеровані події автоматично створюють записи про інциденти у системі керування інформацією та подіями безпеки та у платформі оркестрації, автоматизації та реагування, запускають підготовлені плейбуки реагування і повертають зворотний зв’язок у розвіддані про загрози для подальшого уточнення правил і джерел. У керуванні змінами і конфігураціями кожна запропонована дія з переліку пріоритетів проходить погодження дорадчим комітетом із змін, а політики та налаштування перевіряються засобами інфраструктури як код, щоб гарантувати відтворюваність і контроль якості. Регулярна звітність підтримує ритм роботи. Щотижневі огляди актуальних загроз для операційних команд, щомісячні зведені метрики для керівництва і щоквартальні аудити контролів для перевірки дієвості та відповідності обраній моделі ризику.

Метрики якості та ефективності задають прозорі правила гри для всієї системи. Спершу перевіряємо самі дані, наскільки індикатори унікальні, яка частка записів проходить валідацію без помилок, скільки часу минає від появи сигналу до його потрапляння в конвеєр, який відсоток індикаторів втрачає актуальність до моменту обробки. Далі оцінюємо роботу виявлення та реагування, середній час до спрацювання детекцій, середній час до закриття інциденту, співвідношення істинних і хибних сповіщень, точність і повнота виявлення, а також рівень покриття технік за матрицею тактик і прийомів від організації MITRE. У площині управління ризиками дивимося, яку частку критичних ризиків закриваємо у межах погоджених строків надання послуг, який середній зважений бал ризику мають різні периметри інфраструктури, скільки кейсів доводиться ескалювати на вищий рівень. Потім рахуємо економіку процесу, середню вартість опрацювання одного інциденту, середню вартість збагачення одного артефакта, а також оціночну суму втрат, яких вдалося уникнути завдяки превентивним діям. Для кожного показника встановлюємо базову лінію та цільове значення, відстежуємо їх у динаміці й використовуємо для налаштування джерел, правил виявлення та сценаріїв реагування, щоб система ставала точнішою та швидшою з кожним циклом.

У підсумку запропоновано цілісну архітектуру кібермоніторингу на базі відкритих джерел, яка поєднує збір, нормалізацію, збагачення та кореляцію даних з подальшим ризик орієнтованим прийняттям рішень. Зазначено як індикатори і поведінкові ознаки загроз переводяться у пріоритети через інтегральний бал ризику з урахуванням технічної суворості, прогнозної імовірності експлуатації, експозиції сервісів та критичності активів. Окреслено місце рішення у системі менеджменту інформаційної безпеки: дані потрапляють до реєстру ризиків, запускають керовані сценарії реагування та підтримують погоджені зміни конфігурацій. Сформовано набір метрик якості і ефективності, що дозволяє вимірювати скорочення часу до виявлення та до реагування, рівень покриття прийомів за матрицею тактик і технік, а також економічний ефект від запобігання інцидентам. Практична цінність підходу полягає у прозорій пріоритизації робіт, узгодженій з вимогами бізнесу, та у підвищенні керованості процесів безпеки. Перспективними є автоматичне налаштування ваг у моделі оцінювання, розширення спостереження за зовнішньою поверхнею та поглиблення інтеграції з обліком програмних компонентів і ризиками ланцюга постачання.

Перелік посилань:

1. CERT-UA. Роз’яснення CERT-UA: платформа MISP: що це, як підключатися та які переваги. Доступ: https://cip.gov.ua/ua/faqs/roz-yasnennya-cert-ua-platforma-misp-sho-ce-yak-pidklyuchatisya-ta-yaki-perevagi (дата звернення: 20.10.2025)
2. FIRST. Common Vulnerability Scoring System Version 4.0: Specification Document. 2023. Доступ: https://www.first.org/cvss/v4-0/ (дата звернення: 20.10.2025);
3. National Institute of Standards and Technology. Guide for Conducting Risk Assessments NIST Special Publication 800-30 Revision 1. Gaithersburg, MD: NIST, 2012. DOI: https://doi.org/10.6028/NIST.SP.800-30r1 (дата звернення: 20.10.2025);
4. FIRST. Exploit Prediction Scoring System EPSS: Documentation and Data. 2024–2025. Доступ: https://www.first.org/epss/ (дата звернення: 20.10.2025).

Хоменко М.С.
студент групи БСДМ-51, ННІЗІ ДУІКТ,
Київ, Україна

NIST SP 800-61: Еволюція підходів до реагування на інциденти

Розглядається оновлена редакція NIST SP 800-61 Revision 3, що замінює попередню версію 2012 року. Аналізуються основні зміни в підходах до реагування на інциденти, зокрема узгодження процесу з функціями NIST Cybersecurity Framework 2.0. Визначено перехід від чотириетапної моделі до інтегрованої системи реагування, орієнтованої на управління ризиками та постійне вдосконалення процедур безпеки.

Ключові слова: NIST SP 800-61, Revision 2, Revision 3, реагування на інциденти, Incident Response, кібербезпека, управління ризиками, NIST Cybersecurity Framework, CSF 2.0, інформаційна безпека.

NIST SP 800-61 Revision 2, опублікований у серпні 2012 року, є ключовим посібником із реагування на інциденти в комп’ютерній безпеці від Національного інституту стандартів і технологій США. Український переклад назви документа звучить як "Керівні настанови щодо управління інцидентами, пов’язаними з комп’ютерною безпекою".

Документ деталізує процес Incident Response (IR) через чотири основні фази (рис. 1): підготовку, виявлення та аналіз, стримування, усунення та відновлення, а також пост-аналіз. Він пропонує організаціям практичні рекомендації, шаблони та приклади для мінімізації збитків від різноманітних кіберінцидентів, включно з витоками даних і атаками ransomware.

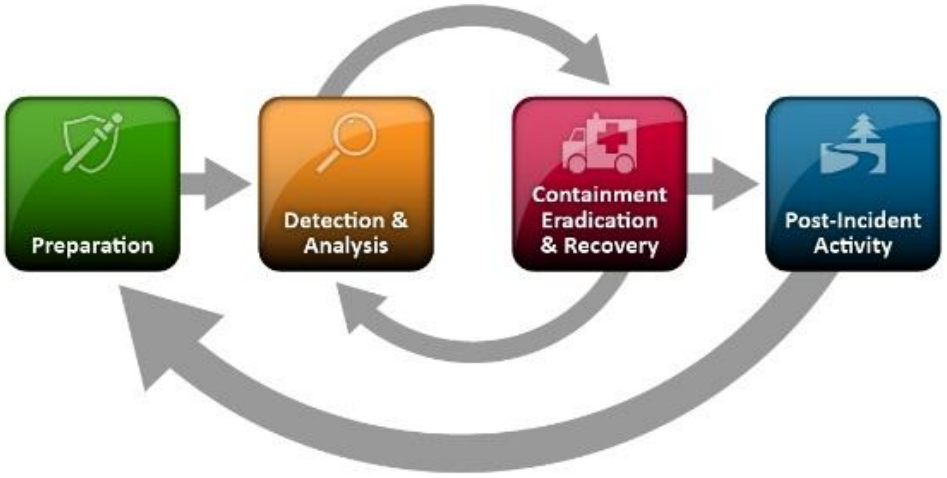

Рис. 1 – Життєвий цикл реагування на інциденти (Revision 2)

Особливу увагу в Revision 2 приділено опрацюванню конкретних сценаріїв інцидентів, таких як атаки на інфраструктуру (DoS на DNS-сервер), внутрішні загрози (несанкціонований доступ до конфіденційних документів) та проблеми безпеки мережі (невідомі точки доступу). Для кожного сценарію пропонуються короткі описи та аналітичні питання, що допомагають командам IR відпрацьовувати реагування в умовах, максимально наближених до реальних. Таким чином, документ слугує практичним керівництвом для організацій будь-якого розміру та рівня підготовки. [1]

NIST SP 800-61 Revision 3

У квітні 2025 року NIST опублікував Revision 3, що стало першим оновленням документа з 2012 року. Нове видання суттєво розширює підхід до реагування на інциденти, інтегруючи його з принципами NIST Cybersecurity Framework 2.0, який визначає шість ключових функцій: Govern, Identify, Protect, Detect, Respond та Recover. Revision 3 орієнтує організації на перегляд і оновлення планів та процедур IR, особливо якщо попередні версії SP 800-61 або програми кібербезпеки були базовані на попередніх редакціях або узгоджені з NIST CSF.

Revision 3 не просто оновлює зміст, а переписує його повністю, підвищуючи чіткість викладу та усуваючи застарілі матеріали. Акцент зміщується з деталізованих інструкцій щодо обробки конкретних інцидентів на інтеграцію реагування в загальну систему управління кіберризиками організації. Модель життєвого циклу IR (рис. 2) стає більш динамічною та гнучкою: вона поєднує підготовку, реагування та відновлення з безперервним вдосконаленням процесів і відповідає сучасним викликам кібербезпеки, що характеризуються високою частотою та складністю атак.

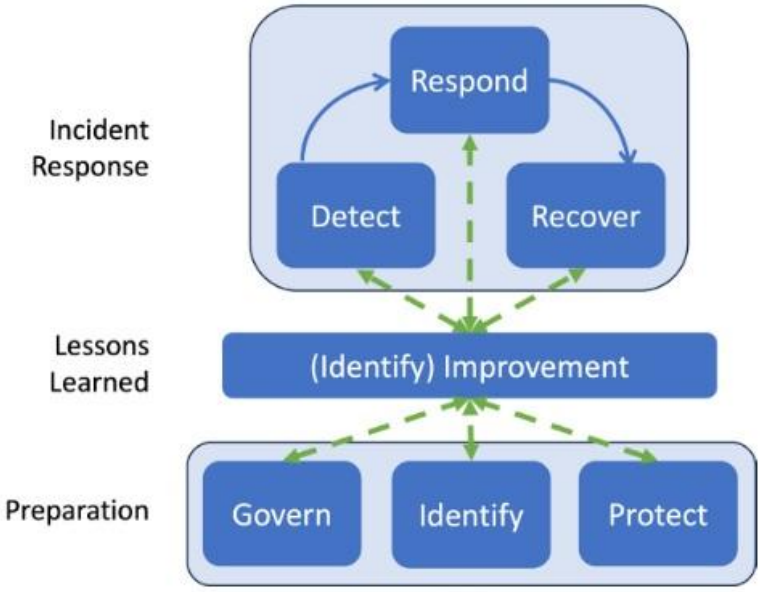

Рис. 2 – Узагальнена модель життєвого циклу реагування на інциденти на основі функцій CSF 2.0

Ключовими оновленнями Revision 3 є: повне узгодження з функціями, категоріями та підкатегоріями NIST CSF 2.0, впровадження рекомендацій щодо синхронізації планів безперервності бізнесу з процесами реагування, підкреслення значення постійного навчання персоналу та створення онлайн-ресурсу для оперативного оновлення практик реагування. В цілому, Revision 3 трансформує процес IR з операційно-орієнтованої моделі у інтегровану систему управління кіберризиками, що забезпечує ефективну і безперервну готовність організацій до сучасних загроз. [2]

Отже, еволюція NIST SP 800-61 від Revision 2 до Revision 3 демонструє перехід від статичних процедур реагування на інциденти до динамічної, інтегрованої моделі, яка поєднує підготовку, моніторинг, реагування та вдосконалення процесів у межах загальної стратегії управління кіберризиками.

Перелік посилань:

6. Реагуємо на кіберінциденти за NIST SP 800-61 Revision 2. *Інтернет журнал Кібербез*. [Електронний ресурс] – Режим доступу: https://cybersec.net.ua/normatyvni-dokumenty/812-reahuiemo-na-kiberintsydenty-za-nist-sp-800-61-revision-2.html

7. NIST Publishes Updated Incident Response Recommendations and Considerations / A. Fein et al. *Lexology*. [Електронний ресурс] – Режим доступу: https://www.lexology.com/library/detail.aspx?g=cd821288-c467-45dd-96ec-9600829896f0

Хорольський Костянтин Андрійович
Студент групи БСДМ-52, ННІКБЗІ ДУІКТ, Київ, Україна

Людський фактор як ключова причина компрометації корпоративних інформаційних систем

У сучасному цифровому світі інформаційна безпека стала критичним елементом сталого функціонування будь-якої організації. Від малих підприємств до великих корпорацій — усі залежать від технологій, які автоматизують бізнес-процеси, забезпечують зберігання даних та підтримують комунікації. Проте парадокс полягає в тому, що зростання рівня технологічної захищеності часто супроводжується підвищенням вразливості до людських помилок. Саме тому людський фактор розглядається як основне джерело ризиків у корпоративних інформаційних системах.

Ключові слова: людський фактор, фішинг, соціальна інженерія, навчання персоналу, багатофакторна автентифікація, корпоративна культура, кіберзагрози, безпека даних.

Під людським фактором у контексті кібербезпеки розуміють поведінкові та психологічні особливості користувачів, які можуть призвести до порушення політик безпеки або компрометації даних. Це можуть бути як ненавмисні дії — наприклад, відкриття фішингового листа, так і свідомі — у випадках внутрішніх загроз (insider

threats), коли співробітник навмисно розкриває інформацію або продає доступ до корпоративних систем.

За даними Verizon Data Breach Investigations Report (2024), близько 88% кіберінцидентів прямо або опосередковано пов'язані з людським чинником. Додаткові дослідження Cybersecurity Ventures свідчать, що загальні світові втрати від кібершахрайства у 2024 році перевищили 9,2 трильйона доларів, і значна частина цих збитків є наслідком неуважності або низької обізнаності персоналу[1].

Типові помилки користувачів залишаються незмінними: довіра до підозрілих листів, використання слабких або повторюваних паролів, нехтування оновленнями системи. У результаті таких дій навіть надійно захищені мережі можуть стати вразливими. Прикладом цього є інцидент із 23andMe, де зловмисники отримали доступ до даних через повторне використання паролів, або випадок із Optus, коли помилка в налаштуваннях API призвела до масштабного витоку клієнтської інформації.

Ситуація ускладнюється ще й тим, що люди схильні до «втоми від безпеки» (security fatigue). Коли працівникам постійно нагадують про політики, паролі, обмеження, вони поступово перестають сприймати це серйозно. Додатковим ризиком є культура толерантності до порушень — коли навіть керівники порушують правила безпеки, подаючи поганий приклад[2, с.14].

Для ефективної протидії людському фактору організаціям потрібно застосовувати комплексний підхід. Його складовими є:

- Навчання персоналу — регулярні тренінги, тестові фішингові кампанії, розвиток цифрової грамотності.
- Технічні заходи — багатофакторна автентифікація (MFA), політики складності паролів, контроль доступу та моніторинг дій користувачів.
- Психологічна підготовка — навчання критичному мисленню, моделювання соціальних атак, формування культури довіри, коли працівники не бояться повідомляти про підозрілі події.
- Організаційна культура — включення безпеки у цінності компанії, підтримка з боку керівництва, заохочення відповідальної поведінки.

В українських реаліях значення людського фактора набуває особливої актуальності. У період гібридної війни кібератаки на державні установи, банки та приватний бізнес стали щоденним викликом. Багато інцидентів, за даними Держспецзв'язку, відбуваються через фішинг, втрату доступу до корпоративних акаунтів або недбале поводження з носіями інформації. Отже, посилення культури безпеки в українських компаніях — не лише питання захисту даних, а й елемент національної стійкості.

Підсумовуючи, можна стверджувати, що людський фактор залишається головним викликом для сучасної кібербезпеки. Проте він може бути не лише слабкою ланкою, а й найкращим захистом — якщо організація перетворить своїх працівників на активних учасників безпеки. Ключ до цього — системне навчання,

усвідомлення ризиків та формування культури, у якій відповідальність за безпеку є спільною для всіх.

Перелік посилань:
1. Людський фактор у кібербезпеці: головна загроза та як її нейтралізувати URL: https://cases.media/article/lyudskii-faktor-u-kiberbezpeci-golovna-zagroza-ta-yak-yiyi-neitralizuvati?srsltid=AfmBOor1cJN5SyX55v-mTMJNnfdTNImxmADQsKnco0AYBA00cL26mk_J
2. Verizon Data Breach Investigations Report 2024 URL: https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf

Цапенко А.А.
*студентка групи Б-125-22-2-БІ, ДУ «*КАІ»*,*
Київ, Україна

МЕТОДИ ОБХОДУ СИСТЕМ ВИЯВЛЕННЯ ЗАГРОЗ ТА СИМУЛЯЦІЯ АТАК

У сфері забезпечення кібербезпеки корпоративних інформаційних систем основними захисними елементами є системи виявлення загроз, антивірусні програми та рішення для виявлення й реагування на інциденти на кінцевих точках. Проте, їхня ефективність постійно піддається випробуванню з боку зловмисників. Ця робота присвячена дослідженню технік обходу (Evasion) зазначених систем, а також на підходах до симуляції атак (Red Teaming), які є важливим інструментом для оцінки стійкості комп'ютерних інформаційних систем. Розглядаються сучасні методи приховування шкідливого програмного забезпечення, застосування легітимних засобів та проактивні методи тестування, які дозволяють організаціям підвищувати свій рівень кіберзахисту до рівня, адекватного сучасним загрозам.

Ключові слова: кібербезпека, корпоративні мережі, EDR, обхід захисту, Red Teaming, симуляція загроз, тестування на проникнення, MITRE ATT&CK.

Кібербезпека корпоративного середовища є динамічним процесом, який вимагає постійної адаптації до нових викликів. Системи AV та EDR, які є важливими механізмами захисту на кінцевих пристроях, використовують аналіз сигнатур, евристичні методи та моделі поведінки для виявлення та запобігання зловмисним діям. У відповідь на це зловмисники розробляють складні методи обходу, щоб приховати свої дії від цих механізмів захисту [1]. Сучасні кібератаки рідко базуються лише на завантаженні відомого вірусу, а використовують цілий арсенал технік, які адаптовані до конкретної мети та відповідають тактикам, задокументованим у фреймворку MITRE ATT&CK [3].

Одним із найпоширеніших і найефективніших методів є приховування шкідливого коду. Цей процес полягає у зміні структури коду без впливу на його функціональність, що дозволяє уникнути виявлення за допомогою сигнатур. Це можливо завдяки поліморфізму, коли кожна версія шкідливого програмного забезпечення має свою унікальну структуру. Крім того, використовуються пакувальники або шифрування для корисного навантаження, які декодуються тільки

при запуску пам'яті, або техніки, що перешкоджають аналізу, блокуючи виконання коду у віртуальних машинах або пісочницях, які часто використовуються системами EDR для динамічного аналізу [2]. Наприклад, деякі програми-вимагачі, такі як Maze і Conti, використовують складні методи стиснення та шифрування. Це ускладнює швидкий аналіз вмісту дослідниками та системами EDR, що призводить до тривалого процесу виявлення загроз.

Більш складні системи EDR використовують API hooking та моніторинг на рівні ядра для відстеження підозрілих системних викликів, особливо тих, що пов'язані з доступом до пам'яті, процесів та файлової системи. У цьому контексті методи ухилення можуть включати такі техніки «Un-Hooking» – відновлення оригінальних адрес системних функцій для уникнення моніторингу EDR, або використання прямих системних викликів (Direct Syscalls), що дозволяє зловмисному коду безпосередньо спілкуватися з ядром, оминаючи рівень користувача, де зазвичай знаходяться гачки систем EDR. Ці техніки є дуже технічними і часто використовуються на кінцевих етапах атаки для отримання постійного контролю.

Іншою важливою категорією є атаки «Living Off the Land» (LotL), які входять до тактик "Виконання" (Execution) та "Стійкість" (Persistence) ATT&CK. Цей метод полягає у використанні легальних інструментів, які вже доступні в цільовій CIS, для здійснення зловмисних дій. Серед цих інструментів можна назвати утиліти операційної системи, такі як PowerShell, WMIC (Windows Management Instrumentation Command-line), CertUtil або BITSAdmin [3]. Оскільки ці програми необхідні для нормального функціонування мережі підприємства, їхня діяльність зазвичай вважається дуже надійною, що ускладнює їх виявлення системами EDR, налаштованими на блокування лише певних відомих шкідливих виконуваних файлів. Конкретний приклад: група APT APT29 (також відома як Cozy Bear) активно використовувала PowerShell для виконання команд і інтерпретатор команд (cmd.exe) для виконання своїх скриптів, маскуючи свою діяльність під виглядом звичайних адміністративних завдань. Ефективність цих атак змушує захисників перейти від моніторингу файлів до моніторингу поведінки та розробки моделей нормальної поведінки користувачів і систем (UEBA – User and Entity Behavior Analytics) [4].

Для проактивного виявлення слабких місць і підтвердження стійкості CIS до цих складних загроз використовується методологія імітації атак (Red Teaming). Red Teaming – це масштабне, багатоетапне і реалістичне тестування безпеки, яке імітує реальну діяльність груп висококваліфікованих кіберзлочинців (Advanced Persistent Threat – APT). На відміну від традиційних тестів на проникнення (Penetration Testing), цілі Red Teaming є ширшими, а сфера його застосування – менш обмеженою, з акцентом на досягненні конкретної комерційної мети (крадіжка критичних даних або переривання роботи важливої служби) і оцінюючи не тільки технічний захист, але й здатність команди безпеки (Blue Team) виявляти, аналізувати та реагувати на такі атаки [4].

Процес Red Teaming включає такі важливі етапи, які детально відображають життєвий цикл APT-атаки (Cyber Kill Chain): дослідження (збір інформації про ціль), озброєння (створення інструментів обходу – C2-frameworks), доставка (інфільтрація, часто за допомогою фішингу), експлуатація (використання вразливостей), контроль (створення опору), бічний рух (Lateral Movement) і виконання місії [2].

Команди Red Team використовують фреймворк MITRE ATT&CK для проектування, впровадження та звітності. Це забезпечує Red Team можливість точно імітувати певну групу APT, а Blue Team — порівнювати виявлені інциденти з відомими зловмисниками, надаючи вичерпну базу знань про тактики (наприклад, «Credential Access») та техніки (наприклад, «OS Credential Dumping»), які використовують кіберзлочинці [3]. Використання цієї рамки гарантує об'єктивність і повторюваність симуляції. Наприклад, команда Red Team може вирішити імітувати техніки групи Lazarus APT (використовуючи утиліту certutil.exe для завантаження файлів) і таким чином перевірити, чи може система EDR організації виявити нестандартне, але законне використання системної утиліти в зловмисних цілях.

Основним результатом Red Teaming є не тільки перелік виявлених технічних вразливостей, але й кількісна та якісна оцінка функціональної ефективності захисних механізмів (AV, EDR, SIEM, WAF) та процесів реагування. Якщо Red Team зможе здійснити свою атаку, не будучи виявленою Blue Team, це свідчить про критичні недоліки в області видимості та моніторингу. Навіть якщо система EDR не змогла запобігти атаці, вона повинна була надати достатньо телеметричних даних для судового аналізу. Недотримання вимог щодо збору достатньої кількості телеметричних даних є такою ж серйозною проблемою, як і пропущена вразливість.

Успішний процес Red Teaming сприяє об'єднанню команд Red і Blue; таке об'єднання називається Purple Teaming. Цей підхід передбачає спільну діяльність, в рамках якої Red Teaming демонструє атаки, а Blue Teaming негайно тестує інструменти та процедури виявлення, адаптуючи їх у режимі реального часу. Це сприяє швидшому посиленню заходів безпеки та вдосконаленню процесів виявлення загроз, підвищуючи рівень кіберстійкості CIS. Цей проактивний і практичний підхід є дуже важливим для надійного захисту корпоративної інформації в світі, де кіберзагрози стають дедалі складнішими [4]. Тому обхід систем захисту та імітація атак є двома протилежними сторонами одного й того самого явища: з одного боку, це інструмент для злочинців, а з іншого — важливий засіб для контролю та посилення безпеки інфраструктури підприємства.

Перелік посилань:

1. MITRE. The MITRE ATT&CK Framework [Електронний ресурс]. – Режим доступу: https://attack.mitre.org/

2. Курачинська А. Р., Єфіменко А. А. Методології та методи тестування на проникнення : навч. посіб. – Житомир : Державний університет «Житомирська політехніка», [б.р.].

3. Jiang Yuning, Meng Qiaoran, Shang Feiyang, Oo Nay, Le Thi Hong Minh, Lim Hoon Wei, Sikdar Biplab. MITRE ATT&CK Applications in Cybersecurity and The Way Forward. – 2025.

4. Red Team Operations and Adversary Simulation [Електронний ресурс]. – SANS Institute, 2022. – Режим доступу: https://www.sans.org/

Tsarova Sofiia Valeriivna
student of group BSDM-51, ESI IS, SUICT,
Kyiv, Ukraine

CYBERTHREATS PREVENTION BY PHISHING SIMULATION CAMPAIGNS

Phishing is one of the most popular and costly cyberthreats organizations face today. It may lead to severe consequence such as limited to credentials theft, remote access malware or ransomware installation. Therefore, confidentiality, integrity and availability of corporate data are directly compromised and it makes phishing a serious risk that must be treated properly. While technical controls like EDR and SIEM are vital for detecting system exploitation attempts, employee security awareness and their ability to detect and respond to phishing threats are very important to prevent cyberattacks in the first place. This paper aims to study the effective implementation of phishing simulations as an organizational control to prevent cyberthreats.

Key words: security awareness, phishing simulations.

Phishing remains the dominant initial vector of attack. The main reasons are the simplicity of preparing phishing campaigns and the fact that human element is still the weakest link in information security systems.

Availability of such services as GoDaddy and Hostinger as well as AI-based services (ChatGPT, Gemini etc.) allows threat actors to create numerous cheap spoofing domains and compose good-looking and grammatically correct phishing emails without any special technical knowledge.

The usual way to trick the users into providing credentials or downloading infected files is the use of spoofed links or malicious attachments. The dominant types of attachments are HTML and PDF files that contain embedded JavaScript code or links that can trigger malware download or redirect to malicious websites.

An easy evasion technique for these attacks is to compress them into RAR or ZIP archives that are protected with passwords. Email-clients such as Gmail or Outlook, which are very popular corporate email services nowadays, cannot scan password-protected archives for malware so the attackers can avoid this type of technical detection [1].

As technical solutions cannot always prevent email-based attacks, security awareness of users is one of the key parts of protecting corporate data. Unfortunately, human traits such as curiosity, carelessness or a sense of trust towards famous brands and services (e. g. Google Workspace or Microsoft 365) as well as the lack of knowledge about phishing make them vulnerable to social engineering techniques that are used by attackers during email attacks.

Therefore, organizational and educational controls must be implemented within companies to ensure their employees are aware of modern cyberthreats and how to detect and them. One of these controls is regular phishing simulations.

Phishing simulation is an educational campaign that is based on sending employees emails that mimic traditional phishing emails and attempt to deceive employees into clicking links, downloading files or providing credentials.

In general, phishing simulation campaigns are developed either for the whole staff of the organization or are tailored to the specific unit and its business operations.

When preparing and performing effective phishing simulation, the information security team should take into consideration the following aspects of the campaign:

- relevance – the phishing emails have to be customized to reflect the realistic threats specific to the organization, that may include mimicking correspondence of the vendors, the company works with, or imitating communication with internal representatives, such as CEO;
- complexity – the simulated phishing emails should represent both typical phishing signs and more sophisticated techniques to encourage the employees to develop stronger analytical skills;
- feedback – the information security team should provide additional trainings on the phishing detection and reporting for employees who failed during the phishing simulation campaigns. It includes assigning additional information security courses about social engineering and phishing as well as performing additional simulations specific for these employees' responsibilities.

The phishing simulation campaign success and its impact on users' ability to recognize and respond to phishing threats heavily relies on the proper reporting and analysis. There should be a detailed report on the phishing simulation results which then will be presented to the Chief Information Security Officer.

The common metrics that should be gathered and analyzed are the percentage of employees who have fell for the phishing attempt and the percentage of employees who have correctly identified and reported it. These metrics demonstrate the effectiveness of the awareness program implemented in the organization and help the information security team to improve it in accordance with current security risks [2].

In conclusion, phishing simulation is an effective tool to improve company's information security posture by improving employees' ability to recognize and respond to phishing threats. User awareness and response at the very beginning of an email attack help avoid financial, reputational and time losses because of potential data breach or systems infection.

References:

1. The State of Cyber Security. Check Point Research, 2025. URL: https://www.checkpoint.com/security-report/.

2. Vamshi Krishna, B., Karthik Reddy, C., Latha, K., Akshitha, M., & Aparna, D. G. (2024). PHISHING SIMULATIONS. NTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT, 9(11), 866–869. https://ijnrd.org/papers/IJNRD2411184.pdf.

Черненко Д. А.
студентка групи БСДМ-52, ННІКБЗІ ДУІКТ,
Київ, Україна

ОЦІНКА ЕФЕКТИВНОСТІ ЗАХОДІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У сучасних умовах розвиток цифрових технологій супроводжується зростанням кіберзагроз та зростанням складності захисту інформаційних систем. Організації і державні установи впроваджують різноманітні технічні й організаційні заходи інформаційної безпеки , та постає питання: наскільки ці заходи ефективні?

Оцінка ефективності заходів інформаційної безпеки дає змогу визначити, чи реально вони зменшують ризики, забезпечують стійкість інформаційних систем та підвищують рівень захищеності. У цьому контексті особливо важливо розуміти, що ефективність не вимірюється лише наявністю політик або технічних засобів, а фактичним результатом їх застосування.

Ключові слова: кіберзагрози, ризик, кіберстійкість, оцінка, методи, ефективність.

Ефективність заходів інформаційної безпеки визначається через комплекс показників, серед яких:

- ризик - ймовірність виникнення інциденту та очікувані збитки;
- кіберзахищеність - ймовірність того, що система витримає атаку;
- працездатність системи - здатність продовжувати виконувати свої функції після кібератаки;
- кіберстійкість - здатність швидко відновлюватися після інцидентів.

Розрахунок ризику здійснюється за формулою:

$$R=P\times Z,$$

де P - ймовірність атаки, Z - потенційні збитки. Через відсутність повної статистики або точних даних використовують експертні оцінки та якісні шкали (дуже низький, низький, середній, високий, критичний). Це дозволяє проводити оцінку навіть у умовах обмеженої інформації.

Також передбачається врахування людського фактора. Ефективність заходів залежить не лише від техніки, а й від того, наскільки користувачі дотримуються політик і процедур.

Етапи практичного застосування методики оцінювання ефективності заходів інформаційної безпеки:

Етап 1. Розробка системи показників - на цьому етапі визначаються конкретні показники та критерії оцінювання, адаптовані до специфіки об'єкта захисту. Формується перелік індикаторів для різних компонентів системи забезпечення інформаційної безпеки.

Етап 2. Планування збору даних - здійснюється підготовка до впровадження системи вимірювання, планування доступу до необхідних даних, розробка процедур обробки та розповсюдження інформації про значення показників. Вихідні дані отримуються за результатами аудиту об'єктів інформаційної інфраструктури.

Етап 3. Обчислення показників - проводиться збір емпіричних даних та обчислення значень обраних показників ефективності. При розрахунку значень ймовірності кібератак та рівня можливого збитку застосовуються:

- статистичні методи (аналіз історичних даних про інциденти);
- експертні оцінки (думки фахівців з інформаційної безпеки);
- елементи теорії прийняття рішень (для складних ситуацій невизначеності).

Етап 4. Інтерпретація результатів - на завершальному етапі здійснюється аналіз отриманих даних та формулювання висновків щодо ефективності заходів захисту.

Якщо виявлено недостатній рівень захищеності, розробляються практичні рекомендації з підвищення ефективності системи забезпечення інформаційної безпеки.

Для опису результатів оцінки ефективності використовуються:

- кіберзахищеність системи (P_kз) - оцінюється від 0 до 1;
- збитки (Z) - за п’ятибальною шкалою: малий, помірний, середній, великий, критичний;
- зниження ризику після впровадження заходів - показує динаміку ефективності.

Значення P_kз інтерпретуються як:

- 0 - 0,25 - незадовільний рівень;
- 0,25 - 0,5 - низький;
- 0,5 - 0,75 - середній;
- 0,75 - 0,9 - високий;
- 0,9 - 1 - максимальний.

Таким чином, можна визначити, які заходи працюють, а які потребують коригування. Наприклад, якщо ризик зменшився після впровадження моніторингу інцидентів і навчання персоналу, це свідчить про їхню ефективність. Водночас заходи, що не вплинули на показники, потребують перегляду або заміни.

Ефективність заходів не обмежується лише технічними характеристиками. Важливо враховувати:

- економічну доцільність - витрати на заходи не повинні перевищувати потенційні збитки;
- постійне оновлення та тестування - системи і процедури мають адаптуватися до нових загроз;
- короткий цикл оцінки - оцінювання має проводитися регулярно, а не одноразово.

Особливість українських реалій полягає в тому, що часто заходи безпеки впроваджуються формально, а моніторинг і оцінка ефективності залишаються на низькому рівні. Реальні інциденти показують, що без постійної практичної перевірки та адаптації заходів система може залишатися вразливою.

Перелік посилань:

1. Козубцова Л.М., Юрій Іванович Хлапонін Ю.І., Козубцов І.М. Методика оцінювання ефективності виконання заходів забезпечення кібербезпеки об’єктів критичної інформаційної інфраструктури організацій. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2021. Т. 41. № 2. С. 17–22. DOI: https://doi.org/10.33099/2311-7249/2021-41-2-17-22 .
2. Петренко К. Удосконалена методика оцінювання ефективності системи забезпечення інформаційної безпеки Міністерства Оборони та Збройних Сил України. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2022. Т. 45. № 3. С. 97–100. DOI: https://doi.org/10.33099/2311-7249/2022-45-3-97-100 .

Юсипів М.С.
Студент групи 125м-24-1, НТУ «ДП»,
Дніпро, Україна

ВИКЛИК СУЧАСНИМ ЗАГРОЗАМ. ЗРОСТАЮЧА ЦІННІСТЬ ПОЛІТИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ. ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ.

Політики безпеки є одним із найважливіших понять у захисті інформації. Політики безпеки встановлюють рамки функціонування бізнесу, правила поводження з інформаційними ресурсами та захист інформації в ІКС. Політики безпеки мають обов'язковий характер впровадження через вимоги стандартів, таких як галузеві, державні, місцеві чи міжнародні, які вимагають наявності даних документів, а також через важливість та вплив політик на бізнес-процеси організацій.

Ключові слова: політика безпеки, захист інформації, кіберпростір, інформаційне середовище, об'єкти критичної інфраструктури, політика інформаційної безпеки, захист інформації.

Політика інформаційної безпеки - документ або сукупність документів системного рівня, які містять набір вимог, правил, обмежень, рекомендацій, що регламентують порядок інформаційної діяльності в ІС і спрямовані на досягнення і підтримку стану інформаційної безпеки системи та організації в цілому. [1, с.3]

У сучасному світі політика інформаційної безпеки відіграє дедалі вагомішу роль. Виклики сьогодення, такі як використання ШІ, дипфейки, фішингові атаки, соціальна інженерія, зловмисне програмне забезпечення ставлять під загрозу безпечне існування людини у кіберпросторі. Україна не виключення з правил, а навпаки Україна знаходиться на вістрі боротьби у кіберпросторі з рф, яка переважає, як ресурсно так і фінансово. В Україні як і в усьому світі є проблеми з забезпеченням безпеки держави у кіберпросторі. Активний розвиток інформаційних технологій ставить під загрозу сталий розвиток цілих держав, тому політика інформаційної безпеки відіграє більшу роль, держава будує свої політики таким чином, щоб суспільство могло розвиватися соціально, політично, економічно й технологічно. Розвиток інформаційних технологій призвів до того, що злочини у інформаційному середовищі несуть руйнівний вплив на економіку й безпеку цілих країн й суспільств. З кожним роком виклики, які ставляться перед політичними діячами, експертному середовищі з КБ потребують більшої уваги до зростаючих загроз, цілі корпорації збільшують штати співробітників, створюються нові відділи, які забезпечують безпечне функціонування компанії й організовують безпеку бізнес-процесів.

Інформаційна безпека не може бути забезпечена без розвитку інформаційно-телекомунікаційної інфраструктури й законодавчого регулювання захисту інформації. Україна пройшла величезний шлях трансформації законодавства після неспровокованої російської агресії проти України й анексії Криму. З 2014-го року Україна суттєво оновила нормативно-правові акти й впроваджує нові закони, стандарти, постави, покращує регулювання сфери інформаційної безпеки. Україна була першою країною, яка на собі зрозуміла, що таке велика, добре спланована кібератака. Найбільша кібератака в світі на телекомунікаційну мережу була скоєна на базі оператору мобільного зв'язку ПрАТ «Київстар», також величезні за розмірами атаки були скоєні на об'єкти критичної інфраструктури, державні

компанії, елементи електронного урядування тощо. Україна має доволі розгалужену систему реагування, запобігання, мінімізації наслідків, розслідування й навіть кібератак в інформаційному середовищі. В Україні діють величезна кількість нормативно-правових актів у сфері інформаційної безпеки, найголовніші, це закони, постанови, нормативні документи з технічного захисту інформації, державні стандарти України.

Політики інформаційної безпеки повинні розвиватися в такому темпі, щоб не відставати від розвитку загроз. Атака на ПрАТ «Київстар» показала, що багато об'єктів критичної інфраструктури (далі - ОКІ) не мають альтернативного зв'язку. Під час збоїв у будь-якого оператора мобільного зв'язку інші ОКІ можуть зупинити, призупинити чи суттєво скоротити своє функціонування та автономність, тим самим ставлячи під загрозу безпеку суспільства й держави. Розвиток ШІ створює суттєві проблеми для всіх організацій у всьому світі. Соціальна інженерія та діпфейки стають дедалі більш загрозливими явищами для цілих корпорацій. Політики інформаційної безпеки та їх складові можуть бути ось тим ключем для захисту від цих зростаючих загроз.

Перелік посилань:

1. Методичні рекомендації щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесами: ДССЗ та ЗІ України від 29 травня 2023 року N 463, 3 с. [Електронний ресурс]. – Режим доступу https://ips.ligazakon.net/document/view/fn077605?an=27&ed=2023_05_29

Чечик М.О.
студент групи БСДМ-61, ННІЗІ ДУІКТ, Київ, Україна

TECHNOLOGY FOR OPTIMIZING SIEM RULES IN WAZUH FOR ANOMALY DETECTION AND REDUCING FALSE POSITIVES

Annotation

The thesis explores methods and technologies for optimizing rule configurations within SIEM systems, focusing on Wazuh as an open-source platform for security monitoring and incident detection. The study analyzes the challenges of false positives, detection accuracy, and rule correlation efficiency in the context of large-scale log environments. Emphasis is placed on developing an optimization methodology based on statistical analysis of alert frequency, machine learning–assisted anomaly identification, and dynamic rule adjustment. The research also considers integration with external threat intelligence and automated response mechanisms to improve the overall accuracy and speed of incident handling.

Modern organizations process vast amounts of event data generated by endpoints, servers, and network devices. Wazuh, as a modular SIEM solution, provides a framework for centralized log collection, correlation, and response automation. However, as the number of active rules and monitored nodes increases, the number of false positives tends

to grow exponentially, leading to analyst fatigue and delayed reaction to genuine incidents. The primary objective of SIEM rule optimization is therefore to enhance detection precision by adapting correlation logic to real operational contexts and minimizing redundant alerts without compromising security visibility.

The optimization process is divided into several key stages. Initially, the raw alert dataset is analyzed to determine event frequency, repetition rate, and statistical deviation from the baseline. This information enables the identification of redundant or overlapping correlation rules that trigger multiple alerts for identical or related events. The next step involves introducing weighting coefficients for rules based on the reliability of data sources, which allows Wazuh to prioritize alerts from critical assets while reducing the impact of noisy inputs [1]. Further enhancement is achieved through the use of anomaly detection algorithms—such as Isolation Forest and Local Outlier Factor—that learn the normal behavior of system metrics and identify deviations indicative of potential attacks. These algorithms can be implemented through Wazuh's integration with Elastic Machine Learning or through external Python-based modules that feed results back into the rule engine [2].

A significant contribution of the proposed approach lies in the dynamic recalibration of correlation rules using feedback from security analysts. Each alert can be assigned a verification label ("true positive" or "false positive"), forming a dataset that continuously improves the scoring mechanism and adjusts rule thresholds accordingly. The process results in an adaptive SIEM environment capable of maintaining a balance between sensitivity and specificity. The following table summarizes the comparative efficiency of Wazuh before and after rule optimization based on an empirical study conducted in a corporate testbed [3].

Parameter	**Baseline Configuration**	**Optimized Configuration**	**Improvement**
Total alerts per day	10,000	3200	−68%
False positive rate	42%	9%	−78%
Average detection latency	12 s	7 s	+41%
Analyst workload (tickets/day)	120	45	−62%

As demonstrated, the reduction of false positives significantly improves the signal-to-noise ratio, allowing analysts to focus on high-priority events. The results indicate that automated rule tuning and feedback-driven threshold adaptation provide measurable efficiency gains in both detection accuracy and operational workload. Additionally, the integration of Wazuh with external threat intelligence feeds such as MISP and VirusTotal enhances contextual awareness, enabling better correlation of alerts with known malicious indicators [4]. Future developments of this research will include the implementation of reinforcement learning models for predictive rule optimization and the assessment of their impact on real-time detection performance in heterogeneous network environments.

References

[1] Wazuh, *"Wazuh Documentation: Detection Rules and Decoders,"* 2025. Available at: https://documentation.wazuh.com

[2] Scarfone, K., Grance, T., & Masone, J., *"Guide to Computer Security Log Management,"* NIST Special Publication 800-92, National Institute of Standards and Technology, 2023.

[3] Sarker, I. H., *"Machine Learning-Based Cybersecurity: State-of-the-Art and Future Directions," Journal of Network and Computer Applications*, vol. 208, 2024.

[4] Ahmed, M., Mahmood, A. N., & Hu, J., *"A Survey of Network Anomaly Detection Techniques," Journal of Network and Computer Applications*, vol. 60, pp. 19–31, 2022.

Комісарук Антон Володимирович,
студент групи ПДМ-61,
спеціальність 121 Інженерія програмного забезпечення,
Державного університету інформаційно-комунікаційних технологій
komisar10001@gmail.com
Науковий керівник: Залива Віталій Вікторович,
доктор філософії (PhD), старший викладач кафедри кафедри Інженерії програмного забезпечення
Державного університету інформаційно-комунікаційних технологій

МЕТОДИКИ ЗАХИЩЕНОГО ОБМІНУ КАДРОВИМИ ДАНИМИ ВІЙСЬКОВОСЛУЖБОВЦІВ: РИЗИКИ ТА ШЛЯХИ МІНІМІЗАЦІЇ

Цифрова трансформація Збройних Сил України є ключовим елементом підвищення їхньої ефективності та оперативної спроможності в умовах сучасної війни. Впровадження новітніх технологій, таких як екосистема «Армія+» та інші цифрові продукти, докорінно змінює підходи до ведення збройної боротьби. Ефективний та захищений обмін даними військовослужбовців є основою для оперативного управління, кадрового забезпечення та соціального захисту. Проте, зі зростанням цифровізації, пропорційно зростають і кіберзагрози, роблячи військові інформаційні системи стратегічною ціллю для ворога. Забезпечення кібербезпеки в методиках обміну кадровими даними військовослужбовців є критично важливим елементом національної безпеки та військової готовності.

Постановка задачі

Незважаючи на переваги цифровізації, вона створює нові кіберризики для кадрових даних військовослужбовців. Застарілі паперові процеси, проблеми сумісності систем, неактуальність даних та кібератаки формують вразливості, що можуть підірвати ефективність управління та безпеку персоналу. Завдання полягає в ідентифікації цих ризиків та розробці шляхів їх мінімізації для забезпечення конфіденційності, цілісності та доступності військових даних.

Мета дослідження

Метою дослідження є аналіз кібербезпекових ризиків обміну кадровими даними військовослужбовців в умовах цифровізації оборонного сектору України та розробка рекомендацій для їх мінімізації, включаючи архітектурні, технологічні та організаційні рішення.

Результати дослідження

1. Актуальні кіберзагрози та вразливості в системах обміну кадровими даними військовослужбовців

Цифровізація військового обліку та управління персоналом в Україні («Оберіг», «Резерв+», «Армія+») значно підвищує ефективність, але водночас розширює поверхню для потенційних кібератак.

Цінність та чутливість даних: Військові дані є стратегічною ціллю для ворога; їх витік або спотворення може мати катастрофічні наслідки.

Паперові процеси та людський фактор: Залишки "паперової армії" , ручне внесення даних та бюрократія створюють вразливості та призводять до неактуальності інформації.

Проблеми сумісності та інтероперабельності: Несумісність з НАТО стандартами та відсутність відкритих API , а також надмірна засекреченість , ускладнюють інтеграцію та захист.

Якість та актуальність даних: Неактуальність інформації або некоректне відображення даних у застосунках можуть призвести до операційних помилок та підірвати довіру.

Ризики хмарних технологій: Використання хмарних сервісів потребує посиленого захисту, особливо при розміщенні в іноземних сховищах.

2. Шляхи мінімізації кіберризиків та забезпечення захисту даних

Для ефективного захисту кадрових даних військовослужбовців необхідний комплексний підхід, що охоплює законодавчі, архітектурні, технологічні та організаційні аспекти.

Законодавче та нормативне регулювання: Обробка даних має відповідати принципам Конвенції 108 (пропорційність, чесність, прозорість, точність) , а законодавство має бути гармонізоване з цифровими процесами.

Архітектурні підходи до захисту:

Побудова комплексної системи захисту інформації (КСЗІ 2.0) для забезпечення конфіденційності, цілісності та доступності даних.

Застосування принципу мінімізації доступу , використання захищених мереж (VPN, firewalls) та шифрування даних.

Впровадження передових методів аутентифікації, таких як ключі безпеки FIDO.

Роль архітектур даних (Data Lake/Lakehouse, Data Mesh) у безпеці:

Data Lake/Lakehouse: Забезпечення вбудованих механізмів безпеки (управління ідентифікацією та доступом, шифрування, маскування, аудит) для зберігання та аналізу великих обсягів даних.

Data Mesh: Децентралізований підхід до зберігання даних, де дані розглядаються як продукт, що належить домену, підвищує стійкість системи та швидкість доступу до даних, зменшуючи єдині точки відмови.

Розвиток цифрових компетентностей та культури кібербезпеки:

Навчання та перекваліфікація персоналу з кібергігієни та цифрової грамотності.

Формування "цифрової довіри" та повне виключення паперового документообігу для підвищення оперативності та безпеки.

Висновки та перспективи

Україна досягла значних успіхів у цифровізації оборонного сектору, оптимізувавши кадрові процеси та зменшивши бюрократію через системи «Оберіг», «Резерв+», «Армія+» та інші. Проте, існують значні виклики: застарілі паперові процеси, проблеми сумісності систем з міжнародними стандартами, забезпечення точності даних та постійне посилення кібербезпеки.

Шлях вперед передбачає подальше вдосконалення методик обміну даними та архітектурних рішень, зокрема перехід до децентралізованих моделей (Data Mesh) для підвищення стійкості та оперативності. Інтеграція штучного інтелекту та машинного навчання дозволить перейти до предиктивного аналізу. Посилення кібербезпеки має бути наскрізним процесом, вбудованим у кожен аспект трансформації. Розвиток цифрових компетентностей та формування нової організаційної культури є критично важливими. Повна інтеграція даних забезпечить Україні оперативну перевагу та створить основу для сучасної, ефективної та інтероперабельної з НАТО армії майбутнього.

Список використаних джерел

1. Вігер, С. Цифрова трансформація ЗСУ: як інновації змінили принципи ведення війни та управління військами у 2024 році. [Електронний ресурс]. Режим доступу: https://i-vin.info/news/cifrova-transformaciya-zsu--yak-innovaciyi-zminili-principi-vedennya-viyni-ta-upravlinnya-viyskami-u-2024-roci-11069.html
2. Міністерство оборони України. Міноборони активно впроваджує новітні технології для зміцнення війська. [Електронний ресурс]. Режим доступу: https://censor.net/ua/tag/1743/minoborony
3. Міністерство оборони України. Зручні сервіси та вихід на міжнародні ринки: як ДП Міноборони «Цифрова Армія» допомагатиме військовим, цивільним і бізнесу. [Електронний ресурс]. Режим доступу: https://mod.gov.ua/news/zruchni-servisi-ta-vihid-na-mizhnarodni-rinki-yak-dp-minoboroni-czifrova-armiya-dopomagatime-vijskovim-czivilnim-i-biznesu
4. Міністерство оборони України. Візія, мета та строки реалізації Стратегії. [Електронний ресурс]. Режим доступу: https://www.mil.gov.ua/content/public_discussion/03_09_2024_proiekt_nakazu.pdf