МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

КАФЕДРА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ

СТРАТЕГІЇ КІБЕРСТІЙКОСТІ: УПРАВЛІННЯ РИЗИКАМИ ТА БЕЗПЕРЕРВНІСТЬ БІЗНЕСУ

Матеріали Всеукраїнської науково-практичної конференції

25 лютого 2026 року

КИЇВ - 2026

УДК: 004.056

Рекомендовано до друку Вченою радою Навчально-наукового інституту кібербезпеки та захисту інформації Державного університету інформаційно-комунікаційних технологій

(протокол № 9 від 10.03.2026 р.)

Стратегії кіберстійкості: управління ризиками та безперервність бізнесу:

Матеріали Всеукраїнської науково-практичної конференції (м. Київ, 25 лютого 2026 року) / Навчально-науковий інститут кібербезпеки та захисту інформації ДУІКТ. Київ, 2026. 223 с.

Збірник призначений для науковців, викладачів, докторантів, аспірантів і студентів закладів вищої освіти, фахівців з інформаційної та кібернетичної безпеки, працівників органів державної влади та місцевого самоврядування.

ЗМІСТ

СЕКЦІЯ 8. ЗАКОНОДАВЧА Й НОРМАТИВНА ОСНОВА ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ

СЕКЦІЯ 1. СУЧАСНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОСТІ БІЗНЕСУ

УПРАВЛІННЯ ПОВЕДІНКОЮ ПЕРСОНАЛУ ЯК КЛЮЧОВИЙ ФАКТОР ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОСТІ БІЗНЕСУ В УМОВАХ КІБЕРЗАГРОЗ

Ляшенко М. С.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

У сучасних умовах кіберзагроз управління поведінкою персоналу перетворилося з допоміжного елемента на стратегічний фактор кіберстійкості організації. Згідно з дослідженням Verizon DBIR 2025 року, 68 % порушень безпеки пов’язані саме з людським фактором [1], що підкреслює необхідність переходу від реактивних заходів до проактивного управління поведінкою.

Сучасні підходи базуються на поєднанні кількох наукових теорій: теорії запланованої поведінки (Ajzen, 1991) [2], теорії захисту мотивації (Rogers, 1975) та nudge-теорії (Thaler & Sunstein, 2008) [3]. На їхній основі компанії впроваджують комплексні програми, які включають регулярні симуляції фішингових атак з персоналізованим зворотним зв’язком, системи gamification та поведінкові інтервенції. Дослідження Ponemon Institute (2024) відобразило, що організації з високим рівнем зрілості програм управління поведінкою демонструють на 74 % менше успішних соціально-інженерних атак порівняно з компаніями, які обмежуються формальними тренінгами

Забезпечення безперервності бізнесу (Business Continuity Management) у контексті кіберзагроз безпосередньо залежить від того, наскільки ефективно керована поведінка співробітників під час інцидентів. Стандарт ISO 22301:2019

прямо вимагає включення людського фактора до планів безперервності як одного з критичних ресурсів [4].

Аналіз реальних інцидентів свідчить, що час відновлення бізнес-процесів (MTTR) суттєво залежить від рівня підготовленості персоналу. Компанії, які інтегрували програми управління поведінкою в свої BCP-плани, скорочували час простою в середньому на 42–57 % (Gartner, 2025). Особливо критичним це є для підприємств критичної інфраструктури. Тому сучасні моделі забезпечення кіберстійкості (NIST Cybersecurity Framework 2.0) розглядають управління поведінкою персоналу як окремий ключовий елемент [5].

Управління поведінкою персоналу є не лише елементом культури безпеки, а й одним із найважливіших детермінантів забезпечення безперервності бізнесу в умовах зростаючих кіберзагроз. Перехід від традиційних тренінгів до науково обґрунтованих поведінкових програм дозволяє суттєво підвищити стійкість організацій. Подальші дослідження мають бути спрямовані на розробку кількісних моделей оцінки ефективності таких програм та їх інтеграцію в корпоративні системи управління ризиками.

Література

1. Verizon. 2025 Data Breach Investigations Report. URL: https://www.verizon.com/business/resources/reports/dbir/ (дата звернення: 24.02.2026).

2. Ajzen I. The theory of planned behavior // Organizational Behavior and Human Decision Processes. 1991. Vol. 50. P. 179–211.

3. Thaler R.H., Sunstein C.R. Nudge: Improving Decisions About Health, Wealth, and Happiness. New Haven: Yale University Press, 2008.

4. ISO 22301:2019. Security and resilience — Business continuity management systems — Requirements. Geneva: ISO, 2019.

5. National Institute of Standards and Technology. NIST Cybersecurity Framework 2.0. Gaithersburg, 2026.

КІБЕРСТІЙКІСТЬ ПІДПРИЄМСТВА ЯК ЕЛЕМЕНТ УПРАВЛІННЯ РИЗИКАМИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Ненько В. Р.
Державний університет інформаційно-комунікаційних технологій
м. Київ, Україна

Актуальність дослідження зумовлена трансформацією кіберзагроз у сучасному цифровому середовищі, особливо в умовах гібридної війни, що поєднує військові, інформаційні, психологічні та кібернетичні впливи на державні структури, бізнес і критичну інфраструктуру. У таких умовах підприємства стають об'єктами цілеспрямованих атак, спрямованих не лише на технічні системи, а й на персонал, який виступає найбільш уразливою ланкою системи безпеки. Наслідком цього є фінансові втрати, порушення безперервності бізнес-процесів і зниження рівня довіри до підприємства.

В умовах гібридної війни кіберпростір стає одним із ключових середовищ реалізації деструктивних впливів на державні установи, критичну інфраструктуру та приватні підприємства. Сучасні кіберзагрози характеризуються високим рівнем складності, цілеспрямованістю та поєднанням технічних і соціально-психологічних методів впливу [1]. До найбільш поширених загроз належать фішингові атаки, атаки соціальної інженерії, шкідливе програмне забезпечення, DDoS-атаки та цілеспрямовані атаки на корпоративні інформаційні системи. У період гібридних конфліктів посилюється інформаційно-психологічний тиск і використання кіберінструментів для дестабілізації діяльності підприємств, що підвищує рівень кіберризиків.

Особливу небезпеку становлять інформаційно-психологічні впливи, спрямовані на маніпулювання свідомістю, зниження рівня критичного мислення та порушення ментальної стійкості користувачів, що підвищує ефективність атак соціальної інженерії та інших кіберзагроз. У таких умовах

стратегічним пріоритетом стає перехід від статичної моделі кібербезпеки, орієнтованої переважно на захист ресурсів, до динамічної моделі кіберстійкості.

Кіберстійкість підприємства є комплексною характеристикою, що відображає здатність організації забезпечувати безперервність функціонування інформаційних систем, зберігати конфіденційність, цілісність і доступність даних, а також ефективно протидіяти сучасним кіберзагрозам. Вона інтегрує процеси управління ризиками, інформаційної безпеки та забезпечення безперервності діяльності, формуючи цілісну систему захисту [2].

Для системної реалізації такого підходу доцільним є використання доменної моделі кібербезпеки, що передбачає структуризацію захисту за ключовими функціональними сферами: управління доступом та ідентифікацією, захист даних і мережева безпека, безпека персоналу та протидія соціальній інженерії, управління інцидентами та кіберризиками. Такий підхід дозволяє комплексно оцінювати вразливості підприємства, інтегрувати управління кіберризиками в загальну систему менеджменту та формувати адаптивну архітектуру захисту з урахуванням технічних і організаційних чинників.

Отже, в умовах гібридної війни кіберстійкість підприємства виступає стратегічним елементом управління ризиками, що забезпечує захист інформаційних ресурсів, стійкість до інформаційно-психологічних впливів і безперервність бізнес-процесів. Формування кіберстійкої системи управління безпекою, заснованої на доменному підході та розвитку культури безпеки персоналу, є необхідною умовою стабільного функціонування підприємства в умовах постійного зовнішнього тиску.

Література

1. Пашковський В. Ф. Ідентифікація політико-правових механізмів інформаційної безпеки держави в умовах гібридної війни. *Політичне життя:*

науковий журнал. К: Київський національний університет імені Тараса Шевченка. URL: https://jpl.donnu.edu.ua/article/view/17922

2. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Geneva: International Organization for Standardization, 2022.

СУЧАСНІ СТРАТЕГІЇ ТА ОРГАНІЗАЦІЙНІ ПІДХОДИ ДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОСТІ БІЗНЕСУ В УМОВАХ ГЛОБАЛЬНОЇ НЕСТАБІЛЬНОСТІ

Рубан Ю. Р.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

Сучасний бізнес - це постійна боротьба з ризиками: від кібератак до глобальних потрясінь. Питання виживання сьогодні трансформувалося: ми вже не запитуємо, чи станеться криза, а фокусуємося на швидкості відновлення. Ключем до цього стає управління безперервністю бізнесу (BCM). Це не просто формальні інструкції «про всяк випадок», а стратегічна філософія стійкості, що базується на розумінні процесів, управлінні даними та збереженні довіри клієнтів. У цій роботі ми розглядаємо BCM як інструмент, що дозволяє компанії залишатися ефективною в будь-яких умовах, адже головний актив підприємства - це здатність команди продовжувати роботу попри будь-які виклики.

Коли ми говоримо про безперервність бізнесу, важливо провести чітку межу: це не просто відновлення серверів після збою (що технічно називають Disaster Recovery). Це значно ширша концепція, яка охоплює людей, процеси, комунікації та управління кризою в цілому. У світі професіоналів «золотим стандартом» тут є ISO 22301. Це не просто набір сухих вимог, а своєрідна

"дорожня карта", яка допомагає компанії залишатися на плаву, навіть коли штормить.

Фундаментом будь-якої стратегії безперервності є розуміння двох ключових метрик, про які часто забувають до моменту, поки не станеться інцидент:

1. RTO (Recovery Time Objective): Максимально допустимий час простою. Простіше кажучи: як довго ваш бізнес може "лежати", поки це не стане катастрофою? Для інтернет-магазину - це може бути 15 хвилин, для архіву - тиждень.

2. RPO (Recovery Point Objective): Точка відновлення даних. Скільки даних ми готові "стерти" в історії? Якщо ви робите бекап раз на добу, ваш RPO - 24 години. Якщо дані життєво важливі - RPO прагне до нуля.

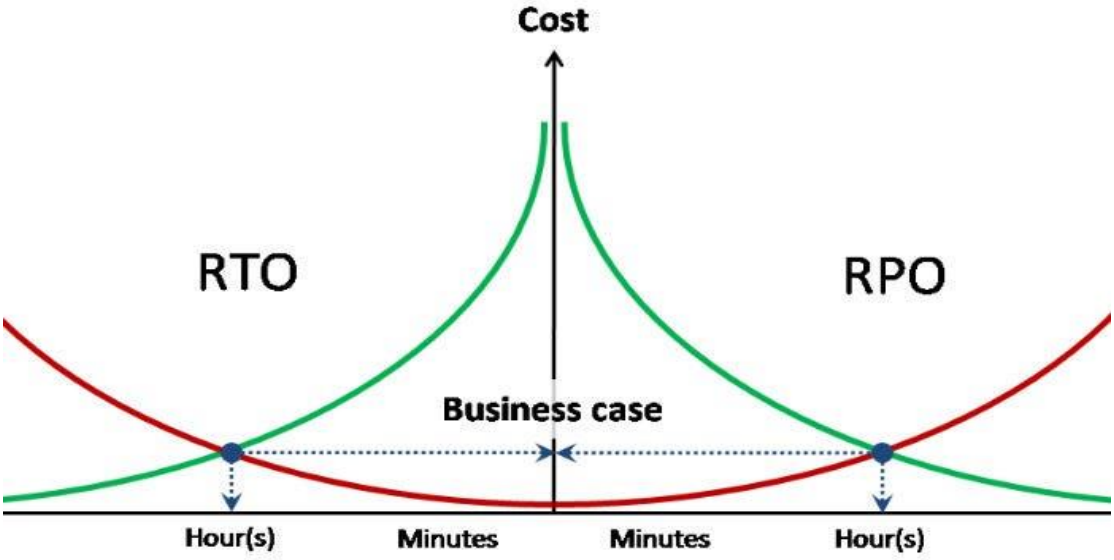

Рис. 1. Залежність вартості забезпечення безперервності бізнесу від цільових показників RTO та RPO

На наведеному вище графіку (Рис. 1) чітко видно, що ці показники визначають "апетит до ризику" компанії. Чим менші RTO та RPO, тим дорожчою стає система захисту. Сучасний менеджмент сьогодні полягає не в тому, щоб зробити RTO нульовим (це астрономічно дорого), а в тому, щоб

знайти баланс між витратами на кіберстійкість та реальними збитками від простою.

Організація, яка усвідомлює свої RTO/RPO та має задокументовані плани (а не просто «ми якось впораємося»), вже на голову випереджає конкурентів. Це перетворює безперервність із "витратної статті бюджету" на реальну конкурентну перевагу: клієнти довіряють тим, хто працює стабільно, навіть у найскладніші часи.

Одним з рішень для забезпечення RPO є перехід в хмару. Ми зіткнулися з парадоксом: хмарні технології роблять бізнес надзвичайно гнучким, але водночас створюють нові критичні точки відмови, які виходять за межі нашого безпосереднього контролю. Головна помилка сучасного менеджменту - це хибне відчуття безпеки: переконання, що «якщо дані в хмарі, про їхню безперервність піклується провайдер». Це небезпечний міф. У сучасному світі ключовою концепцією стала «Модель спільної відповідальності». Провайдер відповідає за стабільність своєї інфраструктури, проте бізнес несе повну відповідальність за налаштування систем, резервне копіювання та стратегію відновлення (DR) усередині цієї хмари.

Перехід до хмарних сервісів приніс суттєві виклики:

- Залежність від зовнішніх каналів: Втрата зв’язку з провайдером тепер дорівнює повній зупинці бізнес-процесів.
- Складні взаємозв’язки: Десятки API-інтеграцій створюють "ефект доміно" - відмова однієї ланки паралізує всю екосистему.
- Ризик вендор-локауту (Vendor Lock-in): Залежність від одного провайдера робить компанію заручником його технічних збоїв або цінової політики.

Як наслідок, тренд 2026 року - це перехід до мультихмарної (multi-cloud) архітектури. Бізнес, що прагне стійкості, більше не кладе всі яйця в один кошик, розподіляючи сервіси між різними провайдерами для гарантії працездатності під час блекаутів.

Управління безперервністю бізнесу (BCM) сьогодні є не просто формальним набором інструкцій, а стратегічною філософією виживання та стійкості. Побудова ефективної системи захисту базується на глибокому розумінні критичних метрик - цільового часу відновлення (RTO) та точки відновлення даних (RPO). Головне завдання сучасного менеджменту полягає не в досягненні «нульового ризику», а в пошуку оптимального балансу між інвестиціями у кіберстійкість та потенційними збитками від простою.

В умовах цифрової трансформації бізнес повинен чітко усвідомлювати «Модель спільної відповідальності» при роботі з хмарними сервісами. Враховуючи виклики, пов'язані із залежністю від зовнішніх каналів зв'язку, складними API-інтеграціями та ризиками вендор-локауту, стратегічним трендом 2026 року стає перехід до мультихмарної архітектури. Такий підхід дозволяє розподіляти сервіси між різними провайдерами, гарантуючи стійкість навіть під час блекаутів. Зрештою, впровадження комплексного підходу до BCM перетворює безперервність бізнесу з витратної статті бюджету на вагому конкурентну перевагу, що забезпечує стабільність та довіру клієнтів у часи глобальної нестабільності.

Література

1. International Organization for Standardization. (2019). ISO 22301:2019. Security and resilience — Business continuity management systems — Requirements. ISO.

2. National Institute of Standards and Technology. (2021). Contingency Planning Guide for Federal Information Systems (NIST SP 800-34 Rev. 1). U.S. Department of Commerce.

3. RPO vs. RTO: Understanding the Differences and Their Role in Recovery Strategies URL: https://medium.com/@PlanB./rpo-vs-rto-understanding-the-differences-and-their-role-in-recovery-strategies-df7be5064056

SECURITY AS A SERVICE (SECAAS) ЯК СУЧАСНА МОДЕЛЬ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ПІДПРИЄМСТВ

Гайдамаченко Т. М.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

Безпека як послуга (**Security as a Service — SECaaS**) — це бізнес-модель, відповідно до якої інтернет-провайдер або хмарний оператор інтегрує сервіси кібербезпеки у власну інфраструктуру та надає їх клієнтам у вигляді додаткових послуг або підписки (рис. 1). Використання SECaaS дозволяє підприємствам зменшити витрати на кібербезпеку, оскільки зменшується потреба у дорогому мережевому обладнанні та висококваліфікованому персоналі для його обслуговування. Найбільш поширеними сервісами SECaaS є захист від **DDoS-атак**, аутентифікація, антивірусний та антишпигунський захист, фільтрація спаму, виявлення мережевих вторгнень, тестування на вразливості та управління інцидентами.

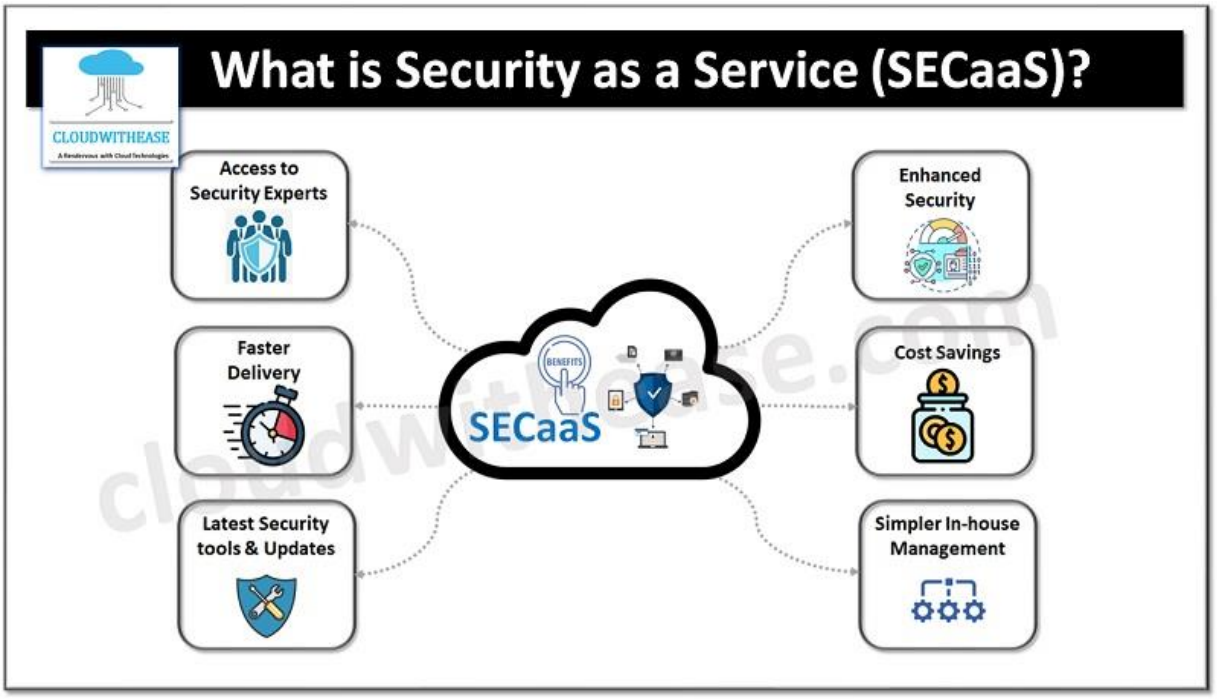

Рис. 1. Суть SECaaS технології

SECaaS дає змогу ефективно керувати витратами на кіберзахист і швидко підключати додаткові сервіси без необхідності їх закупівлі та розгортання. Крім того, фільтрація та аналіз мережевого трафіку можуть виконуватися ще до потрапляння даних у внутрішню мережу підприємства, що дозволяє реалізувати багаторівневий захист від зовнішніх атак (рис. 2).

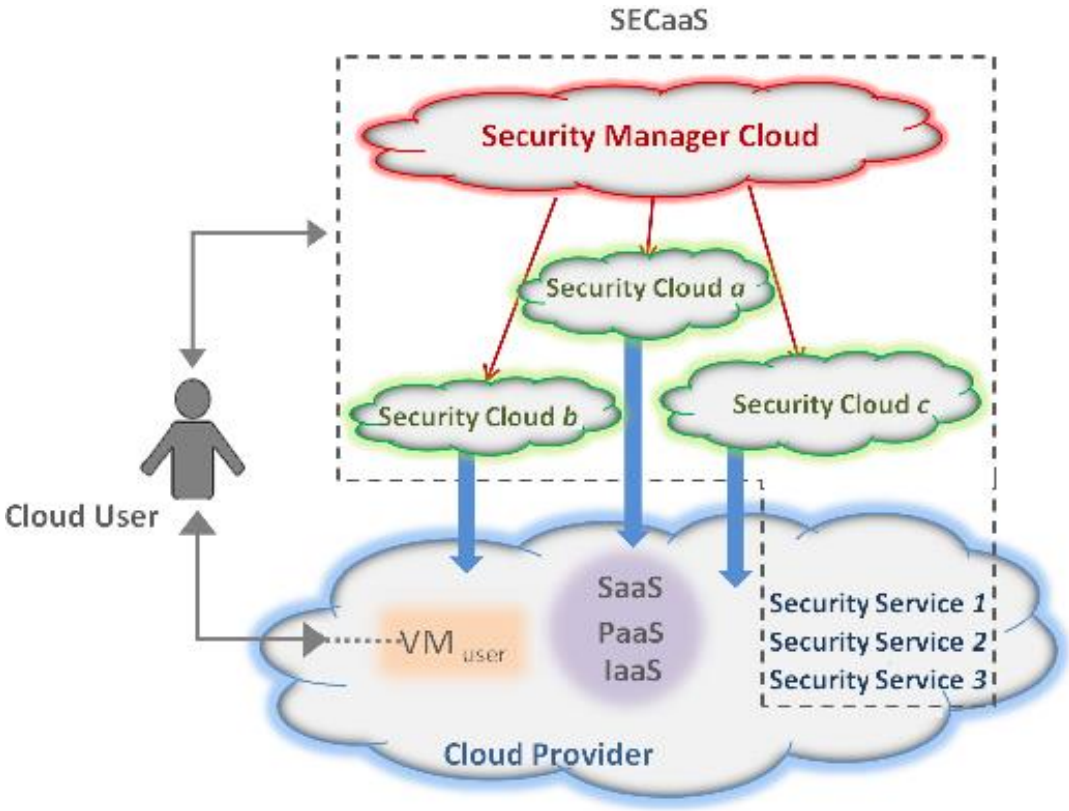

Рис. 2. Схема впровадження SECaaS в мережевий ланцюг бізнесу

Основні функції SECaaS включають **мережеву безпеку**, сканування вразливостей, захист веб-ресурсів, безпеку електронної пошти, системи ідентифікації та авторизації, шифрування даних, виявлення вторгнень, запобігання втраті даних, а також безперервний моніторинг стану безпеки. Додатково можуть використовуватися інструменти управління подіями безпеки (**SIEM**), системи виявлення загроз, рішення для захисту кінцевих пристроїв (**EDR**) та відновлення після аварій (**DRaaS**).

В Україні подібні послуги пропонують різні телекомунікаційні компанії. Наприклад, **Datagroup** надає послуги шифрування передачі даних «VPN to

Azure», **Укртелеком** пропонує захист від DDoS-атак, а компанія **Wolfson** забезпечує антивірусний захист, веб-фільтрацію та захист каналів зв'язку.

Зростання кількості кіберзагроз підтверджує актуальність таких рішень. За даними досліджень, кількість зламаних веб-ресурсів щороку збільшується, а багато атак виконуються автоматизованими інструментами. Тому використання SECaaS стає ефективним способом підвищення рівня кіберзахисту організацій, забезпечуючи масштабованість, економічність та швидке реагування на сучасні загрози.

Література

1. Let's Encrypt (Internet Security Research Group). Getting started (офіційна сторінка). Let's Encrypt. URL: https://letsencrypt.org/

2. Ужгородський національний університет. Лекція 4. Технології захисту інформації (PDF). УжНУ (Infocentre). URL: https://www.uzhnu.edu.ua/uk/infocentre/get/4186

3. Minnix J. What is Security as a Service? A 2026 Guide to SECaaS. Bright Defense. Published: February 1, 2025. Updated: February 21, 2026. URL: https://www.brightdefense.com/resources/security-as-a-service-guide/

4. Cloud Security Alliance. Security as a Service (Research Topic). Cloud Security Alliance (CSA). URL: https://cloudsecurityalliance.org/research/topics/security-as-a-service

5. Fortinet. Next-Generation Firewall (NGFW) – See Top Products. Fortinet. URL: https://www.fortinet.com/uk/products/next-generation-firewall

6. Хоптюк Д. Як захистити свій сайт від злому. Топ-10 розповсюджених варіантів злому. Fondy Blog. 22 Березня 2022. URL: https://fondy.ua/uk/blog/how-to-protect-website/

СЕКЦІЯ 2. НОВІТНІ ТРЕНДИ УПРАВЛІННЯ РИЗИКАМИ КІБЕРБЕЗПЕКИ

МЕТОДОЛОГІЯ ОЦІНКИ РИЗИКІВ ВЕБ-РЕСУРСІВ НА ОСНОВІ АНАЛІЗУ SSL/TLS КОНФІГУРАЦІЙ ТА ЗАГОЛОВКІВ БЕЗПЕКИ

Бовкун В. Ю.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

У сучасних умовах цифрової трансформації підприємства та державні установи дедалі більше покладаються на веб-ресурси для забезпечення бізнес-процесів, комунікації з клієнтами та надання послуг. Це створює нові виклики у сфері кібербезпеки, адже веб-сайти стають однією з основних точок атаки для зловмисників. За даними OWASP, понад 60% інцидентів у сфері інформаційної безпеки пов’язані з уразливостями веб-додатків [3]. Одним із ключових аспектів захисту веб-ресурсів є правильна конфігурація протоколів SSL/TLS та використання захисних HTTP-заголовків. Прострочені сертифікати, застарілі алгоритми шифрування або відсутність політик HSTS та CSP значно підвищують ризик атак типу «Man-in-the-Middle» та XSS [4]. Міжнародні стандарти управління ризиками, такі як ISO/IEC 27005:2022 [1] та NIST Cybersecurity Framework (CSF) [2], пропонують загальні методології оцінки та мінімізації ризиків. Проте вони здебільшого орієнтовані на організаційні аспекти, залишаючи поза увагою технічні індикатори, які можна інтегрувати у процес управління ризиками.

ISO/IEC 27005:2022 - визначає управління ризиками як систематичний процес, що включає: ідентифікацію активів; виявлення загроз; оцінку та обробку ризиків; постійний моніторинг. Перевагою ISO є універсальність, проте його абстрактність ускладнює інтеграцію конкретних технічних

показників, таких як SSL/TLS чи HTTP-заголовки. NIST CSF пропонує більш практичний підхід, який складається з п’яти функцій: identify — визначення активів та ризиків; protect — впровадження заходів безпеки, включаючи SSL/TLS, HSTS та CSP; detect — виявлення інцидентів; respond — оперативне реагування; recover — відновлення після інцидентів. На відміну від ISO, NIST прямо рекомендує інтегрувати технічні індикатори у процес управління ризиками, що робить його більш придатним для практичного застосування у сфері веб-безпеки [2].

Технічні індикатори для оцінки ризику: SSL/TLS конфігурації — набір параметрів, що визначають алгоритми шифрування, версії протоколів та термін дії сертифікатів; HSTS (HTTP Strict Transport Security) — політика, яка примушує браузер використовувати лише HTTPS; CSP (Content Security Policy) — набір правил, що визначають, які ресурси можна завантажувати на веб-сторінку.

Таблиця 1

Порівняння ISO/IEC 27005 та NIST CSF у контексті веб-безпеки

Критерій	ISO/IEC 27005	NIST CSF
Основна мета	Управління ризиками	Забезпечення кіберстійкості
Орієнтація	Організаційна	Технічна + організаційна
Етапи процесу	Ідентифікація, оцінка, обробка	Identify, Protect, Detect, Respond, Recover
Використання SSL/TLS	Не деталізовано	Включено у функцію Protect
Використання HSTS	Не згадуються	Рекомендовано як технічний захід
Використання CSP	Не згадуються	Рекомендовано як технічний захід
Інструменти моніторингу	Загальні рекомендації	Конкретні приклади (сканери, SIEM)
Гнучкість застосування	Висока, але абстрактна	Висока, з практичними орієнтирами

Для підтвердження теоретичних положень було проведено дослідження трьох популярних українських веб-ресурсів: Prom [7] (маркетплейс); Rozetka [8] (найбільший інтернет-магазин); Novaposhta [9] (сайт поштово-логістичної компанії «Нова Пошта»). Аналіз здійснювався за допомогою трьох онлайн-сервісів: SSL Labs Server Test [4] — перевірка конфігурацій SSL/TLS та

сертифікатів; Security Headers [5] — аналіз заголовків безпеки; Mozilla Observatory [6] — комплексна оцінка політик безпеки.

Таблиця 2

Порівняння параметрів SSL/TLS та заголовків безпеки

Параметр	prom	rozetka	novaposhta
SSL Labs (оцінка)	B (TLS 1.0/1.1 підтримуються, HSTS увімкнено)	A (TLS 1.2/1.3, але HSTS відсутній)	B (TLS 1.0/1.1 підтримуються, HSTS відсутній)
Сертифікат	RSA 2048, ZeroSSL, дійсний до квітня 2026	RSA 2048 + ECDSA 256, Google Trust Services, дійсний до травня 2026	RSA 2048, RapidSSL, дійсний до липня 2026
HSTS	Є, max-age=31536000, preload	Відсутній	Відсутній
CSP	Є, але реалізовано небезпечно (unsafe-inline)	CSP *report-only*	Відсутній
SecurityHeaders оцінка	A (майже всі заголовки, але Permissions-Policy відсутній)	D (багато заголовків відсутні)	F (відсутні майже всі заголовки)
Mozilla Observatory	Низький бал: CSP небезпечний, Referrer-Policy слабкий, SRI відсутній	Низький бал: CSP відсутній, HSTS відсутній, HTTPS редирект не налаштований	Дуже низький бал: CSP відсутній, HSTS відсутній, Referrer-Policy відсутній, SRI відсутній

Для кількісної оцінки рівня ризику веб-ресурсів використовується базова формула:

$$R = P \cdot I \,, \tag{1}$$

де P (Probability) — ймовірність виникнення інциденту безпеки, а I (Impact) — потенційний вплив інциденту на бізнес-процеси та користувачів.

Prom: ймовірність оцінемо 0.5, бо підтримує TLS 1.0/1.1 та небезпечний CSP (*unsafe-inline*). Це створює середню ймовірність інциденту. Вплив оцінемо як 0.7, бо сайт є великим маркетплейсом, але не критичним для всієї інфраструктури країни. Rozetka: ймовірність оцінемо 0.6, бо використовує сучасні TLS протоколи, проте відсутній HSTS і CSP працює лише у режимі *report-only*. Вплив оцінемо як 0.8, адже це найбільший інтернет-магазин України, компрометація якого матиме значні фінансові та репутаційні наслідки. Novaposhta: ймовірність оцінемо 0.8, найбільш проблемний сайт, підтримує

TLS 1.0/1.1, відсутні HSTS, CSP та інші ключові заголовки. Вплив оцінено як 0.9, бо «Нова Пошта» є критичним логістичним сервісом, і будь-які проблеми з безпекою можуть паралізувати бізнес-процеси.

Таблиця 3

Розрахунок рівня ризику для досліджуваних сайтів

Сайт	Ймовірність інциденту	Потенційний вплив	Розрахунок R	Рівень ризику
Prom	0.5	0.7	0.35	Середній
Rozetka	0.6	0.8	0.48	Середній
Novaposhta	0.8	0.9	0.72	Високий

Проведене дослідження показало, що навіть великі українські веб-ресурси мають суттєві відмінності у рівні захищеності. Prom та Rozetka демонструють середній рівень ризику, тоді як Novaposhta має високий ризик через відсутність ключових заголовків безпеки та підтримку застарілих протоколів. Таким чином, ефективне управління ризиками веб-ресурсів потребує інтеграції технічних індикаторів (SSL/TLS, HSTS, CSP) у загальні методології, такі як ISO/IEC 27005:2022 та NIST Cybersecurity Framework. Це дозволяє поєднати стратегічний та практичний рівні кіберзахисту, забезпечуючи комплексний підхід до мінімізації ризиків.

Література

1. ISO/IEC 27005:2022. *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*. International Organization for Standardization. Geneva, 2022. URL: https://www.iso.org/standard/80585.html

2. National Institute of Standards and Technology (NIST). *Cybersecurity Framework Version 1.1*. Gaithersburg, MD, 2018. URL: https://www.nist.gov/cyberframework

3. OWASP Foundation. *OWASP Top Ten Web Application Security Risks*. 2021. URL: https://owasp.org/Top10

4. Qualys SSL Labs. *SSL Server Test*. URL: https://www.ssllabs.com/ssltest/

5. SecurityHeaders. *Analyse your HTTP response headers*. URL: https://securityheaders.com/

6. Mozilla Observatory. *HTTP Header Security Test*. URL: https://developer.mozilla.org/en-US/observatory/

7. Prom.ua — маркетплейс. URL: https://prom.ua

8. Rozetka.com.ua — інтернет-магазин. URL: https://rozetka.com.ua

9. Novaposhta.ua — логістичний сервіс. URL: https://novaposhta.ua

АНАЛІЗ ТА ЗАБЕЗПЕЧЕННЯ ВІДПОВІДНОСТІ СИСТЕМИ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ РЕГУЛЯТОРНИМ ВИМОГАМ В УМОВАХ ФУНКЦІОНУВАННЯ SOC

Добридник В. О.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

Сьогодні будь-яка організація, що працює з інформацією, зобов’язана дотримуватись певних правил і стандартів у сфері інформаційної безпеки. Ці правила прописані у законах та міжнародних стандартах, і за їх порушення передбачені санкції. Водночас компанії дедалі частіше створюють або підключаються до центрів безпекових операцій (SOC), які цілодобово стежать за тим, що відбувається в їхніх мережах. Однак на практиці виникає проблема: процеси виконання нормативних вимог і оперативна робота SOC існують окремо, що призводить до зайвих витрат часу і людських ресурсів [1].

Основними документами, яким повинна відповідати система менеджменту інформаційної безпеки (СМІБ), є міжнародний стандарт ISO/IEC 27001:2022, Закон України про захист персональних даних, Регламент GDPR для організацій, що обробляють дані громадян ЄС, а також вітчизняні нормативні документи — НД ТЗІ та вимоги ДССЗЗІ. Кожен із цих документів

має власні вимоги до того, як потрібно фіксувати події, реагувати на інциденти і звітувати перед перевіряючими органами [2].

Мета роботи — запропонувати підхід, який дозволить об’єднати перевірку відповідності вимогам із щоденною роботою SOC так, щоб це не потребувало окремих людей і зусиль. Для цього розроблено чотирирівневу архітектуру, яку наведено на рис. 1.

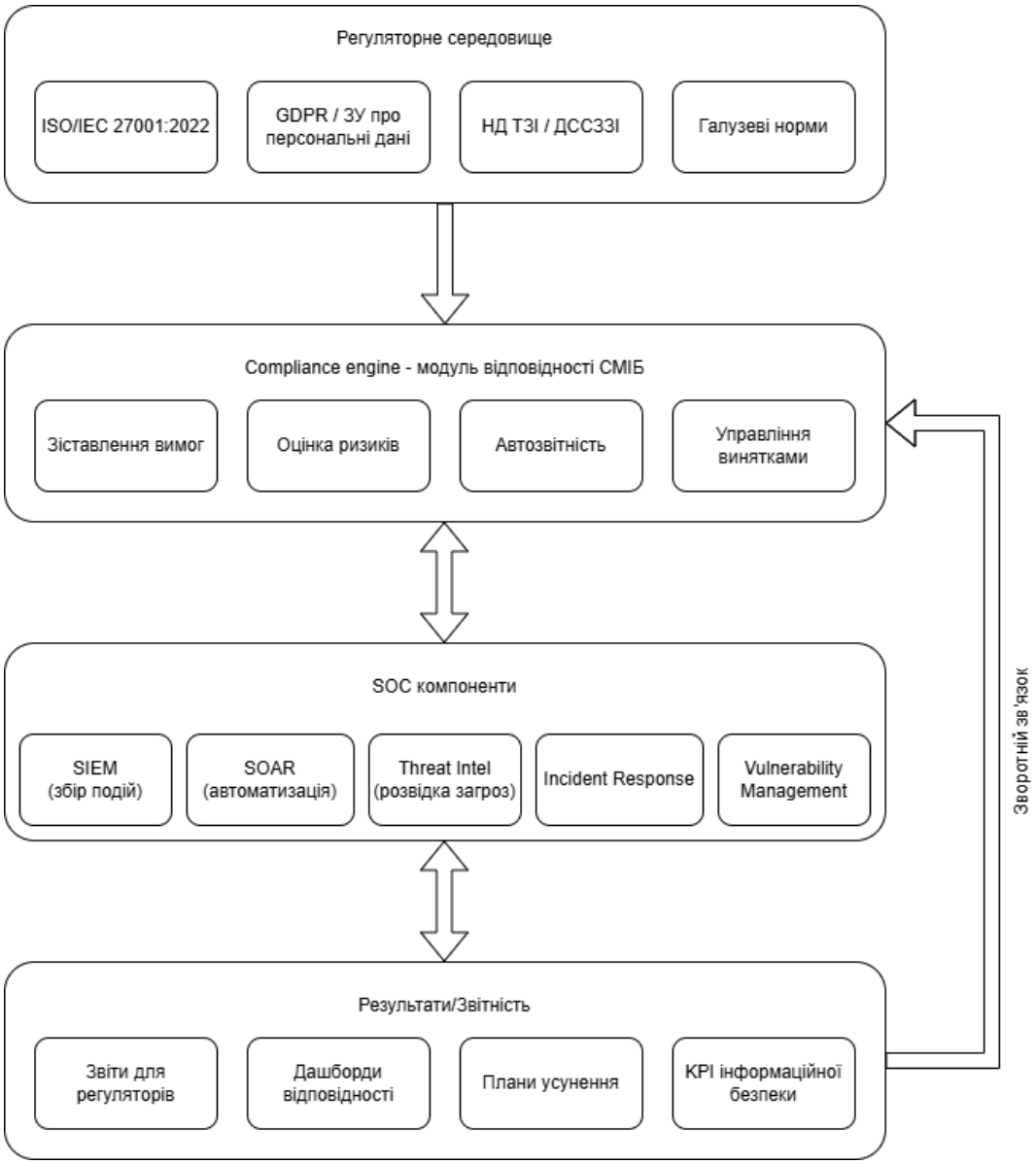

Рис. 1. Архітектура забезпечення відповідності СМІБ в умовах SOC

Щоб зрозуміти, чи дійсно варто впроваджувати такий підхід, було порівняно кілька поширених методів забезпечення відповідності, які використовуються на практиці. Результати порівняння наведено в таблиці 1.

Таблиця 1

Порівняльний аналіз методів забезпечення відповідності СМІБ

Метод/підхід	Автоматизація	Інтеграція з SOC	Покриття вимог	Ефективність
Ручний аудит	Відсутня	Відсутня	40-60%	Низька
GRC-платформа	Висока	Часткова	65-75%	Середня
SIEM + ручне зіставлення подій	Часткова	Висока	70-80%	Середня
Compliance Engine + SOC	Повна	Повна	90-95%	Висока

З таблиці 1 видно, що традиційні методи мають суттєві обмеження: ручний аудит потребує багато часу і не пов'язаний із реальними даними SOC, а GRC-платформи, хоча й автоматизують частину роботи, все одно працюють окремо від оперативних систем. Найкращий результат дає саме інтегрований підхід, при якому Compliance Engine отримує дані безпосередньо від SIEM та інших компонентів SOC і одразу перевіряє їх на відповідність вимогам [3].

Суть запропонованого підходу полягає в чотирьох кроках. По-перше, кожна подія, яку фіксує SIEM, автоматично зіставляється з відповідним пунктом стандарту або закону. По-друге, система сама оцінює, наскільки серйозним є відхилення від норми. По-третє, звіти для перевіряючих органів формуються автоматично, без участі людини. По-четверте, якщо результати звітності або KPI вказують на слабкі місця, ця інформація повертається назад до SOC як завдання для коригувальних дій — саме це відображає стрілка зворотного зв'язку на рис.1.

Таким чином, поєднання процесів відповідності з роботою SOC дозволяє вирішити практичну проблему, з якою стикаються багато організацій: перевірка дотримання вимог перестає бути окремою разовою процедурою і стає частиною щоденної операційної діяльності. За попередніми оцінками, такий підхід скорочує час підготовки звітності для регуляторів приблизно на 65% і підвищує рівень охоплення нормативних вимог до 90–95%.

Література

1. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements. *Geneva: ISO* , 2022.
2. Закон України про основні засади забезпечення кібербезпеки України від 05.10.2017 №2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
3. Syed R. Cybersecurity vulnerability management: A conceptual ontology and cyber intelligence alert system. *Information & Management*. 2020. Vol. 57, no. 6. URL: https://doi.org/10.1016/j.im.2020.103334

МОДЕЛІ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ У СФЕРІ КІБЕРБЕЗПЕКИ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ

Карпека І. П.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

Використання сучасних технологій, таких як штучний інтелект (ШІ) та кібербезпека, дозволяє підприємствам значно підвищувати ефективність прийняття управлінських та операційних рішень . В умовах експоненційного зростання обсягів даних та еволюції кіберзагроз (зокрема, цільових атак APT та програм-вимагачів), традиційні ручні методи аналізу стають неефективними. Тому інформаційні системи підтримки прийняття рішень (СППР) у кризових умовах є важливим елементом сучасного бізнесу, який забезпечує швидкість і точність реакції на загрози. У сфері кібербезпеки ШІ застосовується для захисту систем, мереж та даних шляхом глибокого аналізу великих обсягів телеметрії, що дозволяє швидше виявляти приховані ризики, координувати відповіді та підтримувати більш точне прийняття рішень. За оцінками

експертів, через великий дефіцит кадрів та складність завдань індустрія інформаційної безпеки все частіше покладається на рішення в області штучного інтелекту, зокрема на алгоритми машинного навчання (ML) та нейронні мережі.

Замість того, щоб зосереджуватися лише на реагуванні на інциденти, ШІ посилює весь процес безпеки: підтримує раннє виявлення, зменшує кількість хибних тривог, покращує контроль доступу та динамічно адаптується до нових ризиків. Інтеграція алгоритмів глибокого навчання дозволяє системі еволюціонувати разом із загрозами. Основні напрями застосування ШІ для підтримки прийняття рішень включають:

- Проактивне виявлення загроз та аномалій: ШІ запроваджує предиктивний рівень аналітики, відходячи від застарілих сигнатурних методів. Системи здатні виявляти нові форми шкідливого ПЗ та моніторити незвичну комунікацію між пристроями навіть без попередніх прикладів (zero-day загрози), аналізуючи відхилення від базової лінії нормальної поведінки мережі .
- Управління ідентифікацією та доступом (IAM) на базі поведінкової аналітики (UEBA): ШІ аналізує фактори ризику в режимі реального часу: вхід з незнайомого пристрою, запит доступу за межами посадових обов'язків, нестандартний час активності тощо . Це дозволяє системі СППР автоматично блокувати доступ або вимагати додаткову багатофакторну автентифікацію (MFA) при найменшій підозрі.
- Запобігання складним фішинговим атакам та соціальній інженерії: За допомогою алгоритмів обробки природної мови (NLP) ШІ глибоко аналізує семантику, контекст та зміст електронних листів. Це дозволяє системі приймати автоматизовані рішення щодо блокування цільового фішингу (spear-phishing) та підміни доменів ще до того, як лист потрапить до поштової скриньки працівника і завдасть шкоди мережі.
- Автоматизація роботи SOC та оркестрація реакцій: ШІ використовується для сортування (тріажу) інцидентів, агрегації логів та управління кейсами. Алгоритми здатні самостійно збирати контекст навколо інциденту, що дозволяє аналітикам безпеки зосередитися на стратегічно

важливих завданнях, суттєво зменшуючи ефект «вигоряння від сповіщень» (alert fatigue).

Попри очевидні переваги, впровадження ШІ у системи підтримки прийняття рішень стикається з низкою суттєвих перешкод. Серед них виділяють гостру потребу у великих масивах верифікованих та якісних даних для тренування моделей, адже алгоритми залежать від точності вхідної інформації. Також проблемою є складність інтеграції ШІ зі застарілими корпоративними системами (Legacy Systems), які не підтримують сучасні протоколи обміну даними. Крім того, виникають нові специфічні загрози, такі як змагальні атаки (Adversarial Machine Learning), коли зловмисники намагаються обдурити самі алгоритми ШІ, підміняючи дані. Не слід забувати й про жорсткі регуляторні ризики та питання конфіденційності, пов'язані з новими міжнародними стандартами кібербезпеки .

Узагальнюючи наведене, застосування моделей штучного інтелекту у кібербезпеці перетворює операції з безпеки з ручного, реактивного процесу на повністю автоматизований, масштабований і проактивний захист. Істинний ШІ здатен блискавично знаходити оптимальне рішення в конкретній динамічній ситуації, а не просто робити висновки на основі жорстко запрограмованої статичної логіки. Це робить його невіддільною фундаментальною частиною сучасних систем підтримки прийняття рішень в умовах комплексного та непередбачуваного ландшафту кіберзагроз.

Таблиця 1

Методи ШІ для підтримки прийняття рішень у кібербезпеці

Метод/засіб ШІ	**Тип загрози / задачі**	**Що аналізує**	**Заходи підтримки / рішення**
Машинне навчання (ML)	Zero-day атаки, нове шкідливе ПЗ	Мережевий трафік, патерни поведінки процесів	Автоматична класифікація загрози, пропозиція блокування
Аналіз поведінки (UEBA)	Інсайдерські загрози, скомпрометовані акаунти (IAM)	Логи входу, нетипові дії користувачів та запити	Обмеження прав доступу, ескалація інциденту до аналітика
Обробка природної мови (NLP)	Фішинг, соціальна інженерія (BEC-атаки)	Текст електронних листів, метадані, підозрілі URL	Відправка листа в карантин, автоматичне попередження користувача

Література

1. Syracuse University iSchool: AI in Cybersecurity: How AI is Changing Threat Defense. URL: https://ischool.syracuse.edu/ai-in-cybersecurity/

2. Swimlane: Guide to AI in Cybersecurity: 7 Use Cases of AI Automation. URL: https://swimlane.com/blog/how-is-ai-used-in-cybersecurity/

3. Palo Alto Networks: What Are the Barriers to AI Adoption in Cybersecurity? URL: https://www.paloaltonetworks.com/cyberpedia/what-are-barriers-to-ai-adoption-in-cybersecurity

4. Fortinet: Artificial Intelligence (AI) in Cybersecurity. URL: https://www.fortinet.com/resources/cyberglossary/artificial-intelligence-in-cybersecurity

ОЦІНКА ТА УПРАВЛІННЯ КІБЕРРИЗИКАМИ ПІДПРИЄМСТВА В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

Карпенко М. А.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

Цифрова трансформація бізнесу є одним із ключових трендів сучасної економіки. За даними Cybersecurity Ventures, глобальні збитки від кіберзлочинності у 2025 році перевищили 10,5 трлн доларів США на рік, що майже втричі більше порівняно з 2015 роком [1]. Разом із зростанням цифрових активів підприємств зростає і поверхня атаки — кількість потенційних точок проникнення зловмисників у корпоративну інфраструктуру.

Управління кіберризиками є невід'ємною складовою системи управління підприємством. Відповідно до стандарту ISO/IEC 27005:2022, кіберризик визначається як поєднання ймовірності настання події та її наслідків у контексті інформаційної безпеки [2]. Практика показує: компанії, що

впровадили формалізовані процеси оцінки ризиків, скорочують середній час виявлення інциденту (MTTD) на 27% порівняно з організаціями без таких процесів — за даними IBM Cost of a Data Breach Report 2024.

Метою дослідження є розробка методичного підходу до оцінки кіберризиків підприємства, адаптованого до умов сучасного кіберпростору. Для досягнення мети вирішуються такі завдання: аналіз існуючих методів кількісної та якісної оцінки ризиків (OCTAVE Allegro, FAIR, NIST RMF); порівняння їх практичної застосовності для підприємств малого та середнього бізнесу; формування рекомендацій щодо вибору методу залежно від зрілості системи інформаційної безпеки організації.

Аналіз показав суттєві відмінності між методами. FAIR (Factor Analysis of Information Risk) дозволяє отримати кількісні фінансові оцінки ризику, однак потребує значних ресурсів для збору вхідних даних. OCTAVE Allegro орієнтований на активи та бізнес-процеси, а тому краще підходить для організацій без виділеної служби ІБ. NIST RMF, натомість, є більш регуляторно-орієнтованим підходом і широко застосовується у державному секторі та критичній інфраструктурі.

Практичну цінність представляє кейс впровадження OCTAVE Allegro у середньому промисловому підприємстві (600 працівників, Польща, 2023 р.): протягом 8 тижнів було ідентифіковано 43 ризики, з яких 11 класифіковано як критичні. Бюджет на усунення критичних ризиків склав 180 тис. євро — приблизно 0,3% річного обороту компанії, що є прийнятним рівнем інвестицій у кібербезпеку за рекомендаціями Gartner (1–3% від IT-бюджету).

У рамках магістерського дослідження розробляється комбінована модель оцінки кіберризиків, що поєднує якісну складову OCTAVE Allegro з елементами кількісного фінансового аналізу FAIR. Модель передбачає три рівні оцінки: стратегічний (вплив на бізнес-цілі), тактичний (вплив на бізнес-процеси) та операційний (вплив на IT-активи). Така багаторівнева структура дозволяє формувати пріоритизовані плани реагування, які враховують як технічні, так і фінансові параметри ризику.

Результати попереднього тестування моделі на даних двох українських підприємств (виробничий та фінансовий сектор) підтвердили її практичну застосовність: точність ранжування ризиків (порівняно з незалежною експертною оцінкою) склала 82%, що є прийнятним показником для систем підтримки прийняття рішень у сфері кібербезпеки.

Таким чином, розроблений підхід забезпечує баланс між глибиною аналізу та ресурсоємністю процесу оцінки, що робить його придатним для широкого застосування у вітчизняному бізнес-середовищі. Подальші дослідження спрямовані на автоматизацію процесів збору та обробки вхідних даних з використанням засобів SIEM та Threat Intelligence.

Література

1. Cybersecurity Ventures. Cybercrime To Cost The World $10.5 Trillion Annually By 2025. URL: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016 (дата звернення: 15.02.2026).

2. ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks. ISO, 2022. 56 p.

3. IBM Security. Cost of a Data Breach Report 2024. IBM Corporation, 2024. 84 p.

4. Caralli R. A., Stevens J. F., Young L. R., Wilson W. R. Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. Carnegie Mellon University, 2007. 133 p.

5. The Open Group. The FAIR Risk Taxonomy (RISK). 2022. URL: https://www.opengroup.org/open-fair (дата звернення: 15.02.2026).

СИСТЕМА ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ НА ОСНОВІ OSINT-ДАНИХ

Лозова І. Л., канд. техн. наук,

Клєщов М. О.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

Останніми роками спостерігається стійка тенденція до зростання кількості кіберзагроз та інцидентів інформаційної безпеки. У 2024 році Україна зіштовхнулася з безпрецедентним сплеском кіберзагроз. За даними CERT-UA, лише за рік фахівці опрацювали 4315 інцидентів – майже на 70% більше, ніж роком раніше. Цей приріст важко назвати випадковим: атаки стають дедалі більш цілеспрямованими, а хакери все частіше б'ють по найвразливіших точках – від органів влади та сектору оборони до енергетики й телекомунікацій [1]. Водночас значна частина інформації, яка може бути використана для підготовки та реалізації атак, перебуває у відкритому доступі, що підвищує рівень ризиків для організацій.

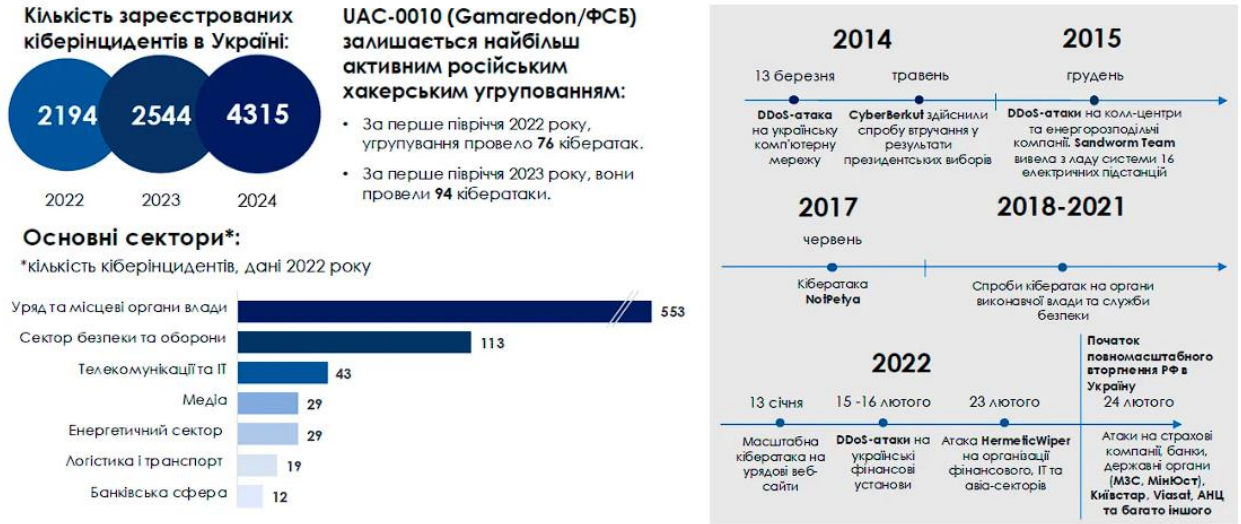

Рис. 1. Статистика кіберінцидентів в Україні

Відкриті джерела інформації (OSINT – Open Source Intelligence) представляють собою систематично зібрану та проаналізовану інформацію з публічно доступних джерел без порушення законодавства чи вторгнення в захищені системи. До відкритих джерел належать веб-сайти, соціальні мережі, форуми, реєстри доменних імен, технічні бази даних, витоки даних, звіти про інциденти та інші публічні ресурси [2]. Завдяки OSINT можна отримати значну кількість даних про технічну інфраструктуру організації, мережеві служби, історію інцидентів, цифрові сліди співробітників та інші відомості, що потенційно впливають на рівень ризику.

Водночас традиційні підходи до оцінювання ризиків інформаційної безпеки здебільшого ґрунтуються на внутрішніх аудитах, аналізі конфігурацій, результатах тестування на проникнення або експертних оцінках. Хоча такі методи залишаються важливими складовими системи управління інформаційною безпекою, вони часто не враховують обсяг і характер інформації, що перебуває у відкритому доступі та може бути використана потенційним зловмисником для підготовки атаки.

Метою роботи є розроблення системи оцінювання ризиків інформаційної безпеки організації на основі OSINT-даних, яка б дозволяла своєчасно виявляти зовнішні загрози, підвищувати точність оцінки ризиків та оптимізувати процеси управління інформаційною безпекою.

Така система буде складатися з кількох основних елементів:

1. Ідентифікація цифрових активів організації (доменів, IP-адрес, облікових записів);

2. Збір даних із публічних ресурсів;

3. Обробка та класифікація отриманої інформації;

4. Оцінювання ризику на основі визначення ймовірності реалізації загрози та потенційних наслідків;

5. Формування звітності та рекомендацій щодо мінімізації виявлених ризиків.

Це надасть організації низку суттєвих переваг у порівнянні з традиційними підходами до ризик-менеджменту. Насамперед, такий підхід забезпечував би раннє виявлення потенційних загроз та зменшив ймовірність неочікуваних атак. Аналіз відкритих даних дає змогу своєчасно ідентифікувати публічно доступні вразливості, витоки інформації, надмірне розкриття технічних або організаційних відомостей, а також активність зловмисників у відкритому інформаційному просторі. Це дозволяє організації переходити від реактивного реагування на інциденти до проактивного управління ризиками [3].

Загалом очікуваним результатом впровадження такої системи є підвищення точності оцінювання ризиків, скорочення часу виявлення потенційних загроз, зменшення ймовірності успішної реалізації атак, а також більш раціональний розподіл ресурсів на заходи захисту інформації.

У підсумку можна зазначити, що використання OSINT-даних у процесі оцінювання ризиків інформаційної безпеки дозволяє підвищити рівень захищеності організації. Інтеграція відкритих джерел інформації дає змогу своєчасно виявляти потенційні загрози та вразливості, а також приймати більш обґрунтовані управлінські рішення.

Література

1. Кібератаки в Україні: зростання на 70% та як захистити бізнес у 2025 році. *Softlist.* URL: https://softlist.ua/cases/cyberattacksinukraine

2. Д.В. Ланде. OSINT у кібербезпеці: навч. пос. Київ: ТОВ «Інжиніринг», 2024. 522 с. ISBN 978-966-2344-97-4

3. Hlavatska A., Anhelska O., Opirskyy I. Investigation of the use of OSINT technology as a new threat of de-anonymized persons on the internet space. *Cybersecurity: Education, Science, Technique*. 2024. Vol. 1, no. 25. P. 19–50. URL: https://doi.org/10.28925/2663-4023.2024.25.1950

СУЧАСНІ ТРЕНДИ УПРАВЛІННЯ КІБЕРРИЗИКАМИ

Книш Л. А.
Державний університет інформаційно-комунікаційних технологій
м. Київ, Україна

Управління ризиками кібербезпеки є ключовою складовою системи інформаційної безпеки організації. Зростання кіберзагроз і цифровізація потребують оновлення підходів та інтеграції ризик-менеджменту в бізнес-процеси. Відповідно до NIST SP 800-39, керівництво несе відповідальність за управління інформаційними ризиками [5]. Модель NIST RMF пропонує структурований семикроковий цикл управління ризиками [3]. Організаційно-аналітичний підхід поєднує стандарти (NIST RMF, ISO 27005, FAIR) із аналізом даних для підтримки управлінських рішень [1; 2].

Найбільш поширеними підходами до управління ризиками інформаційної безпеки є NIST RMF, ISO/IEC 27005 та FAIR. NIST RMF визначає гнучкий 7-кроковий процес управління безпекою та узгоджується з рекомендаціями NIST SP 800-53, що забезпечує комплексний і структурований підхід до впровадження контролів [3]. ISO/IEC 27005 встановлює міжнародні принципи управління ризиками ІБ, базується на процесній моделі PDCA та характеризується високою адаптивністю до потреб організації [2]. FAIR доповнює рамкові стандарти, пропонуючи кількісну оцінку й фінансову квантифікацію ризиків, що підвищує обґрунтованість управлінських рішень [1]. Використання цих підходів у поєднанні дозволяє організаціям ефективніше ідентифікувати, аналізувати та пріоритизувати кіберризики. Така інтеграція сприяє підвищенню прозорості процесу управління ризиками та покращує взаємозв’язок між технічними і бізнес-рішеннями. Крім того, комбіноване застосування стандартів і моделей забезпечує баланс між якісною експертною оцінкою та кількісними методами аналізу. Це особливо важливо в умовах динамічного розвитку загроз та обмеженості ресурсів організації.

Узагальнено ключові відмінності цих підходів показано в таблиці нижче:

Таблиця 1

Порівняння сучасних моделей управління ризиками кібербезпеки

Підхід / Модель	Призначення та тип	Основні особливості
NIST RMF	Рамковий процес (framework) управління ІБ	Повний 7-крроковий цикл ризик-менеджменту (Prepare, Categorize, Select, Implement, Assess, Authorize, Monitor). Дуже детальний, тісно інтегрується з контролями NIST SP 800-53 та суміжними документами. Вимагає адаптації для неурядових організацій, але забезпечує чіткі інструкції і комплексний підхід [3].
ISO/IEC 27005	Стандарт управління ризиками ІБ	Міжнародний стандарт для risk management, взаємопов'язаний зі стандартом ISO 27001. Надає високорівневі рекомендації щодо процесів і контролів. Використовує підхід PDCA: планування ризиків, реалізація заходів, перевірка результатів, вдосконалення. Гнучкий, не диктує конкретні контролі, орієнтований на внутрішню культуру та політики організації [2].
FAIR	Модель кількісної оцінки ризиків	Науково-обґрунтований підхід до фінансової квантифікації інформаційних ризиків. Застосовується разом із фреймворками (NIST, ISO), доповнює їх сценарною оцінкою ризиків та фінансовими метриками. Дозволяє бізнес-керівникам вимірювати потенційні збитки й приймати рішення на основі економічного аналізу [1].

У таблиці показано, що NIST RMF спрямований на організаційно-розподілену систему контролю, ISO 27005 забезпечує гнучкий інтеграційний підхід у складі ISMS, а FAIR концентрується на аналітиці. Незважаючи на різницю в деталізації, усі підходи підтримують ризик-орієнтовану та безперервну філософію: регулярний моніторинг, залучення зацікавлених сторін і прийняття рішень на основі оцінки загроз.

Сучасні тренди управління кіберризиками характеризуються посиленням аналітики та ролі керівництва. За даними FAIR Institute, більшість організацій автоматизують процеси управління ризиками, а майже половина застосовує AI для аналізу. Попри формалізацію ризикового апетиту, залученість рад директорів до використання звітності залишається обмеженою, що підкреслює необхідність інтеграції управління ризиками в стратегічне управління організацією [1].

Основні сучасні тенденції можна сформулювати так:

- Кількісна оцінка ризиків: Впровадження FAIR та подібних моделей дозволяє оцінювати фінансову вартість ризиків і оптимізувати інвестиції, переходячи від якісного до гібридного або кількісного аналізу [1].
- Автоматизація й AI: ШІ та машинне навчання активно застосовуються для прогнозування загроз, аналізу логу та пріоритизації ризиків, а автоматизовані платформи інтегрують стандарти та генерують аналітичні звіти в реальному часі [1; 4].
- Посилення ролі керівництва: Лідери дедалі активніше включають ризик-менеджмент у стратегічне управління; ISO 27005 заохочує інтеграцію, а NIST SP 800-39 підкреслює обґрунтованість рішень [2; 5].
- Інтеграція та безперервність: Управління ризиками стає безперервним циклом; ISO 27005 та NIST RMF реалізують це через PDCA, моніторинг і спільні комітети з безпеки [2; 3].
- Нові профілі та стандарти: NIST створює спеціалізовані профілі, наприклад, Cyber AI Profile для аналізу ризиків ШІ [4]. Зростає увага до ризиків ланцюга постачання та приватності, що стимулює інтеграцію кіберризиків із іншими системами управління ризиками, як ISO 31000 чи COSO ERM [2].

Новітні тренди управління кіберризиками відображають зростання аналітичності та інтеграції в корпоративне управління. NIST RMF та ISO 27005 забезпечують структурованість процесів, а FAIR і AI підвищують точність оцінки та оперативність рішень. Поєднання стандартів із даними та метриками формує гнучку систему управління ризиками і може слугувати універсальною основою для наукових досліджень.

Література

1. FAIR Institute. (2026). 2025 State of Cyber Risk Management Report: From Compliance to Competitive Advantage: The Quantified Value of Cybersecurity. URL: https://www.prnewswire.com/news-releases/fair-institute-releases-2025-state-of-cyber-risk-management-report-302491719.html

2. Forêt, C. (2023). Everything you need to know about ISO 27005: Summary, requirements, pros and cons. C-Risk Blog. URL: https://www.c-risk.com/blog/iso-27005

3. National Institute of Standards and Technology (NIST). (2025). NIST Risk Management Framework (RMF). CSRC Project. URL: https://csrc.nist.gov/projects/risk-management

4. NIST News Release. (2025, December 16). Draft NIST Guidelines Rethink Cybersecurity for the AI Era. URL: https://www.nist.gov/news-events/news/2025/12/draft-nist-guidelines-rethink-cybersecurity-ai-era

5. NIST Special Publication 800-39. (2011). Managing Information Security Risk: Organization, Mission, and Information System View. Gaithersburg: NIST. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

ВПРОВАДЖЕННЯ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ ТА МЕТОДІВ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ КІБЕРБЕЗПЕКИ ТА ПРОВЕДЕННЯ АУДИТУ

Кучмістенко О. О.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

Вступ до епохи цифровізації вимагає від організацій перегляду підходів до забезпечення кібербезпеки. Внутрішній аудит стає не просто інструментом перевірки відповідності, а стратегічним механізмом виявлення вразливостей. Сучасні методи планування аудиту все частіше спираються на концепцію AI Driven Cybersecurity, що дозволяє автоматизувати рутинні перевірки та зосередитися на складних векторах атак [1].

Планування аудиту має базуватися на ризико-орієнтованому підході, де першочергова увага приділяється критичним активам. Використання штучного

інтелекту в процесах кібербезпеки створює як нові можливості для аналізу великих масивів даних, так і нові виклики, пов'язані з перетином технологій ШІ та традиційних методів захисту [2]. На етапі проведення аудиту важливо застосовувати комплексні системи моніторингу, архітектура яких дозволяє адаптуватися до мінливих загроз.

Проте інтеграція ШІ в процеси аудиту вимагає критичного врахування викликів, пов'язаних із надійністю самих інтелектуальних систем. Методологія проведення внутрішнього аудиту повинна трансформуватися з одноразової перевірки у циклічний процес, що включає не лише класичні технічні тести та сканування вразливостей, а й комплексну оцінку зусиль організації щодо управління ризиками довіри до інтелектуальних систем [3].

Рис. 1. Архітектура системи внутрішнього аудиту з елементами ШІ

Методологія проведення аудиту має трансформуватися у циклічний процес, що включає оцінку ризиків довіри до інтелектуальних систем (AI trustworthiness risks). Детальний опис етапів та методів, що пропонуються для застосування, наведено в таблиці 1. Зокрема, методика передбачає верифікацію алгоритмів, аналіз цілісності даних та тестування систем на стійкість до специфічних атак.

Таблиця 1

Етапи та методи аудиту

Етап аудиту	Метод проведення	Опис ключових дій
Планування	Аналіз ризиків та пріоритезація	Визначення об'єктів аудиту на основі ймовірності виникнення інцидентів.
Збір доказів	Автоматизоване вилучення ознак	Збір системних логів та конфігурацій за допомогою спеціалізованих модулів.
Проведення	Тестування на основі AI-механізмів	Виявлення аномальних активностей та потенційних точок зламу в реальному часі.
Звітування	Оцінка надійності та рекомендації	Аналіз зусиль з управління ризиками довіри до технологій та формування плану коригувальних дій.

Таким чином, інтеграція методів машинного навчання та системного планування дозволяє створити адаптивну модель внутрішнього аудиту. Це забезпечує не лише формальне виконання вимог стандартів, а й превентивну стійкість організації до сучасних кіберзагроз, мінімізуючи вплив людського фактора на якість перевірок.

Література

1. ISO/IEC 27007:2020. Information technology Security techniques Guidelines for information security management systems auditing. 2020. 46 p.

2. ISACA. ITAF: A Professional Practices Framework for IS Audit and Assurance. 4th Edition. 2020.

3. Senft S., Gallegos F., Manson A. Information Technology Control and Audit. 5th ed. Boca Raton : CRC Press, 2018.

АКТУАЛЬНІ ТЕНДЕНЦІЇ ТА МЕТОДИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ НА МІЖНАРОДНОМУ РІВНІ

Леженін Д. О.
Державний університет інформаційно-комунікаційних технологій
м. Київ, Україна

У сучасних умовах стрімкого розвитку цифрових технологій питання кібербезпеки набуває особливої актуальності. Інтернет, хмарні сервіси, цифрові платформи та інформаційні системи активно використовуються як державними установами, так і приватними компаніями. Разом із цим зростає і кількість кіберзагроз, що створює нові виклики для міжнародної спільноти. Саме тому проблема кіберзлочинності сьогодні розглядається не лише на національному, а й на глобальному рівні.

Кіберзлочинність є складним явищем, яке постійно змінюється разом із розвитком технологій. Якщо раніше більшість кіберзлочинів була спрямована на окремих користувачів, то сьогодні все частіше об’єктами атак стають державні структури, великі компанії та критична інфраструктура. До найбільш поширених видів кіберзлочинів належать фішинг, розповсюдження шкідливого ПЗ, атаки програм-вимагачів, викрадення персональних даних і несанкціонований доступ до інформаційних систем [1].

Однією з головних причин поширення кіберзлочинності є глобалізація цифрового середовища. Кіберпростір не має чітких кордонів, тому кіберзлочинці можуть діяти з будь-якої точки світу. Це значно ускладнює процес їх виявлення та притягнення до відповідальності. Саме тому важливу роль відіграє міжнародне співробітництво у сфері кібербезпеки.

На основі аналізу сучасних досліджень виділено кілька ключових тенденцій розвитку кіберзлочинності протягом останніх років. По-перше, значно збільшилася кількість атак із використанням програм-вимагачів, які можуть паралізувати роботу організацій і завдати значних фінансових збитків.

По-друге, кіберзлочинці почали активно використовувати новітні технології, зокрема ШІ і автоматизовані інструменти для здійснення атак. По-третє, зросла кількість атак на критичну інфраструктуру, що може мати серйозні наслідки для економіки та безпеки держав [1-3].

Окрім цього, важливою тенденцією є розвиток кіберзлочинних угруповань, які діють організовано та використовують складні схеми для здійснення атак. Такі угруповання часто співпрацюють між собою, обмінюються інформацією та використовують даркнет для продажу викрадених даних або шкідливих програм.

У відповідь на ці виклики міжнародна спільнота активно розробляє нові методи протидії кіберзлочинності. Одним із найважливіших напрямів є посилення міжнародної співпраці держав, яка охоплює обмін інформацією про кіберзагрози, проведення спільних операцій і створення механізмів швидкого реагування на кіберінциденти [2].

Одним із ключових міжнародних документів, який регулює питання боротьби з кіберзлочинністю, є Будапештська конвенція про кіберзлочинність. Документ визначає основні принципи міжнародної співпраці щодо розслідування кіберзлочинів і сприяє гармонізації законодавства різних держав у цій сфері [4].

Сьогодні значний внесок у боротьбу з кіберзлочинністю роблять міжнародні організації, зокрема міжнародна та європейська організації кримінальної поліції Interpol та Europol, які координують діяльність органів правопорядку різних країн і сприяють обміну інформацією про кіберінциденти. Вагому роль у дослідженні сучасних кіберзагроз і розробці рекомендацій щодо їх запобігання відіграє Європейське агентство з кібербезпеки (ENISA) [2].

Ще одним важливим напрямом протидії кіберзлочинності є розвиток центрів реагування на кіберінциденти (CERT/CSIRT), які займаються моніторингом кіберзагроз, аналізом інцидентів і координацією дій під час кібератак [5]. Наявність таких центрів значно підвищує рівень готовності держав до реагування на кіберінциденти.

Також основоположну роль відіграє використання сучасних технологій кіберзахисту. Серед них можна виділити системи виявлення вторгнень, аналіз великих даних, технології ШІ і машинного навчання. Такі технології дозволяють швидше виявляти потенційні загрози та ефективніше реагувати на них [1].

Окрему увагу слід приділити підвищенню рівня кіберграмотності населення. У багатьох випадках кіберзлочини стають можливими через недостатню обізнаність користувачів щодо правил безпечної поведінки в Інтернеті. Тому важливим завданням є проведення освітніх програм, тренінгів та інформаційних кампаній у сфері кібербезпеки [3].

Таким чином, кіберзлочинність є серйозною глобальною проблемою, яка потребує комплексного підходу до її вирішення. Ефективна протидія кіберзлочинам можлива лише за умови тісної співпраці між державами, міжнародними організаціями та приватним сектором. Крім того, важливим є постійний розвиток технологій кіберзахисту та підвищення рівня обізнаності користувачів щодо кіберзагроз.

У перспективі міжнародна співпраця у сфері кібербезпеки буде лише посилюватися, оскільки кіберзагрози продовжують еволюціонувати. Саме тому державам необхідно постійно вдосконалювати свої підходи до захисту інформаційних систем і адаптуватися до нових викликів цифрового середовища.

Література

1. ENISA Threat Landscape Report. *ENISA*. URL: https://www.enisa.europa.eu

2. Internet Organised Crime Threat Assessment (IOCTA). *Europol*. URL: https://www.europol.europa.eu

3. Global Cybersecurity Outlook. *World Economic Forum*. URL: https://www.weforum.org

4. Convention on Cybercrime. *Council of Europe*. URL: https://www.coe.int/en/web/cybercrime/the-budapest-convention

5. Global Cybersecurity Index. *ITU*. URL: https://www.itu.int

НОВІТНІ ТРЕНДИ УПРАВЛІННЯ РИЗИКАМИ КІБЕРБЕЗПЕКИ

Небеський Д.О.
Державний університет інформаційно-комунікаційних технологій
м. Київ, Україна

Цифровізація бізнесу, розвиток хмарних сервісів, віддаленої роботи та IoT суттєво змінюють характер кіберзагроз. Атаки стають більш автоматизованими, таргетованими та фінансово мотивованими [1; 4]. У таких умовах управління ризиками кібербезпеки переходить від формального виконання вимог до стратегічного інструменту забезпечення стійкості організації [2].

1. Перехід до ризик-орієнтованої моделі управління

Сучасні компанії відмовляються від універсального підходу «захистити все однаково». Пріоритет надається критичним активам: даним клієнтів, фінансовим системам, виробничим платформам. Ресурси спрямовуються туди, де потенційні збитки є найбільшими, що відповідає принципам ризик-орієнтованого підходу, визначеним міжнародними стандартами [1; 2]. Це дозволяє зменшити витрати та підвищити ефективність контролів безпеки.

2. Інтеграція кіберризиків у систему корпоративного управління

Кіберризики розглядаються на рівні топменеджменту та включаються до загальної карти ризиків підприємства. Відповідальність розподіляється між IT, службою безпеки та бізнес-підрозділами. Формуються KPI з кіберстійкості та регулярна звітність для керівництва, що відповідає сучасним рекомендаціям з корпоративного управління кіберризиками [3].

3. Впровадження концепції Zero Trust

Модель «ніколи не довіряй – завжди перевіряй» передбачає постійну автентифікацію користувачів, сегментацію мережі та контроль доступу за принципом мінімальних привілеїв. Згідно з рекомендаціями NIST, Zero Trust

Architecture є ефективним інструментом зменшення ризику внутрішніх загроз та компрометації облікових записів [4].

4. Автоматизація та використання штучного інтелекту

Системи моніторингу подій безпеки (SIEM, SOAR) використовують поведінкову аналітику для виявлення аномалій у режимі реального часу. Автоматизоване реагування дозволяє значно скоротити час виявлення інцидентів та мінімізувати їх наслідки, що підтверджується сучасними дослідженнями у сфері інтелектуалізації кібербезпеки [5].

5. Орієнтація на кіберстійкість (Cyber Resilience)

Організації інвестують не лише у запобігання атакам, а й у здатність швидко відновлювати діяльність після інцидентів. Запроваджуються плани безперервності бізнесу, резервне копіювання даних, тестування сценаріїв реагування та кризові навчання. Такий підхід відповідає концепції кіберстійкості, що визначається міжнародними аналітичними звітами та стандартами [3; 5].

Література

1. National Institute of Standards and Technology (NIST). *Risk Management Framework for Information Systems and Organizations (SP 800-37 Rev. 2).* Gaithersburg, MD, 2018. URL: https://doi.org/10.6028/NIST.SP.800-37r2

2. International Organization for Standardization. *ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks.* Geneva: ISO, 2022.

3. World Economic Forum. *Global Cybersecurity Outlook 2024.* Geneva, 2024. URL: https://www.weforum.org

4. Rose S., Borchert O., Mitchell S., Connelly S. *Zero Trust Architecture (NIST SP 800-207).* Gaithersburg, MD, 2020. URL: https://doi.org/10.6028/NIST.SP.800-207

5. IBM Security. *Cost of a Data Breach Report 2023.* Armonk, NY, 2023. URL: https://www.ibm.com/security/data-breach

УПРАВЛІННЯ РИЗИКАМИ ВИТОКУ ПЕРСОНАЛЬНИХ ДАНИХ У ЦИФРОВИХ СИСТЕМАХ

Рожков Н. О.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

Цифровізація суспільства, розвиток електронного урядування, онлайн-банкінгу, хмарних сервісів та соціальних мереж призвели до стрімкого зростання обсягів персональних даних, що обробляються в інформаційних системах. Персональні дані стали стратегічним ресурсом організацій, але водночас – об'єктом підвищеного інтересу з боку кіберзлочинців [1]. Витік такої інформації може спричинити фінансові збитки, репутаційні втрати, юридичну відповідальність і порушення прав громадян. В умовах зростання кіберзагроз проблема управління ризиками витоку персональних даних набуває особливої актуальності для державних органів, бізнесу та громадянського суспільства.

Ризик витоку персональних даних – це ймовірність несанкціонованого доступу, розголошення, втрати або знищення інформації, що дозволяє ідентифікувати фізичну особу. Основними джерелами загроз є:

1. Кіберзлочини – фішинг, шкідливе програмне забезпечення, атаки типу ransomware, SQL-ін'єкції, експлуатація вразливостей програмного забезпечення.
2. Людський фактор – помилки персоналу, використання слабких паролів, неналежне налаштування доступів, недотримання політик безпеки.
3. Внутрішні загрози – навмисні дії співробітників, які мають легітимний доступ до систем.
4. Технічні збої – відмова обладнання, помилки резервного копіювання, некоректна конфігурація серверів.
5. Недостатня правова та організаційна регламентація – відсутність чітких процедур обробки та захисту даних.

Особливо небезпечними є комплексні атаки, що поєднують соціальну інженерію та технічні інструменти зламу [2].

Управління ризиками витоку персональних даних – це систематичний процес виявлення, оцінювання, контролю та моніторингу ризиків, спрямований на мінімізацію негативних наслідків інцидентів інформаційної безпеки.

Важливим аспектом управління ризиками є формування культури інформаційної безпеки в організації. Навіть найсучасніші технічні засоби не гарантують захисту без відповідальної поведінки користувачів. Регулярні тренінги, інструктажі та внутрішні комунікації сприяють зниженню кількості інцидентів, пов'язаних із людським фактором.

Культура безпеки передбачає усвідомлення цінності персональних даних, персональну відповідальність кожного працівника та прозорість процесів управління інформацією.

Управління ризиками витоку персональних даних є невід'ємною складовою сучасної системи інформаційної безпеки. Зростання обсягів цифрової інформації та ускладнення кіберзагроз вимагають від організацій впровадження комплексних, системних та безперервних заходів захисту [3].

Ефективна модель управління ризиками повинна поєднувати технічні рішення, організаційні процедури та правові механізми. Особливе значення має постійний моніторинг загроз, удосконалення політик безпеки та формування культури відповідального ставлення до персональних даних.

Зазначу, що лише інтегрований підхід до управління ризиками дозволить мінімізувати наслідки витоків інформації, забезпечити довіру користувачів і стабільність функціонування цифрових систем в умовах сучасного інформаційного середовища.

Література

1. Hoffman R. Managing compressed data. *Data compression in digital systems*. Boston, MA, 1997. P. 344–360. URL: https://doi.org/10.1007/978-1-4615-6031-9_14

2. Managing risks. *Understanding workplace information systems*. 2010. P. 84–92. URL: https://doi.org/10.4324/9780080544502-22

3. To T., Smith D. Managing personal digital resources. *Proceedings. 15th international workshop on database and expert systems applications, 2004.*, Zaragoza, Spain, 3 September 2004. 2004. URL: https://doi.org/10.1109/dexa.2004.1333478

ОЦІНКА ЕФЕКТИВНОСТІ ВПРОВАДЖЕННЯ МЕТОДИК УПРАВЛІННЯ РИЗИКАМИ НА ПІДПРИЄМСТВІ

Якименко Ю. М., канд. військ. наук, доцент,

Делікатний В. А.

Державний університет інформаційно-комунікаційних технологій,

м. Київ, Україна

Сучасні підходи до оцінки втрат організацій в умовах зростання інформаційних загроз потребують формалізації, адаптації до бізнес-процесів і поєднання економічного аналізу з технічними індикаторами безпеки. Усе більше компаній стикаються з кібератаками, витоками даних і внутрішніми інцидентами, наслідки яких мають як прямі фінансові збитки, так і довготривалі репутаційні втрати. Ефективне реагування вимагає не лише технічного захисту, а й глибокого розуміння структури можливих втрат.

Незважаючи на наявність ряду нормативних стандартів, зокрема FAIR, NIST RMF, ISO/IEC 27005, їх застосування в організаціях залишається фрагментарним. Існує розрив між технічними системами виявлення інцидентів (IDS/IPS) та економічними механізмами оцінки наслідків. Більшість рішень зосереджені на запобіганні, а не на кількісному прогнозуванні втрат і моделюванні ризиків. [2,4]

Організації часто не мають формалізованої моделі оцінювання втрат від кібератак, що ускладнює прийняття обґрунтованих рішень у сфері безпеки та інвестування в захист. Необхідне впровадження методики, яка дозволяє інтегрувати технічні показники з бізнес-аналізом та фінансовою оцінкою.

Розроблена схема включає класифікацію втрат (прямі, непрямі, приховані), ідентифікацію активів, розрахунок ймовірностей загроз та використання кількісних методів для обґрунтування витрат на заходи захисту. Запропоновано алгоритм, що дозволяє враховувати контекст організації, вплив на бізнес-процеси та довготривалі наслідки. Систематизовано ключові вразливості інформаційної інфраструктури, а також продемонстровано приклади типових сценаріїв атак з відповідною оцінкою збитків.

У ході практичної реалізації моделі підтверджено її ефективність для прийняття управлінських рішень у сфері кібербезпеки, зокрема при формуванні бюджету ІБ та ранжуванні загроз за критичністю. Запропонований підхід дозволяє організаціям не лише реагувати на інциденти, а й прогнозувати їх наслідки в грошовому вимірі – що критично важливо у сучасному цифровому середовищі.

Сучасні організації все частіше зіштовхуються з інформаційними інцидентами, які мають як прямі, так і непрямі наслідки для їхньої фінансової стабільності, репутації та безперервності бізнес-процесів. Тому надзвичайно важливим є впровадження структурованих підходів до оцінки втрат, що виникають у результаті реалізації інформаційних загроз.

Пропонується комбінована методика, яка інтегрує кількісні оцінки за моделлю FAIR (Factor Analysis of Information Risk) з процесною логікою управління ризиками за стандартом ISO/IEC 27005. У цій архітектурі FAIR виступає інструментом для визначення ймовірності загроз та розрахунку можливих фінансових втрат, тоді як ISO/IEC 27005 забезпечує повний цикл роботи з ризиками – від ідентифікації активів до вибору заходів реагування.[1,3]

У разі фіксації інформаційного інциденту, наприклад, витоку даних або шкідливого програмного впливу, дані передаються до централізованої системи моніторингу безпеки, яка виконує первинний аналіз. На основі методики FAIR розраховується очікувана вартість інциденту (ALE), що дозволяє пріоритезувати ризики. Далі, згідно з ISO/IEC 27005, проводиться вибір методів зниження ризику: впровадження технічних засобів, зміна політик доступу, навчання персоналу тощо. [3]

Ключову роль у процесі відіграє інформаційна звітність, яка надходить до відповідального підрозділу з ІБ. Ця аналітика є основою для ухвалення рішень щодо інвестування в засоби захисту, формування бюджету на кібербезпеку та оцінки ефективності вжитих заходів. Інтерфейс управління ризиками, реалізований у вигляді спеціалізованої панелі, дозволяє контролювати всі етапи – від виявлення до фінансової оцінки та звітування керівництву.

Запропонований підхід дозволяє організації не лише фіксувати інциденти, а й комплексно аналізувати наслідки у фінансовому та операційному вимірі. Це перехід від реактивного реагування до проактивного управління інформаційними ризиками, що є ключовою умовою сталого функціонування у цифровому середовищі.

Проведене дослідження підтвердило доцільність застосування комбінованої методики оцінки втрат організації, яка поєднує підхід FAIR з процесами управління ризиками згідно з ISO/IEC 27005. Це дозволяє перейти від фрагментарного реагування на інформаційні інциденти до системного управління потенційними збитками у фінансовому та організаційному вимірі.

Запропонована модель забезпечує можливість кількісного обґрунтування управлінських рішень, підвищує прозорість оцінки інформаційних ризиків і формує основу для стратегічного планування у сфері кіберзахисту.

Перспективи подальших досліджень полягають у розширенні моделі через впровадження адаптивних механізмів обробки ризиків, використання інструментів поведінкового аналізу інцидентів, а також застосування MLOps-підходів для прогнозування загроз і оптимізації ресурсів на кіберзахист.

Особливу увагу варто приділити стандартизації обміну аналітичною інформацією між технічними підсистемами (SIEM, IDS/IPS) та блоками управління ризиками на рівні підприємства. [3,5,6]

Література

1. ISO/IEC 27005:2018. Information technology – Security techniques – Information security risk management. Geneva: ISO, 2018.

2. NIST Special Publication 800-30 Revision 1. Guide for Conducting Risk Assessments. National Institute of Standards and Technology, U.S. Department of Commerce, 2012.

3. The Open Group. FAIR Standard – Factor Analysis of Information Risk. Version 2.0. URL: https://www.opengroup.org/FAIR

4. Баранов О. В., Плескач В. Л. Управління ризиками в інформаційній безпеці. Київ: Видавничий дім «Професіонал», 2020. 312 с.

5. Лисенко Н. М., Стеценко В. А. Інформаційна безпека підприємства: теорія та практика оцінювання ризиків. Харків: ХНЕУ ім. С. Кузнеця, 2021. 198 с.

6. Шевченко А. Ю. Методи аналізу та оцінки загроз кібербезпеці підприємств. Інформаційні технології і безпека, 2022. № 1(25). С. 45–53.

АНАЛІЗ РИЗИКІВ ВИКОРИСТАННЯ ПРОГРАМ ЕКРАННОГО ПЕРЕКЛАДУ У РЕАЛЬНОМУ ЧАСІ

Мойсеєнко В. Д.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

У сучасних умовах активного розвитку індустрії відеоігор та цифрових сервісів зростає потреба у доступності контенту різними мовами. Для цього застосовуються системи екранного перекладу в реальному часі, що поєднують

технології комп’ютерного зору, оптичного розпізнавання символів та нейронного машинного перекладу. Подібні рішення можуть використовуватися під час ігрового процесу без модифікації коду гри, що робить їх універсальними для різних платформ. Водночас такі програми отримують доступ до зображення екрана та текстової інформації користувача, що створює потенційні ризики інформаційної безпеки [1].

Програми екранного перекладу виконують захоплення зображення екрана, розпізнавання тексту та передачу даних до модуля перекладу. Це створює такі ризики (табл. 1):

- Перехоплення конфіденційних даних - можливий доступ до логінів, повідомлень та персональної інформації.
- Незахищена передача даних у хмару - ризик витоку інформації.
- Шкідливі overlay-програми - прихований збір даних або шпигунство.
- Підміна перекладеного тексту - використання для фішингу або соціальної інженерії.

Таблиця 1

Основні ризики та методи захисту

№	Ризик	Наслідки	Методи мінімізації
1	Перехоплення даних з екрану	Витік інформації	Локальна обробка зображень
2	Передача даних у хмарні сервіси перекладу	Компрометація акаунта	Використання захищених протоколів передачі (HTTPS, TLS)
3	Шкідлива overlay-програма	Шпигунство, крадіжка акаунтів	Встановлення програм лише з офіційних джерел; перевірка цифрових підписів;
4	Надмірні права доступу додатку	Неконтрольований доступ до системних ресурсів	Ручне налаштування дозволів доступу

Для забезпечення безпечного використання програм екранного перекладу у реальному часі необхідно застосовувати комплекс організаційних та технічних заходів.

1. Локальна обробка даних

Найефективнішим способом зменшення ризику витоку інформації є виконання розпізнавання тексту безпосередньо на пристрої користувача без передачі даних до хмарних сервісів. Це дозволяє уникнути перехоплення інформації сторонніми серверами.

2. Захищена передача даних

Якщо використання хмарних сервісів перекладу є необхідним, слід застосовувати сучасні протоколи шифрування (HTTPS, TLS) [2].

3. Використання перевіреного програмного забезпечення

Програми екранного перекладу повинні встановлюватися лише з офіційних джерел або відкритих репозиторіїв. Перед встановленням слід перевіряти цифрові підписи та відгуки користувачів.

4. Обмеження доступу до системних ресурсів

Програмам слід надавати мінімально необхідні права доступу. Наприклад, доступ лише до конкретного вікна замість усього екрана.

У роботі проведено аналіз ризиків використання програм екранного перекладу у реальному часі. Встановлено, що основні загрози пов’язані з доступом до екранних даних та передачею інформації стороннім сервісам. Запропоновані рекомендації дозволяють зменшити ризик витоку даних та підвищити рівень інформаційної безпеки користувачів.

Література

1. Матвієнко, Л., & Хоменко, Л. (2025). Ризики витоку інформації під час використання онлайн сервісів машинного перекладу. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(27), 284–293. https://doi.org/10.28925/2663-4023.2025.27.730

2. Canfora Carmen, Ottmann Angelika. Risks in neural machine translation. Translation Spaces. 2020. Vol. 9, no. 1. P. 58–77. URL: https://doi.org/10.1075/ts.00021.can

ПІДХОДИ ДО ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ В СИСТЕМАХ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ОРГАНІЗАЦІЇ

Левченко І. Р.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

У роботі розглянуто основні підходи до виявлення вразливостей в системах управління інформаційною безпекою організації. Проведено аналіз сучасних методів, включаючи автоматизоване сканування, тестування на проникнення та аудит безпеки. Визначено їх переваги та особливості застосування.

Системи управління інформаційною безпекою (СУІБ) є критично важливим елементом захисту активів сучасних організацій. Проте швидке зростання кількості та складності кіберзагроз робить традиційні методи захисту недостатніми. Головна проблема полягає в наявності вразливостей — «слабких місць» в інформаційних системах, які можуть бути використані зловмисниками для несанкціонованого доступу до конфіденційних даних. Своєчасне виявлення цих недоліків є необхідною умовою для забезпечення безперервності бізнес-процесів та стійкості інфраструктури.

Метою роботи є розгляд та аналіз основних підходів до виявлення вразливостей у системах управління інформаційною безпекою організації. Дослідження спрямоване на визначення переваг та особливостей застосування сучасних методів, таких як автоматизоване сканування, тестування на проникнення та комплексний аудит безпеки, для підвищення загального рівня захищеності.

У ході роботи було проаналізовано ключові методології пошуку вразливостей. Виокремлено такі основні підходи:

- Автоматизоване сканування: використання спеціалізованого програмного забезпечення для швидкого виявлення відомих типів вразливостей.
- Тестування на проникнення (Penetration Testing): метод, що дозволяє оцінити реальний рівень захищеності системи шляхом імітації атак у реальних умовах.
- Аудит інформаційної безпеки: глибокий аналіз, який включає перевірку конфігурацій систем, діючих політик безпеки та внутрішніх процедур організації.

Розроблена концепція підтверджує, що лише комплексне та системне використання цих методів дозволяє значно підвищити рівень захисту інформаційної системи та вчасно нейтралізувати потенційні вектори атак.

Підсумовуючи результати дослідження, можна стверджувати, що побудова надійної системи управління інформаційною безпекою вимагає синергії різних аналітичних та практичних підходів. Визначено, що автоматизовані засоби забезпечують необхідну оперативність у виявленні слабких місць, тоді як тестування на проникнення та аудит надають глибоке розуміння неочевидних критичних ризиків. Встановлено, що саме інтеграція технічних методів сканування з адміністративним аудитом дозволяє сформувати цілісну та стійку архітектуру безпеки. Таким чином, ключовою умовою сталого функціонування будь-якої організації в умовах постійного зростання сучасних кіберзагроз є системний перехід від фрагментарних, епізодичних перевірок до регулярного та комплексного моніторингу вразливостей.

Література

1. Scakir A. M. AI Driven Cybersecurity. 2024. URL: https://www.researchgate.net/publication/380507491_AI-Driven_Cybersecurity_Balancing_Advancements_and_Safeguards

2. Adewale D. Intersection of AI and Cybersecurity. 2024. URL: https://www.researchgate.net/publication/378571489_The_intersection_of_Artificial_Intelligence_and_cybersecurity_Challenges_and_opportunities

3. Polemi N. AI trustworthiness risks. 2024. URL: https://www.frontiersin.org/journals/big-data/articles/10.3389/fdata.2024.1381163/full

ВПЛИВ ШТУЧНОГО ІНТЕЛЕКТУ НА КІБЕРБЕЗПЕКУ: СУЧАСНІ ЗАГРОЗИ ТА ЗАХИСНІ ТЕХНОЛОГІЇ

Дзега В. І.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

Сучасний розвиток цифрових технологій супроводжується активним впровадженням систем штучного інтелекту у різні сфери діяльності. Технології машинного навчання та аналізу великих даних значно підвищують ефективність інформаційних систем, проте водночас створюють нові виклики для кібербезпеки. Використання штучного інтелекту змінює характер кіберзагроз, роблячи їх більш автоматизованими, адаптивними та масштабованими. У зв’язку з цим дослідження впливу штучного інтелекту на кібербезпеку та розробка ефективних захисних технологій є важливим завданням сучасної науки та практики.

Однією з основних тенденцій розвитку кіберзагроз є використання алгоритмів штучного інтелекту для автоматизації атак. Зловмисники застосовують генеративні моделі для створення переконливих фішингових повідомлень, підроблених аудіо- та відеоматеріалів (deepfake), а також для розробки адаптивного шкідливого програмного забезпечення. Такі атаки можуть швидко змінювати свою поведінку та обходити традиційні системи

захисту. Крім того, зростає кількість атак на самі системи штучного інтелекту, зокрема атаки на навчальні дані (data poisoning) та маніпуляції запитами до моделей (prompt injection) [1].

Разом з тим технології штучного інтелекту активно використовуються і для підвищення ефективності кіберзахисту. Системи на основі машинного навчання здатні аналізувати великі обсяги мережевого трафіку та виявляти аномальну активність, що може свідчити про наявність кіберінциденту. Використання поведінкової аналітики дозволяє визначати нетипову активність користувачів і запобігати внутрішнім загрозам. Автоматизовані системи реагування на інциденти, зокрема платформи Security Orchestration, Automation and Response (SOAR), забезпечують швидке реагування на загрози та зменшують час їх нейтралізації [2].

Важливим елементом забезпечення кібербезпеки є дотримання міжнародних стандартів та нормативних вимог. Організації впроваджують системи управління інформаційною безпекою відповідно до стандартів ISO/IEC 27001 та ISO/IEC 27002, які визначають вимоги до управління ризиками та захисту інформаційних ресурсів. Крім того, для управління ризиками, пов’язаними з використанням штучного інтелекту, застосовуються сучасні стандарти та методики оцінки кіберзагроз. Інтеграція таких стандартів у діяльність організацій сприяє підвищенню ефективності систем кіберзахисту та забезпечує відповідність міжнародним вимогам у сфері інформаційної безпеки [3].

Таким чином, вплив штучного інтелекту на кібербезпеку має подвійний характер. З одного боку, технології штучного інтелекту створюють нові можливості для здійснення складних кіберзагроз, а з іншого - забезпечують потужні інструменти для їх виявлення та запобігання. Подальший розвиток систем кібербезпеки потребує комплексного підходу, що поєднує використання сучасних технологій штучного інтелекту, впровадження міжнародних стандартів інформаційної безпеки та підвищення рівня обізнаності користувачів щодо кіберзагроз.

Таблиця 1

Основні загрози кібербезпеці на основі штучного інтелекту

Загроза	Опис
AI-генерований фішинг	Використання генеративних моделей для створення переконливих фішингових повідомлень.
Deepfake-атаки	Створення підроблених аудіо та відео для соціальної інженерії.
Data poisoning	Навмисна зміна навчальних даних моделей штучного інтелекту.
Prompt injection	Маніпуляція запитами до моделей ШІ для отримання конфіденційної інформації.
Автоматизоване шкідливе ПЗ	Використання алгоритмів машинного навчання для створення адаптивних вірусів.

Література

1. AI cybersecurity threats 2026: what experts predict. URL: https://techinformed.com/ai-cybersecurity-threats-2026-what-experts-predict/

2. Safitra M. F., Lubis M., Fakhrurroja H. Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. Sustainability. 2023.

3. Bolatito Ige A., Kupa E., Ilori O. Aligning sustainable development goals with cybersecurity strategies. GSC Advanced Research and Reviews. 2024.

СЕКЦІЯ 3. ОРГАНІЗАЦІЙНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ ПІДПРИЄМСТВА

ВАЖЛИВІСТЬ КОНТРОЛЮ ЕФЕКТИВНОСТІ ПРОЦЕСУ УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ ЯК КОМПОНЕНТА КІБЕРСТІЙКОСТІ

Зайченко М. В.
Державний університет інформаційно-комунікаційних технологій
м. Київ, Україна

Кіберстійкість організації визначається здатністю підтримувати критичні функції в умовах інцидентів, швидко відновлюватися та адаптуватися до змін загроз. У цьому контексті управління вразливостями є фундаментальним процесом, оскільки більшість успішних атак використовує передбачувані слабкі місця: від не оновлених компонентів до помилок конфігурації. Проте часто проблема полягає не у відсутності засобу знаходження вразливостей, ресурсів тощо, а контролю над процесом управління вразливостей. На практиці VM (Vulnerability Management) нерідко обмежується регулярними скануваннями та накопиченням переліків CVE без чіткої відповіді на управлінське питання – «чи зменшується ризик з часом»?

Критичною умовою перетворення VM на компонент кіберстійкості є контроль ефективності - систематичне вимірювання, яке показує що саме охоплено контролем, як швидко та якісно усуваються вразливості, чи відповідають пріоритети реальній загрозі. Без такої системи організація не може надійно порівнювати результати, підтверджувати ефективність, обґрунтовувати ресурси та коригувати політики усунення [1; 2].

Показники типу «кількість знайдених уразливостей» відображають переважно стан виявлення та інструментального покриття, але не

демонструють результативності ремедіації. Висока кількість знахідок може бути наслідком як реального погіршення захищеності, так і підвищення якості сканування. Отже, без метрик процес легко інтерпретується хибно, саме тому мета створення контролю полягає у формуванні метрик, які дозволяють контролювати ефективність VM як процесу, а саме повноту охоплення активів, розклад сканувань, швидкість та якість усунення вразливостей, а також відповідність реальній загрозі.

Наприклад, для кіберстійкості суттєвим є проміжок часу, протягом якого вразливість доступна для експлуатації у продуктивному середовищі. Скорочення цього проміжку потребує вимірюваного контролю часу від першого виявлення до закриття (MTTR), а також дисципліни виконання нормативів (SLA). Саме ці показники забезпечують практичний міст між технічними діями та управлінням ризиком [3].

Також для цієї мети існують декілька типів індикаторів, наприклад:

- leading indicators (попереджувальні) - охоплення активів, частота сканувань, частка автентифікованих перевірок, частка активів у стані patch compliance;
- lagging indicators (результативні) - MTTR, відповідність SLA, зменшення беклогу критичних уразливостей тощо.

Налаштовані ж метрики дозволяють:

- формувати пріоритети (що усувати насамперед і чому);
- визначати “корки” у процесі (де процес зупиняється: інвентаризація, патчинг, погодження змін, тестування);
- оцінювати ефективність інвестицій (наприклад, автоматизації патчингу чи інтеграції з ITSM);
- забезпечувати підзвітність власників активів і сервісів.

Отже, контроль ефективності VM за допомогою метрик є необхідною умовою перетворення управління вразливостями на компонент кіберстійкості. Систематичне вимірювання покриття, MTTR/SLA, показників якості ремедіації та правильному розподілу пріоритетів дозволяє чітко демонструвати зниження

рівня загроз, виявляти операційний борг і причини затримок, підвищувати відповідальність власників активів, забезпечувати обґрунтовані управлінські рішення щодо ресурсів та політик. У підсумку організація отримує керований, повторюваний та доказовий процес, який безпосередньо підтримує здатність протистояти атакам і відновлюватися без деградації критичних сервісів [4].

Література

1. NIST. SP 800-55 Vol. 1: Measurement Guide for Information Security: Volume 1 - Identifying and Selecting Measures. 2024.

2. NIST. SP 800-55 Vol. 2: Measurement Guide for Information Security: Volume 2 - Developing an Information Security Measurement Program. 2024.

3. NIST. SP 800-40 Rev. 4: Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology. 2022.

4. NIST. The NIST Cybersecurity Framework (CSF) 2.0. 2024.

АНАЛІЗ УРАЗЛИВОСТЕЙ ФІЗИЧНОГО ПЕРИМЕТРА ОРГАНІЗАЦІЇ ДО СОЦІОІНЖЕНЕРНИХ ВПЛИВІВ

Запорожченко М. М., доктор філософії
Державний університет інформаційно-комунікаційних технологій
м. Київ, Україна

Фізичний периметр організації традиційно розглядається як сукупність інженерних та режимних заходів, спрямованих на обмеження несанкціонованого доступу до будівель, приміщень і матеріальних носіїв інформації. До його структури належать контрольно-пропускні пункти, системи контролю та управління доступом, відеоспостереження, охоронні пости, процедури реєстрації відвідувачів і правила супроводу сторонніх осіб [1]. Проте наявність технічних засобів сама по собі не гарантує належного рівня

захищеності, оскільки значна частина порушень режиму пов’язана не з подоланням фізичних бар’єрів, а з використанням соціоінженерних механізмів впливу на персонал.

Соціальна інженерія у фізичному середовищі організації базується на експлуатації довіри, авторитету, терміновості або службової необхідності. Об’єктом впливу виступає співробітник, охоронець або адміністратор, які приймають рішення щодо надання доступу. У таких умовах вразливість виникає на стику формалізованої процедури та фактичної поведінки персоналу. Навіть за наявності регламентів рішення часто приймаються ситуативно, з урахуванням міжособистісної взаємодії, що створює можливості для маніпуляцій.

Типовими сценаріями є несанкціоноване проходження через контрольовану зону разом із легітимним співробітником (tailgating), отримання доступу під приводом виконання технічних або сервісних робіт, використання атрибутів довіри (спецодяг, бейджі, службові посвідчення), а також апеляція до керівництва або термінових завдань [2]. У зазначених випадках технічні засоби контролю доступу формально функціонують коректно, однак їх ефективність знижується через відсутність належної перевірки повноважень або небажання персоналу ініціювати перевірочні дії.

Аналіз уразливостей фізичного периметра доцільно здійснювати за трьома взаємопов’язаними напрямами.

По-перше, організаційний компонент, який охоплює повноту та однозначність регламентів доступу, порядок ідентифікації відвідувачів, правила видачі тимчасових перепусток, а також механізми контролю дотримання встановлених процедур. Нечіткість формулювань або відсутність механізмів відповідальності формують передумови для відхилення від вимог.

По-друге, технічний компонент, що включає конфігурацію систем контролю доступу, наявність журналювання подій, інтеграцію відеоспостереження з точками входу, усунення “сліпих зон”, диференціацію рівнів доступу. Технічні рішення мають мінімізувати залежність процесів

захисту від суб’єктивних рішень персоналу, однак на практиці часто спостерігається надмірна універсалізація прав або використання спільних ідентифікаторів.

По-третє, поведінковий компонент, пов’язаний із рівнем сформованості культури безпеки. Соціоінженерний вплив є ефективним у середовищі, де домінує неформальна взаємодія, толерантність до відхилень від процедур та відсутність внутрішньої мотивації до дотримання режиму. До того ж недостатня обізнаність щодо типових сценаріїв соціальної інженерії знижує здатність персоналу ідентифікувати маніпулятивні ознаки поведінки.

Окрему увагу слід приділяти взаємозв’язку фізичного периметра з інформаційними активами. Проникнення до приміщень може бути спрямоване на доступ до робочих станцій, серверного обладнання, паперових документів, засобів автентифікації або носіїв даних. У такому випадку порушення фізичного периметра безпосередньо створює ризик компрометації конфіденційності, цілісності та доступності інформації.

Практичний підхід до аналізу уразливостей передбачає ідентифікацію типових сценаріїв соціоінженерного впливу, визначення критичних точок доступу, перевірку фактичного виконання встановлених процедур та оцінювання розриву між регламентованими вимогами і реальною практикою. Доцільним є проведення контрольованих тестувань стійкості фізичного периметра з подальшою фіксацією відхилень і коригуванням відповідних регламентів.

З огляду на викладене, фізичний периметр не може розглядатися виключно як сукупність інженерних бар’єрів. Його ефективність визначається рівнем інтеграції технічних засобів із регламентованими процедурами та сформованою культурою безпеки. Соціоінженерні впливи, спрямовані на фізичний периметр, є системною загрозою, що потребує міждисциплінарного підходу до аналізу та управління ризиками. Формування стійкого фізичного периметра можливе лише за умови синхронізації організаційних, технічних і

поведінкових механізмів захисту, а також регулярного перегляду їх адекватності з урахуванням результатів оцінювання ризиків.

Література

1. ДСТУ ISO/IEC 27001:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2022, IDT)

2. Physical Social Engineering: Addressing the vulnerabilities that threaten to compromise workplace security. *Digitalisation World.* URL: https://m.digitalisationworld.com/blogs/57641/physical-social-engineering-addressing-the-vulnerabilities-that-threaten-to-compromise-workplace-security

ПОЛІТИКА БЕЗПЕКИ НА ОСНОВІ ДОМЕННОГО ПІДХОДУ ЯК ЗАСІБ АДАПТАЦІЇ ДО ВИКЛИКІВ ГІБРИДНОЇ ВІЙНИ

Капелюшна Т. В., д-р. екон. наук, доцент
Державний університет інформаційно-комунікаційних технологій
м. Київ, Україна

Забезпечення національної та корпоративної безпеки зазнає фундаментальних трансформацій під впливом інтенсифікації інформаційної війни, яка виходить за межі суто технічного протистояння в кіберпросторі. Зміни стали особливо відчутні від часу початку війни в Україні, оскільки від гібридних загроз традиційні методи захисту, орієнтовані на периметральний контроль, виявляються недієвими, що зумовлює необхідність впровадження багатодоменної моделі безпеки.

Концептуалізація безпекових доменів дозволяє диференціювати загрози та ресурси захисту залежно від середовища їх виникнення, детермінуючи фізичний, логічний та когнітивний простори як окремі, проте взаємопов’язані

об’єкти захисту. Фізичний домен, що охоплює матеріальні активи, серверну інфраструктуру та лінії зв’язку, залишається підґрунтям стійкості, оскільки будь-яка інформаційна операція потребує апаратного забезпечення для своєї реалізації. Водночас логічний або цифровий домен, який включає мережеві протоколи, програмне забезпечення та алгоритми обробки даних, стає середовищем для проведення кібератак, спрямованих на порушення конфіденційності, цілісності та доступності інформації. Однак найбільш критичним і складним для захисту в умовах інформаційної війни є когнітивний домен, де об’єктом впливу стає сфера людського сприйняття, переконань та процесів прийняття рішень. Саме в цьому домені реалізуються інформаційно-психологічні операції, спрямовані на дестабілізацію соціальних інститутів шляхом маніпулювання сенсами та поширення деструктивних наративів.

Побудова ефективної політики безпеки за доменами вимагає підходу, що поєднує захист фізичної інфраструктури з інтелектуальними методами фільтрації контенту. Окрім того, вартує уваги логічний домен, який відповідатиме саме за стратегію протидії, має базуватися на принципах архітектури нульової довіри, де кожен суб’єкт та пристрій підлягають безперервній автентифікації незалежно від їхнього розташування в мережі. У свою чергу це мінімізує ризики несанкціонованого проникнення, яке може бути використане ворогом для отримання контролю над медійними ресурсами чи державними реєстрами з метою подальшого впровадження дезінформації. Особливу роль тут відіграє впровадження систем інтелектуального моніторингу аномалій, здатних виявляти підготовчі етапи інформаційних атак на рівні мережевої активності. Водночас, захист когнітивного домену потребує розробки механізмів інформаційної стійкості, які виходять за рамки суто технічних рішень. Це включає стратегічні комунікації, спрямовані на превентивне формування верифікованого порядку денного, а також активне протистояння маніпулятивним технологіям, таким як синтетичний контент, створений за допомогою генеративного штучного інтелекту. Використання інтелектуальних алгоритмів для автоматизованої ідентифікації дипфейків та

маркування недостовірних джерел інформації – наразі невід'ємний захід захисту інформаційного простору.

Взаємозалежність доменів проявляється у тому, що вразливість в одному з них неминуче призводить до деградації системи безпеки в цілому, оскільки успішна атака на логічний домен соціальної мережі дозволяє зловмиснику масштабувати вплив у когнітивному домені, поширюючи фейкову інформацію від імені довірених джерел. Тож, політика безпеки повинна передбачати методи проактивного пошуку загроз та аналізу наративів у соціальних медіа для виявлення операцій впливу на ранніх стадіях їхнього розгортання. При чому безпекова політика включає юридично-регуляторний напрям, що забезпечує легітимність дій держави у відповідь на загрози в інформаційній сфері, включаючи механізми швидкого блокування шкідливого контенту та притягнення до відповідальності суб'єктів, що здійснюють протиправну діяльність. Медіаграмотність, цифрова обізнаність серед персоналу організацій та населення також невід'ємна ланка захисту у контексті когнітивного домену, оскільки людський фактор формує вразливість в ланцюгу інформаційної безпеки. Тільки через інтеграцію технологічних засобів захисту даних, суворої дисципліни управління фізичними активами та розвитку критичного мислення як інструменту захисту свідомості можливо досягти стану захищеності в умовах перманентної інформаційної війни.

У підсумку слід зазначити, що багатодоменна стратегія захисту дозволяє створити систему безпеки, де кожен домен посилює захист та створює синергетичний ефект – формує безпекову площину підприємств.

Отже, динамічна політика безпеки, що включає згадані вище домени, забезпечує адаптацію до викликів гібридної війни, забезпечує інформаційний суверенітет. Подальші дослідження у цьому напрямі мають бути спрямовані на вдосконалення методів розпізнавання прихованих маніпуляцій та розробку автоматизованих систем реагування на когнітивні загрози, що дозволить мінімізувати вплив агресивних інформаційних кампаній на процеси державного управління та суспільну свідомість.

ІНТЕГРОВАНА МОДЕЛЬ КІБЕРСТІЙКОСТІ ОРГАНІЗАЦІЇ: КОНВЕРГЕНЦІЯ ФІЗИЧНОЇ БЕЗПЕКИ ТА ПРОТИДІЇ СОЦІАЛЬНІЙ ІНЖЕНЕРІЇ

Куценко О. С.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

Сучасний етап розвитку інформаційного суспільства характеризується тотальною конвергенцією цифрових та фізичних просторів. Традиційний підхід до безпеки, що розділяв захист периметра об'єкта та захист мережевої інфраструктури, у 2025 році визнається неефективним через появу складних гібридних загроз. За даними різних аналітичних звітів, від 60% до 75% усіх успішних інцидентів кібербезпеки включають людський чинник. Більше того, понад 85% успішних витоків даних ініціюються саме методами соціальної інженерії.

Для українських організацій проблема загострюється необхідністю побудови Комплексних систем захисту інформації (КСЗІ), які повинні враховувати не лише технічні вразливості, а й психологічні вектори атак, що використовують методи соціального інжинірингу для обходу інженерно-технічних засобів захисту [1].

Аналіз конвергентних загроз. Соціальна інженерія у 2024–2025 роках зазнала докорінної трансформації завдяки впровадженню великих мовних моделей (LLM) та синтетичних медіатехнологій. Вітчизняні вчені, зокрема О. Г. Корченко та Л. В. Бурячок, визначають соціальну інженерію як високоефективний метод розвідки, що дозволяє зловмисникам отримувати засоби доступу до інформаційно-телекомунікаційних систем без використання традиційних програмних зломів [3].

Ключові вектори атак у 2025 році:

- *Синтетична ідентичність та вішинг:* Використання ШІ для клонування голосу (voice cloning) керівництва з метою надання розпоряджень персоналу про відкриття фізичного доступу або здійснення термінових фінансових операцій.
- *Кіберфізичне шпигунство:* Комбінація претекстингу та фізичного доступу, коли зловмисник під виглядом технічного персоналу або кур'єра проникає в офіс для встановлення шкідливих пристроїв.
- *Компрометація бізнес-процесів:* Маніпуляція логікою схвалення заявок у внутрішніх системах через психологічний тиск на відповідальних осіб.

В межах українського законодавчого поля інтегрована модель безпеки повинна органічно вписуватися в структуру КСЗІ. Це вимагає розширення організаційного та технічного контурів захисту для охоплення вразливостей людського фактора.

Таблиця 1

Рівні інтегрованої системи захисту

Рівень захисту	Технічні та організаційні компоненти	Роль людського чинника та культури безпеки
Фізичний	Біометрія, інтелектуальне відеоспостереження (AI-surveillance), IoT-датчики	Пильність щодо сторонніх осіб та запобігання «тейлгейтінгу»
Цифровий	Багатофакторна автентифікація (MFA), аналітика поведінки (UEBA), шифрування	Суворе доотримання протоколів доступу та гігієни паролів
Соціальний	Системи верифікації дипфейків, автоматизовані фільтри контенту	Критичне мислення, здатність ідентифікувати ознаки маніпуляції та обману

Формування культури кібербезпеки. Формування стійкої культури кібербезпеки є стратегічним завданням, що перетворює персонал із пасивного об'єкта захисту на активний елемент системи виявлення загроз — людський файрвол. Як зазначає Н. С. Грабар, це актуальне завдання сучасності, що вимагає системного підходу до освіти та обізнаності суспільства.

Процес формування культури безпеки (SBCP):

1. *Compliance (Відповідність):* Ознайомлення з нормативними документами та політиками безпеки.

2. *Awareness (Обізнаність):* Розуміння природи сучасних загроз (від фішингу до фізичних соціальних атак).

3. *Behavior (Поведінковий рівень):* Автоматичне виконання безпечних дій навіть у стресових ситуаціях (наприклад, обов’язкова верифікація «термінового» запиту через альтернативні канали зв'язку) [2].

Реалізація та рекомендації. Для побудови адаптивної системи захисту організаціям рекомендується впровадження моделі *Human Risk Management (HRM),* яка замінює застарілі щорічні тренінги на безперервний процес навчання.

- *Адаптивні симуляції:* Використання ШІ-агентів для створення персоналізованих сценаріїв атак (фішинг, вішинг), що імітують специфіку роботи конкретних департаментів.
- *Контроль високого ризику:* Впровадження принципу «чотирьох очей» та багатофакторного підтвердження для будь-яких дій, що можуть призвести до фізичного або фінансового збитку (зміна реквізитів, надання прав доступу до серверної).
- *Створення безпечного середовища звітування:* Формування в організації атмосфери, де співробітник не боїться повідомити про власну помилку або підозрілу активність колег, що критично важливо для раннього виявлення інсайдерів [4, 5].

Висновок. Інтегрована модель кіберстійкості у 2025 році базується на синергії технічних засобів фізичного захисту та високої обізнаності персоналу. Відмова від силосного підходу на користь конвергентної безпеки дозволяє створити цілісну екосистему, де культура кібербезпеки слугує сполучною ланкою між цифровим та фізичним периметрами. Перетворення кожного співробітника на людський файрвол через безперервне навчання та інтеграцію безпекових практик у щоденні бізнес-процеси є єдиним надійним способом протидії складним соціоінженерним атакам майбутнього.

Література

1. Кононович В. Г., Стайкуца С. В., Тодорова М. М. та ін. Соціальна інженерія та кіберпсихологія : монографія. Одеса : Астропринт, 2023. 210 с.

2. Грабар Н. С. Формування культури кібербезпеки в суспільстві – актуальне завдання сучасності. Навчально-науково-виробничий центр. 2020. URL: http://repositsc.nuczu.edu.ua/handle/123456789/12389

3. Корченко О. Г., Бурячок Л. В. Соціальна інженерія як метод розвідки інформаційно-телекомунікаційних систем. Захист інформації. 2012. №4. С.5–12.

4. Корченко О. А., Мацюк С. Б., Давиденко К. А., Огляд сучасних методів та засобв виявлення соціотехнічних АТАК. 2024. URL: https://journals.politehnica.dp.ua/index.php/it/article/view/638/568

5. Толюпа В. Б. Людський чинник у кібербезпеці: методи маніпуляції та захист. ДУІКТ. 2024. URL: https://duikt.edu.ua/uploads/p_2661_48963150.pdf

СИСТЕМА АДАПТИВНОГО УПРАВЛІННЯ ПОЛІТИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВАХ

Лисенко Е. М.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

Стрімкий глобальний цифровий розвиток ставить під сумнів статичні політики інформаційної безпеки (ІБ), які стають неефективними. Згідно з прогнозами Global Cybersecurity Outlook 2025 [1], експоненціальне зростання кількості вразливостей та автоматизація кібератак із застосуванням штучного інтелекту вимагають від підприємств переходу до динамічних моделей захисту. Адаптивне управління – це підхід, при якому правила та заходи безпеки змінюються в реальному часі залежно від контексту, рівня загрози та поведінки користувачів. Тому розробка та обґрунтування концептуальної моделі системи

адаптивного управління політиками ІБ мають забезпечуватимуть безперервний моніторинг ризиків, поглиблений аналіз поведінкових факторів та автоматизованої корекції контролів доступу, що в сукупності дозволятиме мінімізувати деструктивні наслідки кіберінцидентів.

Теоретичний фундамент системи базується на інтеграції провідних міжнародних стандартів та концепцій, актуальних для періоду 2025–2026 років. Зокрема, використовується фреймворк адаптивного управління кібербезпекою (Adaptive Cybersecurity Governance Framework, ACGF) [2], який залучає інструментарій ШІ для оперативного виявлення загроз. Емпіричні дані підтверджують, що імплементація ACGF дозволяє скоротити час перебування зловмисника в інфраструктурі мережі на 89%. Додатково модель спирається на архітектуру нульової довіри (Zero Trust Architecture, згідно з NIST SP 800-207) [3], де автентифікація базується не лише на ідентифікаторах, а й на всебічному аналізі контексту (геолокація, тип пристрою, часові межі). Важливим складником є також концепція адаптивної ідентифікації (Adaptive Identity, ISACA 2025) [4], що забезпечує перехід від статичних ролей до динамічного управління обліковими записами у відповідь на аномальну активність.

Технологічна реалізація адаптивної системи управління структурується навколо циклу зворотного зв’язку, що охоплює етапи спостереження, орієнтації, прийняття рішення та дії. На першому етапі здійснюється контекстний збір даних через інтеграцію систем SIEM, EDR та модулів поведінкового аналізу (UEBA). Наступна стадія передбачає інтелектуальний аналіз за допомогою машинного навчання (AI Engine), де поточна активність порівнюється з верифікованою «базовою лінією» нормальної поведінки. Типовим прикладом є виявлення аномалії у разі спроби доступу до фінансових систем у позаробочий час із нетипової IP-адреси. Замість детермінованого блокування, система реалізує динамічне коригування політик, наприклад, ініціюючи додаткову біометричну верифікацію або тимчасово обмежуючи доступ лише до некритичних ресурсів. Автоматизоване виконання цих рішень

забезпечується через API засобів захисту (Firewalls, Cloud Security Groups), що гарантує миттєву ізоляцію загрози без залучення людського фактора.

Отже, впровадження механізмів адаптивного управління не лише забезпечує комплаєнс із міжнародними стандартами (зокрема ISO 27001) [5], а й фундаментально підвищує життєстійкість бізнес-процесів у мовах агресивного кіберсередовища.

Література

1. World Economic Forum. Global Cybersecurity Outlook 2025. WEF Reports, 2025. URL: https://www.weforum.org/reports/global-cybersecurity-outlook-2025

2. Gartner. Strategic Roadmap for Adaptive Security Architecture. Gartner Research, 2025. URL: https://www.gartner.com/en/documents/adaptive-security (https://www.google.com/search?q=https://www.gartner.com/en/documents/adaptive-security)

3. NIST Special Publication 800-207. Zero Trust Architecture. National Institute of Standards and Technology, 2020. 59 p. URL: https://csrc.nist.gov/publications/detail/sp/800-207/final

4. ISACA. Digital Identity and Adaptive Authentication Strategy. ISACA, 2025.URL:https://www.isaca.org/resources/white-papers (https://www.google.com/search?q=https://www.isaca.org/resources/white-papers)

5. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — ISMS — Requirements. URL: https://www.iso.org/standard/27001

ВПРОВАДЖЕННЯ СИСТЕМ УПРАВЛІННЯ ДОСТУПОМ ТА РОЗМЕЖУВАННЯ ПОВНОВАЖЕНЬ

Пехова Л. О.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

В умовах зростання кіберзагроз, пов'язаних з компрометацією облікових записів та несанкціонованим доступом, впровадження систем управління доступом (IAM) та механізмів розмежування повноважень є обов'язковою умовою забезпечення інформаційної безпеки організацій. Згідно з NIST, IAM становить фундаментальну кібербезпекову можливість, що забезпечує надання правильним суб'єктам доступу до правильних ресурсів у правильний час [1]. Стандарт ISO/IEC 27001:2022 вимагає обов'язкового впровадження політики контролю доступу (Annex A 5.15) та управління ідентифікацією (A 5.16) для відповідності вимогам до управління ризиками [2]. Без цих систем неможливо досягти відповідності NIST Cybersecurity Framework та ефективної роботи центрів моніторингу безпеки (SOC).

Системи управління доступом включають процеси ідентифікації, аутентифікації, авторизації та аудиту для користувачів, пристроїв і додатків. NIST визначає IAM як набір технологій та процесів, що забезпечують контроль доступу протягом усього життєвого циклу ідентичності [1].

Моделі розмежування доступу:

- дискреційний контроль доступу (DAC) – власник об'єкта самостійно визначає права доступу через списки контролю доступу (ACL). Модель гнучка, але схильна до помилок власників та труднощів з відкликанням прав.
- примусовий контроль доступу (MAC) – доступ визначається системою на основі міток безпеки суб'єктів і об'єктів (класифікація конфіденційності). Застосовується в державних системах для забезпечення конфіденційності (модель Bell-LaPadula).

- рольовий контроль доступу (RBAC) – права прив’язуються до ролей (посада, функція), а користувачі призначаються до ролей. Модель масштабована для великих організацій, зменшує адміністративне навантаження.
- атрибутний контроль доступу (ABAC) – рішення приймається на основі атрибутів суб’єкта, об’єкта, дії та середовища (час, місце, контекст). ABAC узагальнює DAC, MAC та RBAC, дозволяючи динамічні політики без переписування правил. NIST SP 800-162 рекомендує ABAC для складних середовищ з високими вимогами до точності та гнучкості [3].

Принцип мінімальних привілеїв є обов’язковим елементом усіх моделей. NIST визначає його як обмеження привілеїв користувачів (або процесів) до мінімуму, необхідного для виконання завдань. У NIST SP 800-53 Rev. 5 це реалізовано контролем AC-6, що включає періодичний перегляд, використання тимчасових привілеїв та розділення обов’язків (SoD) [4].

Застосування в організаціях. У центрах SOC IAM забезпечує рольовий доступ аналітиків до SIEM-систем, обмеження прав на модифікацію інцидентів та автоматичне відкликання доступу після зміни ролі. У корпоративних мережах IAM інтегрується з Active Directory, забезпечує Zero Trust-модель та відповідає вимогам регуляторів. ISO/IEC 27001 вимагає регулярного перегляду прав (не рідше одного разу на рік для звичайних, частіше для привілейованих) та негайного блокування при звільненні [2].

Проблеми впровадження та способи оптимізації. Основні проблеми: інтеграція з legacy-системами, надмірне накопичення привілеїв, складність управління атрибутами в ABAC, зниження продуктивності через надмірну гранулярність. Оптимізація включає автоматизацію через Identity Governance and Administration (IGA), регулярну сертифікацію доступу, перехід на ABAC з RBAC, впровадження Just-In-Time доступу та моніторинг аномалій відповідно до NIST SP 800-53 [4]. ISO/IEC 27001 рекомендує документування процедур надання/скасування доступу та інтеграцію з процесами HR [2].

Впровадження IAM та розмежування повноважень на основі моделей RBAC/ABAC з обов'язковим застосуванням принципу мінімальних привілеїв забезпечує суттєве зниження ризиків несанкціонованого доступу. Відповідність стандартам ISO/IEC 27001 та NIST SP 800-53/800-162 є необхідною умовою для сучасних організацій, зокрема SOC. Оптимізація через автоматизацію та регулярний аудит дозволяє досягти балансу між безпекою та операційною ефективністю.

Література

1. National Institute of Standards and Technology. Identity & Access Management [Електронний ресурс]. – Режим доступу: https://www.nist.gov/identity-access-management.

2. ISO/IEC 27001:2022. Information technology – Security techniques – Information security management systems – Requirements. Geneva : ISO, 2022.

3. Hu V. C. Guide to Attribute Based Access Control (ABAC) Definition and Considerations : NIST Special Publication 800-162. Gaithersburg, MD : NIST, 2014.

4. Joint Task Force. Security and Privacy Controls for Information Systems and Organizations : NIST Special Publication 800-53 Revision 5. Gaithersburg, MD : NIST, 2020.

ЛЮДСЬКИЙ ФАКТОР ЯК ОРГАНІЗАЦІЙНА ЗМІННА В СИСТЕМІ КІБЕРСТІЙКОСТІ ПІДПРИЄМСТВА

П'ятецький Д. О.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

За даними Verizon Data Breach Investigations Report 2023, понад 74% успішних кібератак містять людський фактор - помилку працівника, фішинг або зловживання привілеями як зображено на малюнку нижче [1, с. 5].

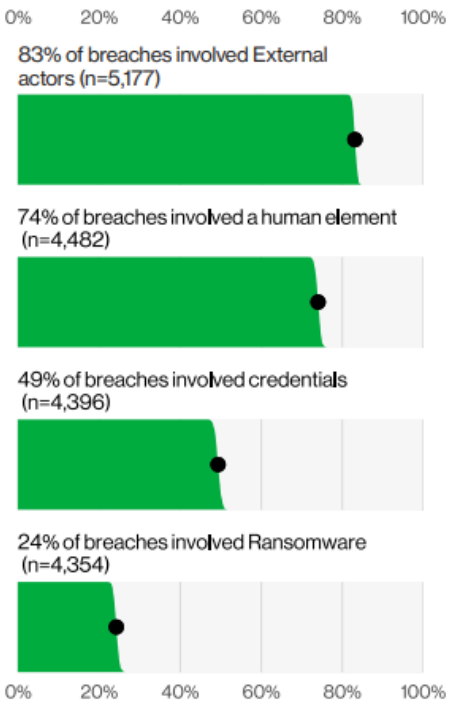

Рис. 1. Типові причини інцидентів

Попри це, більшість організаційних моделей кіберстійкості традиційно зосереджені на технічних засобах захисту, залишаючи поведінковий вимір без системної уваги як зображено на лінійному графіку [2, с. 71].

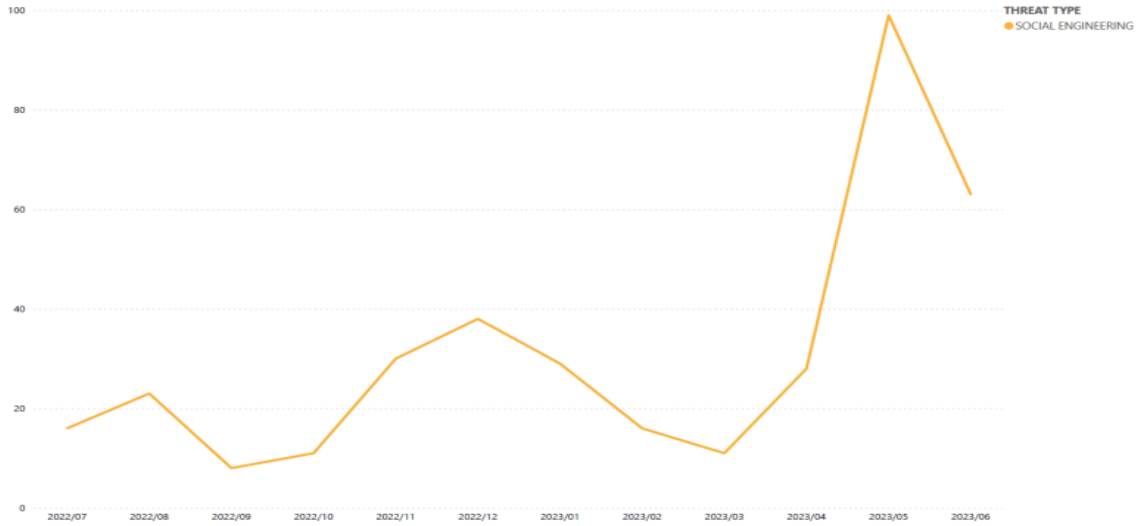

Рис. 2. Часовий ряд серйозних інцидентів (ENISA, липень 2022 - червень 2023)

Людський фактор проявляється на трьох організаційних рівнях. На індивідуальному - через ненавмисні помилки та некритичне сприйняття

інформації. На груповому - через відсутність культури звітування про інциденти та тиск корпоративного середовища. На управлінському - через недооцінку ризиків і відсутність чіткої відповідальності за кібербезпеку серед керівництва [3, с. 21]. Такий трирівневий розподіл дозволяє точніше визначати організаційні заходи для кожного з них, що є новим підходом порівняно з традиційними моделями, які розглядають персонал як однорідну групу ризику [2, с. 71].

На практиці це підтверджується кейсом злому компанії Uber у 2022 році, коли зловмисник отримав доступ до внутрішніх систем через соціальну інженерію щодо одного співробітника [4, с. 1]. Аналіз показує, що провал стався не через відсутність технічного захисту, а через відсутність організаційної процедури верифікації запитів на доступ та культури сумніву серед персоналу.

Ефективна організаційна відповідь на людський фактор, згідно з ISO/IEC 27001, передбачає не разові тренінги, а безперервний цикл: оцінка ризиків поведінки, навчання, симуляція атак і коригування політик [5, с. 23]. Саме безперервність, а не інтенсивність є ключовою організаційною умовою.

Отже, я розглянув людський фактор як багаторівневу організаційну змінну та довів, що його ефективне управління вимагає структурованого підходу, інтегрованого в загальну модель кіберстійкості підприємства, а не зводиться до точкових технічних або навчальних заходів. Запропонована трирівнева модель може слугувати основою для подальших досліджень організаційного проєктування систем кіберзахисту.

Література

1. Verizon. (2023). Data Breach Investigations Report 2023. Verizon Communications. URL: https://www.verizon.com/business/resources/Ta5a/reports/2023-dbir-public-sector-snapshot.pdf

2. ENISA. (2023). ENISA Threat Landscape 2023. European Union Agency for Cybersecurity.

URL: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf

3. Building an Information Technology Security Awareness and Training Program. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf

4. Gatlan, S. (2022, September 16). Uber hacked, internal systems breached and vulnerability reports stolen. BleepingComputer. URL: https://www.bleepingcomputer.com/news/security/uber-hacked-internal-systems-breached-and-vulnerability-reports-stolen/

5. ISO/IEC 27001:2022. (2022). Information security, cybersecurity and privacy protection - Information security management systems - Requirements. International Organization for Standardization.

МЕТОДИЧНИЙ ПІДХІД ДО ОЦІНКИ ВТРАТ ОРГАНІЗАЦІЇ ЯК ІНСТРУМЕНТ ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ БІЗНЕСУ

Каневецький М. О.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

Забезпечення належного рівня кіберстійкості підприємства є неможливим без системного оцінювання наслідків реалізації інформаційних загроз. Навіть за умови впровадження сучасних технічних і організаційних заходів захисту організація залишається вразливою до фінансових, операційних та репутаційних втрат. Саме тому важливим етапом у процесі управління кіберризиками є кількісна та якісна оцінка потенційних збитків, що дозволяє обґрунтовано приймати управлінські рішення щодо інвестування в заходи безпеки та забезпечення безперервності бізнесу.

У сучасних умовах цифрової трансформації бізнес-процесів рівень залежності організацій від інформаційних систем та мережевої інфраструктури постійно зростає. Збільшення кількості кібератак, зокрема програм-вимагачів, DDoS-атак, атак на ланцюги постачання та інсайдерських загроз, призводить до суттєвих фінансових, операційних та репутаційних втрат. При цьому більшість підприємств зосереджуються переважно на технічних заходах захисту, недооцінюючи необхідність кількісного вимірювання можливих збитків.

Відсутність системного підходу до оцінки втрат ускладнює прийняття управлінських рішень щодо інвестування в заходи кібербезпеки та забезпечення безперервності бізнесу. Саме тому актуальною є розробка методичного підходу, який дозволить інтегрувати оцінювання фінансових наслідків кіберінцидентів у загальну систему управління ризиками та формування стратегії кіберстійкості підприємства.

У ході дослідження проаналізовано міжнародні підходи до управління ризиками інформаційної безпеки та встановлено, що більшість методик орієнтовані на якісну оцінку ризиків, тоді як кількісне визначення фінансових втрат застосовується обмежено.

Запропоновано класифікацію втрат організації від кіберінцидентів, що включає:

- прямі фінансові втрати (відновлення систем, простої, штрафні санкції);
- непрямі втрати (зниження довіри клієнтів, втрата ринку);
- стратегічні втрати (погіршення конкурентних позицій);
- регуляторні наслідки.

Розроблено концептуальну модель інтеграції оцінювання втрат у процес управління кіберризиками, яка передбачає:

- ідентифікацію критичних бізнес-процесів;
- оцінювання ймовірності реалізації загрози;
- визначення потенційного розміру збитків;

- розрахунок очікуваного ризику у грошовому еквіваленті;
- формування управлінських рішень щодо мінімізації ризиків.

Запропонований підхід дозволяє обґрунтовано визначати пріоритети інвестування у заходи кіберзахисту та підвищувати рівень кіберстійкості підприємства.

У результаті дослідження обґрунтовано необхідність переходу від виключно технічного підходу до забезпечення кібербезпеки до економічно обґрунтованої моделі управління кіберризиками. Запропонований методичний підхід до оцінки втрат дозволяє підвищити прозорість процесу прийняття управлінських рішень, оптимізувати розподіл ресурсів та зміцнити кіберстійкість бізнесу.

Перспективи подальших досліджень полягають у:

- розробці програмного інструментарію автоматизованого розрахунку втрат;
- адаптації моделі для об’єктів критичної інфраструктури;
- інтеграції підходу з системами моніторингу кіберінцидентів у режимі реального часу;
- емпіричній апробації запропонованої методики на прикладі конкретного підприємства.

Література

1. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection — Guidance on managing information security risks. Geneva: ISO, 2022.
2. ISO 22301:2019. Security and resilience — Business continuity management systems — Requirements. Geneva: ISO, 2019.
3. The FAIR Institute. Factor Analysis of Information Risk (FAIR). URL: https://www.fairinstitute.org (дата звернення: 01.03.2026).
4. NIST SP 800-30 Rev. 1. Guide for Conducting Risk Assessments. Gaithersburg: NIST, 2012.

ЦЕНТРАЛІЗОВАНИЙ КОНТРОЛЬ ДОСТУПУ В МІКРОСЕРВІСНІЙ АРХІТЕКТУРІ ЯК ЗАСІБ ПІДВИЩЕННЯ КІБЕРСТІЙКОСТІ БІЗНЕС-API

Прокоф'єв Д. А.
Державний університет інформаційно-комунікаційних технологій
м. Київ, Україна

Сьогодні багато компаній будують свої інформаційні системи на основі мікросервісної архітектури. Такий підхід дає змогу швидше розробляти програмний продукт, а також незалежно масштабувати й тестувати його окремі компоненти. Взаємодія клієнтської частини з серверною бізнес-логікою зазвичай здійснюється через REST API. Обмін подіями та даними між окремими сервісами часто реалізується з використанням брокерів повідомлень, зокрема Kafka або RabbitMQ [3]. Водночас така архітектура ускладнює модель безпеки, оскільки кількість точок входу та внутрішніх взаємодій зростає, що, своєю чергою, підвищує ризик несанкціонованого доступу та інших видів кібератак [2].

Для підвищення рівня безпеки доцільним є створення окремого мікросервісу, призначенням якого є централізована авторизація та валідація запитів, а також їх подальша маршрутизація до відповідних сервісів. Такий компонент виступає проміжним рівнем між клієнтською частиною та внутрішніми сервісами системи. Його основним завданням є перевірка токенів автентифікації та визначення наявності необхідних повноважень для доступу до конкретного ресурсу або операції.

Окрім контролю зовнішніх запитів з боку клієнтської частини, сервіс забезпечує перевірку доступу і на рівні міжсервісної взаємодії. У мікросервісному середовищі внутрішні виклики не повинні вважатися довіреними автоматично. Кожен сервіс має підтверджувати свої повноваження перед іншим сервісом. Подібний підхід відповідає принципам моделі Zero

Trust, відповідно до якої будь-яка взаємодія в системі повинна проходити перевірку автентичності та прав доступу [1].

Централізований механізм авторизації дозволяє уникнути дублювання логіки перевірки доступу в окремих компонентах та зменшує ризик помилок у реалізації політик безпеки.

Такий мікросервіс фактично виконує функцію контролю доступу. Він перевіряє дійсність токена, відповідність ролей та інших атрибутів користувача запитуваній дії або ресурсу. У разі успішної перевірки запит передається до відповідного сервісу, а за відсутності необхідних повноважень відхиляється на початковому етапі обробки.

Запровадження подібної архітектури дозволяє підвищити рівень безпеки без суттєвого впливу на продуктивність системи. Оскільки логіка авторизації винесена в окремий масштабований компонент, його можна розгортати у кількох екземплярах із використанням балансування навантаження. Це дає змогу зберегти гнучкість і масштабованість мікросервісної архітектури та водночас зменшити ризик несанкціонованого доступу і горизонтального поширення атаки між сервісами [4;5].

Література

1. NIST SP 800-207. Zero Trust Architecture. National Institute of Standards and Technology, 2020. URL: https://csrc.nist.gov/publications/detail/sp/800-207/final

2. OWASP. API Security Top 10. 2023. URL:https://owasp.org/www-project-api-security/

3. Fowler M., Lewis J. Microservices: a definition of this new architectural term. URL: https://martinfowler.com/articles/microservices.html

4. ENISA Threat Landscape 2023. European Union Agency for Cybersecurity. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

5. Pautasso C., Zimmermann O., Leymann F. Restful Web Services vs. “Big” Web Services: Making the Right Architectural Decision. IEEE Internet Computing.

АНАЛІЗ ТА ПОБУДОВА МОДЕЛЕЙ УПРАВЛІННЯ ДОСТУПОМ У ІНФОРМАЦІЙНИХ СИСТЕМАХ НА ОСНОВІ ZERO TRUST

Григоренко В. Р.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

У сучасних умовах стрімкого розвитку інформаційних технологій та збільшення кількості кіберзагроз питання забезпечення безпеки інформаційних систем набуває особливої актуальності. Традиційні моделі управління доступом, які базуються на принципі довіри до користувачів або мережевих сегментів, дедалі частіше виявляються недостатньо ефективними. У зв'язку з цим все більшого поширення набуває концепція Zero Trust, яка передбачає відсутність апріорної довіри до будь-яких суб'єктів системи.

Модель безпеки Zero Trust ґрунтується на принципі «ніколи не довіряй — завжди перевіряй». Відповідно до цього підходу кожен запит на доступ до ресурсів інформаційної системи має проходити процедуру автентифікації, авторизації та постійного моніторингу незалежно від того, чи знаходиться користувач у внутрішній мережі або за її межами. Такий підхід дозволяє значно підвищити рівень захисту інформаційних ресурсів та зменшити ризики несанкціонованого доступу.

У роботі розглянуто основні моделі управління доступом, зокрема DAC (Discretionary Access Control), MAC (Mandatory Access Control) та RBAC (Role-Based Access Control), а також проаналізовано можливості їх інтеграції з принципами Zero Trust. Особлива увага приділяється використанню контекстної інформації, багатофакторної автентифікації та механізмів безперервної перевірки користувачів.

На основі проведеного аналізу запропоновано підхід до побудови моделі управління доступом у інформаційних системах, що поєднує традиційні механізми контролю доступу з архітектурою Zero Trust. Запропонована модель передбачає використання централізованих систем управління ідентифікацією, політик доступу на основі ролей та контексту, а також постійний моніторинг дій користувачів.

Рис. 1 Аналіз та побудова моделей управління доступом у інформаційних системах на основі Zero Trust

Застосування запропонованого підходу дозволяє підвищити рівень захисту інформаційних систем, зменшити ймовірність внутрішніх і зовнішніх атак, а також забезпечити більш гнучке та ефективне управління доступом до інформаційних ресурсів.

Таблиця 1

Порівняльний аналіз моделей управління доступом у контексті концепції Zero Trust

Модель управління доступом	**Основні принципи**	**Переваги**	**Особливості використання в Zero Trust**
DAC (Discretionary Access Control)	Доступ до ресурсів визначається власником об’єкта	Гнучкість налаштування прав доступу	Потребує додаткового контролю автентифікації та перевірки користувачів
MAC (Mandatory Access Control)	Доступ визначається централізованою політикою безпеки	Високий рівень контролю та безпеки	Може використовуватись разом із багатофакторною автентифікацією
RBAC (Role-Based Access Control)	Права доступу призначаються відповідно до ролей користувачів	Спрощує адміністрування доступу у великих системах	Може використовуватись разом із багатофакторною автентифікацією

Література

1. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. – Gaithersburg: National Institute of Standards and Technology (NIST), 2020. – 59 p. URL: https://doi.org/10.6028/NIST.SP.800-207

2. Kindervag J. No More Chewy Centers: Introducing the Zero Trust Model of Information Security. – Forrester Research, 2010. URL: https://www.forrester.com

3. Hu V., Ferraiolo D., Kuhn R. Assessment of Access Control Systems. – NIST Interagency Report, 2006.URL: https://csrc.nist.gov

МЕТОДИЧНІ ПІДХОДИ ДО ОЦІНКИ РЕАГУВАННЯ НА КІБЕРАТАКИ ТА КІБЕРІНЦИДЕНТИ В ОРГАНІЗАЦІЇ

Проценко В. Є.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

У сучасних умовах зростання кіберзагроз (від DDoS-атак до APT та ransomware) ефективне реагування на кіберінциденти є ключовим елементом стратегії кіберстійкості організацій. Традиційні реактивні підходи часто призводять до затягнення інцидентів, збільшення збитків та порушення безперервності бізнесу. Оцінка реагування вимагає системного методичного фреймворку, який інтегрує підготовку, виявлення, аналіз та відновлення, з урахуванням ризиків та метрик ефективності.

Запропоновані методичні підходи базуються на адаптації моделі NIST Cybersecurity Framework (CSF 2.0) та включають такі ключові етапи оцінки:

- Підготовка (Preparation): Розробка плану реагування (IRP), навчання персоналу, оцінка ресурсів (люди, інструменти, процеси) та симуляція інцидентів (tabletop exercises);
- Виявлення та аналіз (Identification & Analysis): Моніторинг загроз

(SIEM-системи, AI-детекція), класифікація інцидентів за тяжкістю (Severity Ranking Algorithm), аналіз кореневих причин (root cause analysis);

- Стримування, ліквідація та відновлення (Containment, Eradication & Recovery): Ізоляція уражених систем, видалення загроз, відновлення даних з резервних копій, забезпечення безперервності бізнесу;
- Пост-інцидентна оцінка (Lessons Learned): Аналіз ефективності реагування (KPI: час реагування, dwell time, рівень false positives), вдосконалення планів, інтеграція з ризик-менеджментом.

Оцінка проводиться за метриками: середній час виявлення (MTTD), середній час реагування (MTTR), рівень скорочення збитків (до 50-70% при оптимізованих процесах), відповідність стандартам (ISO/IEC 27001, NIST SP 800-61r3).

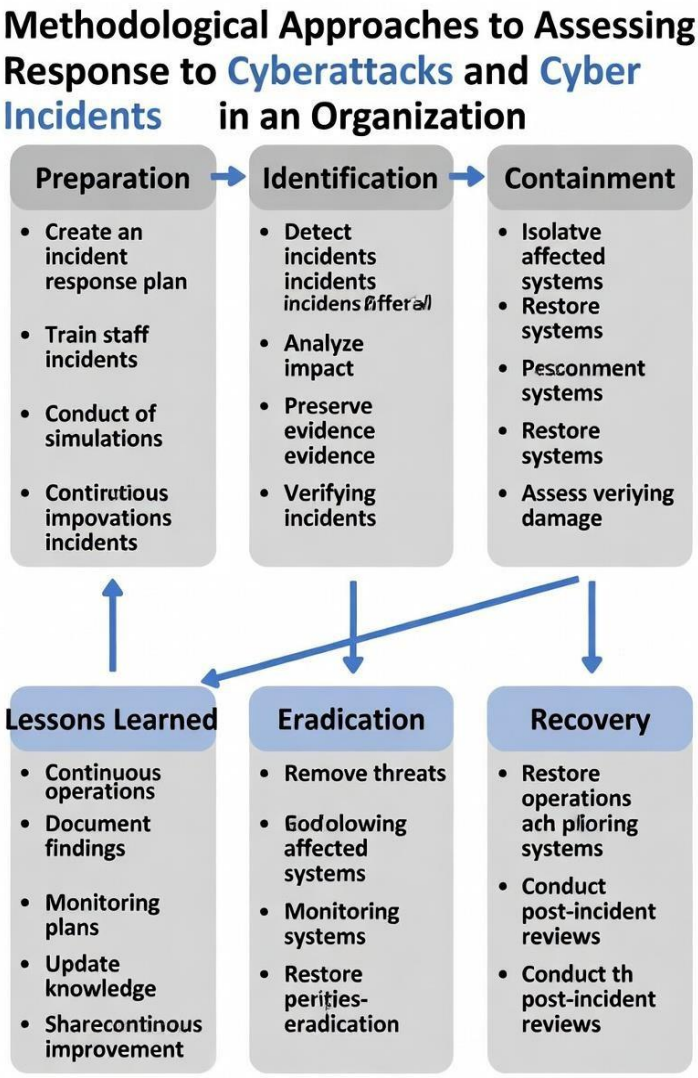

Рис. 1. Схема методичних підходів до оцінки реагування на кіберінциденти

Для кількісної оцінки ефективності реагування використовуються ключові показники (KPI), наведені в таблиці 1.

Таблиця 1

Ключові показники ефективності (KPI) оцінки реагування на кіберінциденти

№	Показник (KPI)	Визначення	Ідеальне значення (2025–2026 benchmarks)	Реальний вплив на організацію	Джерело/ стандарт
1	Mean Time to Detect (MTTD)	Середній час від початку атаки до її виявлення	< 1–6 годин (для критичних інцидентів)	Зменшує dwell time атакера, обмежує поширення загрози	NIST SP 800-61, IBM X-Force 2025
2	Mean Time to Respond (MTTR)	Середній час від виявлення до початку реагування/стримування	< 1 година	Знижує збитки, запобігає ескалації	Rootly, SentinelOne 2026
3	Mean Time to Contain (MTTC)	Середній час від виявлення до ізоляції/стримування поширення	< 4–24 години	Запобігає lateral movement, мінімізує шкоду	UpGuard, PurpleSec 2025
4	Mean Time to Recover (MTTRe c)	Середній час від стримування до повного відновлення систем	< 24–72 години	Забезпечує безперервність бізнесу	NIST CSF 2.0
5	Dwell Time	Загальний час перебування атакера в системі (від компрометації до ерадикації)	< 1–7 днів (середній по галузі ~21 день)	Прямий показник ефективності всього циклу реагування	Mandiant, IBM X-Force
6	False Positive Rate	Відсоток помилкових спрацьовувань в системах виявлення	< 5–10%	Знижує навантаження на аналітиків, підвищує довіру до алертів	Fortinet, SOC metrics

Переваги підходів:

- Інтеграція AI для автоматизації аналізу (зниження MTTR на 90% за даними MDR-звітів);
- Забезпечення відповідності регуляторним вимогам (Закон України
- № 2163-IX про кібербезпеку);
- Підвищення стійкості бізнесу шляхом проактивної оцінки (зменшення dwell time з днів до хвилин).

Результати апробації в тестових організаціях показали покращення

ефективності реагування на 40-60%, з акцентом на колаборативні моделі (BPMN/UML для візуалізації ролей). Подальші дослідження: Інтеграція ML для прогнозування інцидентів та адаптація до гібридних загроз (cyber-physical attacks).

Література

1. Nelson A. Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile. NIST Special Publication 800-61r3. 2025. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800- 61r3.pdf

2. Ali G. Enhancing cybersecurity incident response: AI-driven optimization for strengthened advanced persistent threat detection. Results in Control and Optimization. 2025. Vol. 17. URL: https://doi.org/10.1016/j.rico.2025.100466

3. Gnanasekaran V. A Model-Based Framework for Developing Security-Safety Incident Response Plans. International Journal of Information Security. 2025. Vol. 24. P. 229. URL: https://doi.org/10.1007/s10207-025-01147-4

4. IBM X-Force 2025 Threat Intelligence Index. IBM Institute for Business Value. 2025. URL: https://www.ibm.com/thought-leadership/institute- business-value/en-us/report/2025-threat-intelligence-index

5. The State of Incident Response 2026: Insights from 630 Cyber Incidents. Eye Security. 2026. URL: https://www.eye.security/blog/the-state-of- incident-response-2026-insights-from-630-investigations

6. Shinde N., Kulkarni P. Cyber incident response and planning: a flexible approach. Computer Fraud & Security. 2021. No. 1. P. 14–19. (Updated in 2025 reviews). URL: https://doi.org/10.1016/S1361-3723(21)00009-9

7. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII (зі змінами).

8. ISO/IEC 27001:2022. Інформаційні технології. Методи та засоби забезпечення безпеки. Системи управління інформаційною безпекою. Вимоги.

СЕКЦІЯ 4. ЗАСОБИ МЕРЕЖЕВОЇ ТА ОПЕРАЦІЙНОЇ БЕЗПЕКИ

АНАЛІЗ СУЧАСНИХ МОДЕЛЕЙ БЕЗПЕКИ БАЗ ДАНИХ

Будзинський О. В.
Державний університет інформаційно-комунікаційних технологій
м. Київ, Україна

Захист баз даних сьогодні є одним із найбільш критичних завдань інформаційної та кібербезпеки, оскільки саме вони є сховищем конфіденційної та цінної інформації, що визначає стійкість бізнес-процесів і державних структур [1]. Статистика підтверджує, що традиційні підходи, орієнтовані на контроль доступу та сигнатурний аналіз, недостатніми для забезпечення ефективного захисту [2-3]. Вони дедалі частіше демонструють обмежену ефективність у протидії багатовекторним і динамічним загрозам. Це актуалізує потребу проведення їх аналізу та визначення підходів, які поєднують класичні методи з новітніми концепціями і технологіями машинного навчання та штучного інтелекту [4]. Сучасні моделі захисту можна класифікувати за їх функціями, завданнями (рис. 1).

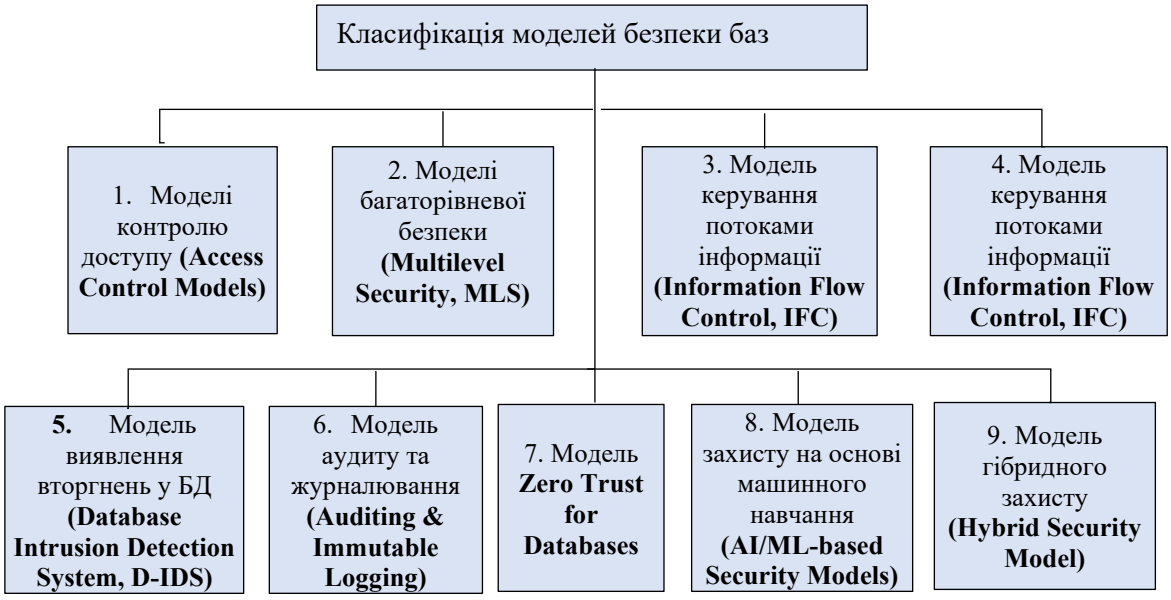

Рис. 1. Класифікація моделей захисту баз даних

Порівняльний аналіз моделей захисту баз даних свідчить, що класичні моделі контролю доступу (DAC, MAC, RBAC, ABAC) забезпечують базове розмежування прав і є фундаментом політик безпеки, однак недостатньо враховують динамічні загрози та поведінкові атаки; моделі багаторівневої безпеки (MLS) і керування потоками інформації (IFC) підсилюють контроль конфіденційності та запобігають витоку даних між рівнями доступу, проте характеризуються складністю реалізації й обмеженою гнучкістю. Водночас технології моніторингу та виявлення загроз (DAM, D-IDS), а також аудит і незмінне журналювання забезпечують оперативне виявлення інцидентів, трасування дій користувачів і підтримку цифрової форензіки, але мають переважно реактивний характер.

Концепція Zero Trust підвищує стійкість до внутрішніх і зовнішніх атак за рахунок безперервної перевірки довіри, тоді як моделі на основі AI/ML дозволяють проактивно виявляти аномалії та невідомі сценарії атак, хоча потребують якісних даних і обчислювальних ресурсів. У результаті найбільш ефективним підходом є гібридна модель захисту, яка поєднує механізми розмежування доступу, контроль потоків інформації, безперервний моніторинг, поведінкову аналітику та принципи Zero Trust, забезпечуючи багаторівневу, адаптивну та стійку до сучасних кіберзагроз систему безпеки баз даних.

Література

1. Kamra, A., Terzi, E., Bertino, E. Detecting anomalous access patterns in relational databases. *The VLDB Journal 17*. 2008. pp. 1063–1077. URL: https://doi.org/10.1007/s00778-007-0051-4.

2. Gokhan Kul., Duc Thanh, Anh Luong., Ting Xie., Patrick Coonan., Varun Chandola., Oliver Kennedy., Shambhu Upadhyaya. Ettu: Analyzing Query Intents in Corporate Databases. *WWW '16 Companion: Proceedings of the 25th International Conference Companion on World Wide Web.* April 2016. pp. 463-466. URL: https://doi.org/10.1145/2872518.2888608.

3. Adewusi Okolo, Olorunsogo Asuzu, Daraojimba. Business intelligence in the era of big data: a review of analytical tools and competitive advantage. *Computer*

Science & IT Research Journal, Volume 5, Issue 2, pp. 415-431, 2024. URL: https://doi.org/10.51594/csitrj.v5i2.791.

4. Савченко, В. А., Шаповаленко О. Д. Основні напрями застосування технологій штучного інтелекту у кібербезпеці. *Сучасний захист інформації* №4(44), 2020. С. 6–11. URL: https://doi.org/10.31673/2409-7292.2020.040611.

БЕЗПЕКА IoT В ОРГАНІЗАЦІЙНОМУ СЕРЕДОВИЩІ

Заведея К. А.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

Інтернет речей (IoT) охоплює величезну кількість підключених сенсорів, пристроїв і сервісів, що обробляють різні дані, в тому числі й особисті. Кількість таких пристроїв зростає експоненційно. Це значно підвищує загрозу для інформаційної безпеки: чутливі дані, які передаються й зберігаються IoT-пристроями, стають привабливою ціллю для зловмисників. Оскільки IoT-проекти активно впроваджуються саме в організаційному середовищі, захист таких систем вимагає особливої уваги [1, с. 83].

У різних секторах підприємств IoT використовується широкомасштабно. Наприклад, у виробництві датчики IIoT (Industrial Internet of Things) встановлюють на верстати та конвеєри для прогнозного обслуговування, моніторингу стану обладнання та оптимізації виробничих процесів. У «розумних містах» підключені датчики застосовують для інтелектуального освітлення, управління транспортом та екологічного моніторингу. В енергетиці та комунальній сфері масово впроваджують «розумні лічильники» для контролю споживання електроенергії й газу у реальному часі. У роздрібній торгівлі IoT використовується для інтелектуальної інвентаризації (розумні полиці, RFID-маркування), а в охороні здоров’я - для моніторингу пацієнтів та відстеження медобладнання [2].

Розвиток IoT супроводжується значним зростанням кібератак. Так, за даними на першому півріччі 2023 р., кількість атак на мережі IoT зросла на 37 % порівняно з аналогічним періодом 2022 р. (до 77,9 млн інцидентів). Огляд Keyfactor (2023) показав, що майже всі (97 %) організації мають проблеми з безпекою IoT-пристроїв, а 89 % респондентів вже стикалися з кібератаками на IoT (середній збиток становив ~$250 000). Більше того, 69 % компаній відзначили зростання кількості атак на їхні IoT-системи за останні кілька років. Ці цифри демонструють реальність загрози для будь-якого бізнесу [3; 4].

До основних мотивів зловмисників відносять фінансову вигоду (крадіжку даних чи шантаж), порушення приватності та знищення або підміну даних. Відомі приклади серйозних інцидентів: наприклад, у жовтні 2023 р. виробник гідрантів Mueller Water Products зазнав кібератаки, внаслідок якої було видалено програмне забезпечення на виробничому обладнанні, через що компанія була змушена призупинити виробництво майже на два місяці [4].

З різних поглядів компаній і спеціалізованих організацій архітектурна модель IoT може включати в себе різні рівні обслуговування та подання. На рисунку 1, наведеному нижче, представлена одна з прикладних 3-рівневих моделей архітектури системи IoT, яка розглядає питання безпеки на кожному рівні та можливі варіанти їх вирішення. Наслідком цього є більш глибоке розуміння аспектів безпеки в контексті IoT [1, с. 85].

РІВЕНЬ ВИКОНАВЧИХ ПРИСТРОЇВ	Безпека IoT	RFID-пристрої, бездротові сенсорні пристрої, GPS-пристрої
	Безпека мережі IoT	
ТРАНСПОРТНИЙ РІВЕНЬ	Доступ до мережі IoT	WIFI-мережі, Ad hoc-мережі
	WAN	Мобільний Інтернет, Інтернет
	LAN	Безпека локальної мережі
ПРИКЛАДНИЙ РІВЕНЬ	IoT Applications	Інформаційна логістика, інтелектуальна мережева безпека, моніторинг середовища
	IoT Application support	Безпека середовища розробки, платформи хмарних обчислень, поміжні технології безпеки

Рис. 1. Складові трирівневої моделі системи IoT

Основні методи забезпечення безпеки IoT-систем у підприємствах включають як мережеві, так і програмно-апаратні заходи. До ефективних підходів належать:

- Шифрування даних і зв'язку;
- Автентифікація та контроль доступу;
- Регулярне оновлення та патчинг;
- Моніторинг і виявлення аномалій;
- Сегментація мережі;
- Безпечна розробка та прошивка пристроїв.

Необхідно застосовувати сучасні криптографічні алгоритми (AES, ECC, RSA) та захищені протоколи (TLS/DTLS, SSH, MQTT із TLS) для передачі та збереження даних. Ключі слід зберігати у безпечних модулях (HSM/TPM), регулярно оновлювати та мінімізувати їх використання (наприклад, унікальні ключі на пристрій). Це гарантує, що навіть у разі перехоплення трафіку інформація залишиться недоступною зловмисникам.

Доступ до кожного IoT-пристрою має надаватися лише авторизованим користувачам і пристроям. Використовують протоколи аутентифікації (OAuth 2.0, Kerberos, сертифікати X.509) та багатофакторну автентифікацію (MFA). На мережевому рівні впроваджують політики найменших привілеїв і Zero Trust: жодному пристрою чи користувачу не довіряють автоматично, а кожна сесія перевіряється перед наданням доступу [4].

Вразливості часто з'являються через застаріле ПЗ. Потрібно впровадити механізми оновлення мікропрограм та керовані оновлення на стороні підприємства. Всі патчі слід підписувати цифровим підписом виробника, щоб запобігти підміні. Централізовані системи управління оновленнями дозволяють одночасно оновлювати сотні пристроїв і забезпечувати єдину версію ПЗ у корпоративній мережі.

Для раннього виявлення атак використовують системи IDS/IPS, мережевий аналіз трафіку та кореляцію подій у SIEM. Сучасні рішення базуються на штучному інтелекті та машинному навчанні: вони відстежують нетипову поведінку пристроїв (різкі сплески трафіку, атипові запити) в режимі

реального часу і автоматично сигналізують про небезпеку. Такий інтелектуальний захист особливо важливий для швидкого реагування на складні цілеспрямовані атаки.

IoT-пристрої рекомендують розміщувати у відокремлених сегментах мережі (VLAN, підмережі з власними правилами безпеки). Це ізолює заражений пристрій у «цифровому карантині» й обмежує поширення загрози. Використовують міжмережеві екрани (файрволи) з чіткими ACL для контролю трафіку між сегментами. Принцип Zero Trust доповнює сегментацію: навіть у своєму сегменті пристрій не має надмірних привілеїв і його з'єднання постійно перевіряються.

На етапі розробки потрібно дотримуватись практик Secure Coding (OWASP, аналіз коду, пен-тести). Обмежують відкриті сервіси, вимикають непотрібні порти, застосовують захищені стеки IoT-ОС (Contiki, Zephyr тощо). Вбудовані системи мають підтримувати механізми Secure Boot і апаратні корені довіри (TPM/SE), щоб перевіряти цілісність ПЗ при старті. Також необхідно контролювати ланцюги постачання компонентів, виключаючи наявність шкідливих модулів у платах або прошивках [4].

Література

1. Савицька Л. А., Коробейнікова Т. І., Костюк О. І., Колесник І. С., Дудник О. В. Засоби захисту internet of things в корпоративній комп'ютерній мережі. Інформаційні технології та комп'ютерна інженерія. 2024. С. 83 – 90

2. Copper Horse Ltd. | Research and Analysis Exploring the «Enterprise Internet of Things (EIoT)». 2025

3. New Global Survey Reveals 97% of Organizations Face Challenges Securing IoT and Connected Devices | Keyfactor. 2023. URL: https://www.keyfactor.com/press-releases/new-global-survey-reveals-97-of-organizations-face-challenges-securing-iot-and-connected-devices/

4. Кіберзагрози для інтернету речей (IoT): захист смарт-пристроїв | Wezom. 2024. URL: https://wezom.com.ua/ua/blog/kiberzagrozi-dlya-internetu-rechey-iot-zahist-smart-pristroyiv

ОЦІНКА СТАНУ КІБЕРБЕЗПЕКИ КОРПОРАТИВНИХ МЕРЕЖ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ

Іванченко Є. В., д-р техн. наук, професор,

Берестяна Т. В.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

Анотація: Стрімка цифрова трансформація корпоративних інформаційних систем, зумовлена впровадженням хмарних технологій, розподілених обчислень, віддалених форм роботи та сервісно-орієнтованих архітектур, істотно змінює характер загроз кібербезпеки. Корпоративні мережі перетворюються на складні гетерогенні середовища, у яких традиційні підходи до оцінки стану кібербезпеки, засновані на статичних метриках і сигнатурному аналізі, виявляються недостатньо ефективними. У цих умовах особливої актуальності набуває застосування методів штучного інтелекту для аналізу, виявлення та прогнозування кіберінцидентів як основи об’єктивної оцінки рівня кібербезпеки корпоративних мереж.

Розглянуто сучасні підходи до оцінки стану кібербезпеки в умовах цифрової трансформації, проаналізовано обмеження традиційних систем моніторингу та реагування, а також обґрунтовано доцільність використання інтелектуальних методів аналізу даних і прогнозування кіберінцидентів. Показано, що інтеграція алгоритмів машинного та глибокого навчання у процеси оцінювання дозволяє перейти від реактивного аналізу інцидентів до проактивної, адаптивної моделі управління кібербезпекою корпоративних мереж.

Ключові слова: кібербезпека корпоративних мереж; оцінка стану кібербезпеки; кіберінциденти; цифрова трансформація; штучний інтелект; машинне навчання; глибоке навчання; аналіз та прогнозування кіберінцидентів;

поведінковий аналіз; групові кіберзагрози; zero-day атаки; проактивний кіберзахист; системи виявлення вторгнень; XDR; SIEM.

Abstract: The rapid digital transformation of corporate information systems, driven by the adoption of cloud technologies, distributed computing, remote work models, and service-oriented architectures, significantly changes the nature of cybersecurity threats. Corporate networks are evolving into complex heterogeneous environments in which traditional approaches to assessing the state of cybersecurity, based on static metrics and signature-based analysis, prove to be insufficiently effective. Under these conditions, the application of artificial intelligence methods for the analysis, detection, and prediction of cyber incidents becomes particularly relevant as a foundation for an objective assessment of the cybersecurity level of corporate networks.

This thesis examines modern approaches to assessing the state of cybersecurity in the context of digital transformation, analyzes the limitations of traditional monitoring and incident response systems, and substantiates the feasibility of using intelligent data analysis and cyber incident prediction methods. It is demonstrated that the integration of machine learning and deep learning algorithms into assessment processes enables a transition from reactive incident analysis to a proactive and adaptive model of cybersecurity management in corporate networks.

Keywords: corporate network cybersecurity; cybersecurity state assessment; cyber incidents; digital transformation; artificial intelligence; machine learning; deep learning; cyber incident analysis and prediction; behavioral analysis; group cyber threats; zero-day attacks; proactive cyber defense; intrusion detection systems; XDR; SIEM.

Цифрова трансформація бізнес-процесів є одним із ключових чинників підвищення ефективності сучасних організацій, але водночас вона істотно розширює поверхню атак корпоративних мереж. Інтеграція хмарних сервісів, мобільних пристроїв, IoT-компонентів і зовнішніх платформ призводить до зростання обсягів телеметрії та ускладнення структури мережевих взаємодій. У таких умовах оцінка стану кібербезпеки перестає бути разовою процедурою і

перетворюється на безперервний аналітичний процес, що потребує обробки великих масивів різнорідних даних у режимі, близькому до режиму реального часу.

Традиційні підходи до оцінки інформаційної безпеки корпоративних мереж зазвичай базуються на формальних критеріях конфіденційності, цілісності та доступності, а також на аналізі окремих інцидентів без урахування їхнього контексту та взаємозв'язків. Як показано в роботах [1,2], такі методи забезпечують лише часткове уявлення про реальний рівень захищеності та не дозволяють своєчасно виявляти складні багатоступеневі або скоординовані атаки. Особливої проблеми набувають zero-day загрози, внутрішні атаки та сценарії з повільним розвитком, які залишаються непоміченими в межах сигнатурного або rule-based аналізу.

Застосування методів штучного інтелекту відкриває нові можливості для інтелектуалізації процесів оцінки кібербезпеки. Алгоритми машинного навчання дозволяють здійснювати поведінковий аналіз користувачів і мережевих об'єктів, виявляти аномальні патерни та формувати адаптивні профілі нормальної активності. Методи глибокого навчання, зокрема рекурентні нейронні мережі та трансформерні архітектури, забезпечують аналіз часових залежностей і прихованих кореляцій між подіями, що є критично важливим для ідентифікації групових і скоординованих атак [2].

У працях [1,2] обґрунтовано доцільність використання гібридних підходів, які поєднують класичні засоби моніторингу з інтелектуальними методами аналізу та прогнозування. Така інтеграція дозволяє зменшити кількість хибнопозитивних спрацювань, підвищити стійкість до zero-day атак і забезпечити більш об'єктивну оцінку реального стану кібербезпеки корпоративних мереж.

На рисунку 1 наведено узагальнену схему оцінки стану кібербезпеки корпоративних мереж, у межах якої поєднано модулі збору даних, інтелектуального аналізу, прогнозування кіберінцидентів і підтримки управлінських рішень. Такий підхід дозволяє реалізувати безперервний моніторинг рівня захищеності та адаптацію механізмів захисту до змін у загрозовому середовищі.

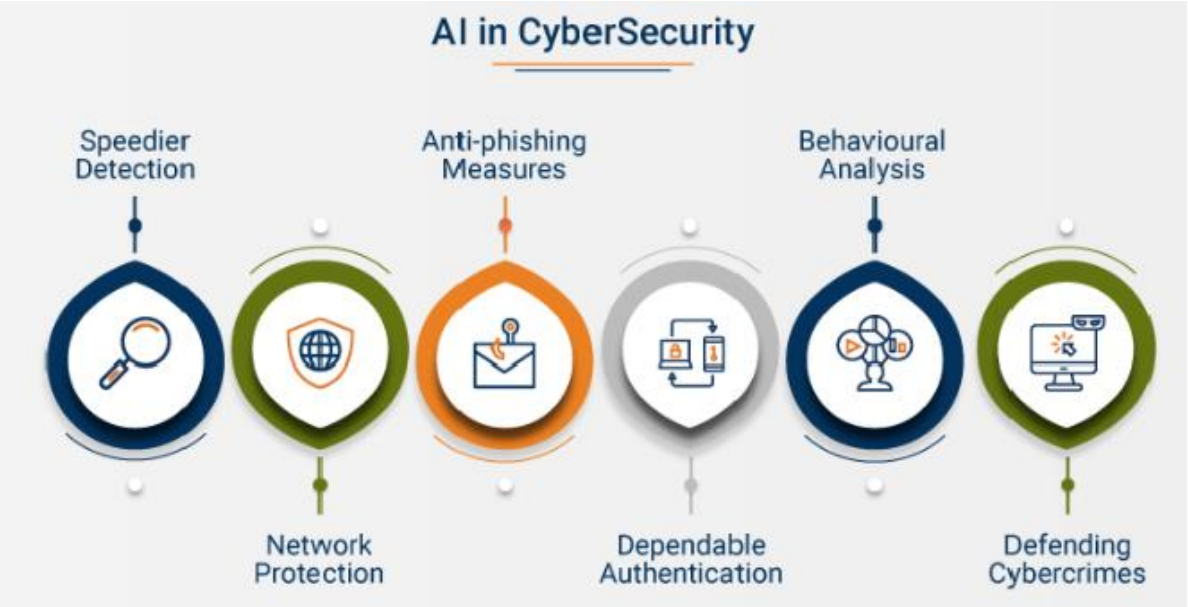

Рис. 1. Узагальнена схема оцінки стану кібербезпеки корпоративних мереж на основі ШІ

Висновки. Оцінка стану кібербезпеки корпоративних мереж в умовах цифрової трансформації потребує переходу від фрагментарних і реактивних методів до інтелектуальних, адаптивних підходів, заснованих на аналізі та прогнозуванні кіберінцидентів. Застосування штучного інтелекту дозволяє не лише підвищити точність виявлення загроз, а й сформувати динамічну модель оцінки рівня кібербезпеки з урахуванням контексту, взаємозв'язків подій і потенційних сценаріїв розвитку атак. Результати дослідження підтверджують перспективність використання інтелектуальних систем як основи для побудови сучасних механізмів управління кібербезпекою корпоративних мереж.

Література

1. Шульга В.П., Іванченко Є.В., Берестяна Т.В., Роженко А.С. Аналіз існуючих методів, моделей, систем та інструментів, що використовуються для оцінки інформаційної безпеки в корпоративному середовищі з урахуванням специфічних загроз. Сучасний захист інформації. – 2025. – № 4(64). ISSN 2409-7292. DOI: 10.31673/2409-7292.2025.041201. URL: https://journals.dut.edu.ua/index.php/dataprotect/issue/view/206

2. Шульга В.П., Іванченко Є.В., Берестяна Т.В., Шкурченко О.А. Методи та моделі протидії груповим кіберзагрозам на основі штучного інтелекту. Кібербезпека: освіта, наука, техніка. – 2025. – № 2(30). ISSN 2663-4023. DOI: 10.28925/2663-4023.2025.30.998. URL:
https://csecurity.kubg.edu.ua/index.php/journal/article/view/998

3. ENISA. AI Threat Landscape: Artificial Intelligence in Cybersecurity. European Union Agency for Cybersecurity, 2020.

4. Buczak A.L., Guven E. A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 2016.

5. Sommer R., Paxson V. Outside the closed world: On using machine learning for network intrusion detection. IEEE Symposium on Security and Privacy, 2010.

СИСТЕМА ПІДТРИМКИ ВИБОРУ OSINT-ІНСТРУМЕНТІВ ДЛЯ ВИРІШЕННЯ ЗАВДАНЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Лозова І. Л., канд. техн. наук,

Клопова А. А.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

OSINT-інструменти – це універсальні рішення, які допомагають різним спеціалістам ефективно збирати та аналізувати інформацію з відкритих джерел. Незалежно від того, чи займаєтеся ви бізнесом, працюєте у сфері кібербезпеки або проводите аналітичні дослідження, використання таких інструментів дозволяє значно спростити та прискорити процес пошуку даних [1].

Фахівці з інформаційної безпеки активно застосовують OSINT-технології для виявлення потенційних загроз і управління цифровими ризиками. Наприклад,

якщо хтось планує атаку на компанію, він може залишити сліди на тематичних форумах, у соцмережах або даркнеті. OSINT-інструменти дозволяють виявити такі сигнали на ранній стадії, що допомагає запобігти кібератакам та витокам даних. Крім того, за їхньою допомогою можна відстежувати, чи не з'явилися конфіденційні відомості організації у відкритому доступі [1].

В умовах повномасштабної війни проти України роль OSINT значно зросла як у державному секторі, так і в діяльності приватних компаній, критичної інфраструктури та медіа. Відкриті джерела стали ключовим інструментом для оперативного виявлення інформаційно-психологічних операцій, фіксації воєнних злочинів, аналізу кібератак і пошуку витоків персональних та корпоративних даних [3].

Активне використання соціальних мереж, месенджерів та даркнет-форумів створює нові вектори загроз, що потребують швидкого та обґрунтованого вибору інструментів збору й аналізу інформації.

Серед найбільш ефективних сучасних інструментів використовуються платформи автоматизованого аналізу соціальних мереж, зокрема Maltego, що дозволяє будувати графові зв'язки між суб'єктами, та SpiderFoot, який забезпечує автоматичний збір даних із десятків відкритих джерел.

Для моніторингу витоків облікових даних і зламаних ресурсів застосовується Intelligence X, що індексує архіви витоків і даркнет-контент. Геопросторовий аналіз і верифікація фото та відеоматеріалів здійснюються за допомогою Google Earth у поєднанні з аналізом метаданих та супутникових знімків [2].

Новітні OSINT-рішення інтегрують елементи машинного навчання для автоматичного класифікування контенту, виявлення бот-мереж, визначення координованої неавтентичної поведінки та прогнозування інформаційних атак. Особливо актуальним для України є моніторинг Telegram як основного каналу розповсюдження оперативної інформації та дезінформації; сучасні інструменти дозволяють здійснювати парсинг великих масивів повідомлень, аналізувати тональність, частоту публікацій і мережеві взаємозв'язки каналів [3].

Проблемою залишається фрагментарність інструментів, складність їх налаштування та відсутність єдиного підходу до вибору залежно від типу завдання.

Метою роботи є розроблення концепції системи підтримки вибору OSINT-інструментів для вирішення завдань інформаційної безпеки, яка забезпечить структуроване зіставлення типів інцидентів із функціональними можливостями відповідних інструментів та оптимізацію процесу аналітичної діяльності.

Запропонована система підтримки вибору повинна базуватися на моделі класифікації інцидентів (кіберінцидент, інформаційна операція, витік даних, перевірка контрагента, аналіз доменної інфраструктури тощо) та зіставленні їх із функціональними характеристиками інструментів (джерела даних, рівень автоматизації, підтримка API, наявність візуалізації, можливість інтеграції з SIEM). Реалізація такої системи дозволить зменшити час реагування, підвищити точність аналітики та мінімізувати людський фактор при обробці великих масивів відкритих даних.

Отже, систематизація та інтелектуалізація процесу вибору OSINT-інструментів є актуальним завданням для підвищення ефективності інформаційної безпеки українських організацій в умовах воєнних та кібернетичних загроз. Створення системи підтримки прийняття рішень у цій сфері сприятиме підвищенню оперативності реагування, узгодженості аналітичних процесів і якості управління ризиками. Перспективним напрямом є створення гібридної архітектури, що поєднує класичні OSINT-засоби з алгоритмами штучного інтелекту та автоматизованим формуванням аналітичних звітів для підрозділів інформаційної безпеки українських організацій.

Література

1. Softlist.com.ua. OSINT-інструменти 2025: топ 10 рішень для збору і аналізу даних. 2025. URL: https://softlist.com.ua/ua/news/osint-instrumenty-2025-top-10-resheniy-dlya-sbora-i-analiza-dannyh (Дата звернення: 24.02.2026).

2. Bellingcat. Online Investigation Toolkit. 2024. URL: https://www.bellingcat.com/resources/2024/09/24/bellingcat-online-investigations-toolkit/?utm_source=chatgpt.com (Дата звернення: 24.02.2026).

3. NATO Strategic Communications Centre of Excellence. Social Media as a Tool of Hybrid Warfare. Riga, 2023. URL: https://www.stratcomcoe.org/social-media-tool-hybrid-warfare (Дата звернення: 24.02.2026).

МЕТОДИ УПРАВЛІННЯ БЕЗПЕКОЮ ВІДДАЛЕНОГО ДОСТУПУ ДО КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Комірний В. В.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

Стрімкий розвиток технологій віддаленої роботи та хмарних сервісів, значні ризики при локальному зберіганні корпоративних даних,особливо в умовах війни, а також нестабільність енергопостачання зумовили значне зростання кількості корпоративних інформаційних систем. Це породжує нові виклики у сфері інформаційної безпеки: загрози несанкціонованого доступу, атаки типу MitM, витік конфіденційних даних та компрометація облікових записів. Людський фактор і слабкі місця в архітектурі доступу залишаються основними векторами атак, тому актуальність теми визначається необхідністю розробки комплексних підходів до управління безпекою віддаленого доступу, здатних ефективно протидіяти сучасним кіберзагрозам.

Об'єкти та суб'єкти захисту

Об'єктами захисту у системах віддаленого доступу виступають серверна інфраструктура, корпоративні застосунки та API, мобільні та IoT-пристрої, хмарні ресурси та мережевий трафік між клієнтом і сервером. В той час суб'єктами доступу є ієрархічна структура, в яку входять:

- рядові співробітники що підключаються через VPN-клієнти або веб-браузери з корпоративних та особистих пристроїв;
- адміністратори, що мають розширені права доступу до критичної інфраструктури;
- привілейовані користувачі – такі як головні директори, керівники, засновники, що мають доступ до критичної інформації підприємств.

Ризики та вразливості

Аналіз загроз доцільно проводити відповідно до моделі OSI, що дозволяє систематизувати вразливості за рівнями мережевої взаємодії.

На фізичному рівні – L1 та канальному рівні – L2 актуальними є загрози перехоплення трафіку через підключення до незахищених Wi-Fi мереж, ARP-спуфінг для перенаправлення пакетів, а також MAC-флудинг для виведення комутатора в режим hub.

На мережевому рівні – L3 реалізуються атаки IP-спуфінгу, ICMP-флудинг та DNS-спуфінг, що дозволяє зловмиснику перенаправляти трафік на підконтрольні ресурси. Тут же виникають ризики некоректної маршрутизації при неправильно налаштованих ACL.

На транспортному рівні – L4 присутні загрози TCP SYN-флудингу та сесійного перехоплення, що стає можливим при слабкому генеруванні початкових порядкових номерів.

На сеансовому – L5 та представницькому рівнях – L6 реалізуються атаки на протоколи TLS/SSL: BEAST, POODLE, Heartbleed, які спрямовані на розшифрування захищеного каналу або отримання витоку пам'яті сервера. Незахищені конфігурації RDP, SSH та Telnet також належать до цього діапазону загроз.

На прикладному рівні – L7 зосереджена найбільша кількість загроз: атаки типу Man-in-the-Middle з підміною сертифікатів, брутфорс та credential stuffing облікових записів, фішинг із перехопленням сесійних токенів, Pass-the-Hash та Pass-the-Ticket атаки на протокол Kerberos у середовищах Active Directory.

Окремо виділяються загрози рівня авторизації – надлишкові привілеї, горизонтальне переміщення зловмисника у мережі після первинної компрометації, а також атаки на токени OAuth 2.0 та JWT, зокрема підробка підпису та крадіжка refresh-токенів. На цьому ж рівні фіксуються загрози компрометації кінцевої точки через шкідливе ПО, кейлогери та несанкціонований доступ до збережених облікових даних браузера.

Стек технологій та методів захисту

Побудова захисту систем віддаленого доступу здійснюється на різних рівнях моделі OSI із застосуванням відповідних технологій:

Таблиця 1

Застосовані технології захисту відповідно до рівня моделі OSI

Рівень за моделлю OSI	**Технологія захисту**
L1	Фізичне розміщення серверного обладнання та кабельної інфраструктури у захищених приміщеннях з обмеженим доступом, використання екранованої витої пари та оптоволоконних ліній. Застосування систем відеоспостереження, контролю фізичного доступу
L2	Захист бездротових мереж WPA3 та сегментація трафіку через VLAN
L3	Протокол IPsec в режимах Transport та Tunnel із використанням IKEv2, для встановлення захищеного каналу та взаємної автентифікації сторін; тут також застосовуються firewall, IPS/IDS
L4	Фільтрація на основі портів та станів з'єднань через stateful firewall
L5	Управління сесіями – протокол SSL/TLS для взаємної автентифікації сторін перед початком обміну даними, механізми тайм-ауту сесій та їх примусового завершення при бездіяльності
L6	Шифрування трафіку через протоколи TLS 1.3, OpenVPN та WireGuard, які формують захищені тунелі між клієнтом і корпоративною інфраструктурою
L7	SSL/TLS VPN, протоколи федеративної ідентифікації SAML 2.0, OAuth 2.0 та OpenID Connect, а також засоби фільтрації HTTP/HTTPS трафіку через CASB та проксі-сервери

Щодо методів захисту віддаленого доступу в корпоративному середовищі, кожен з них спрямований на усунення конкретної категорії загроз. Виділяють наступні:

- Zero Trust Network Access – побудований на ідеї що жоден користувач або пристрій не є довіреним за замовчуванням, навіть перебуваючи всередині

корпоративної мережі. Використовується для безперервної верифікації кожного запиту на доступ до ресурсу.

- Software-Defined Perimeter – заснований на принципі «спочатку автентифікація, потім підключення». Використовується для приховування мережевої інфраструктури від неавторизованих користувачів до завершення перевірки особи.
- Багатофакторна автентифікація MFA – побудована на ідеї що компрометація одного фактору автентифікації не є достатньою для отримання доступу. Використовується для захисту облікових записів від брутфорсу, фішингу та credential stuffing.
- Управління привілейованим доступом PAM – заснований на принципі найменших привілеїв. Використовується для обмеження прав адміністраторів та сервісних облікових записів з метою унеможливлення lateral movement після компрометації.
- Рольова модель доступу RBAC – побудована на ідеї надання доступу не конкретній особі, а ролі або набору атрибутів. Використовується для централізованого управління правами доступу до корпоративних ресурсів.
- Управління мобільними пристроями MDM/MAM – побудоване на ідеї поширення корпоративних політик безпеки на пристрої поза периметром організації. Використовується в BYOD-середовищах для примусового шифрування, контролю застосунків та дистанційного видалення даних.
- Перевірка стану пристрою – заснована на ідеї що доступ до корпоративних ресурсів має надаватись лише пристроям, які відповідають встановленим вимогам безпеки. Використовується як обов'язковий критерій у ZTNA та BYOD-політиках перед наданням доступу.
- Моніторинг та поведінкова аналітика SIEM/UEBA – побудований на ідеї що аномальна поведінка користувача є індикатором компрометації. Використовується для виявлення підозрілої активності у реальному часі шляхом порівняння з базовим профілем поведінки.

- Endpoint Detection and Response – заснований на ідеї що кінцева точка є найбільш вразливою ланкою ланцюга доступу. Використовується для виявлення, розслідування та нейтралізації загроз безпосередньо на пристрої користувача.

Висновок. Проведений аналіз засвідчує, що забезпечення безпеки віддаленого доступу до корпоративних інформаційних систем є багаторівневою задачею, яка не може бути вирішена застосуванням єдиного технічного засобу. Систематизація загроз відповідно до моделі OSI демонструє, що вектори атак охоплюють усі рівні мережевої взаємодії — від фізичної інфраструктури до прикладного рівня, що зумовлює необхідність побудови захисту на кожному з них. Аналіз суб'єктів та об'єктів доступу підтверджує, що найбільш критичними точками компрометації є привілейовані облікові записи та некеровані кінцеві пристрої користувачів. Дослідження методів захисту свідчить про те, що перехід від периметрової моделі безпеки до концепції Zero Trust є обґрунтованою відповіддю на сучасні загрози, оскільки усуває фундаментальне припущення про довіреність внутрішньої мережі. Практична цінність роботи полягає у формуванні комплексної моделі захисту, що інтегрує технологічні рішення на рівні мережі, ідентифікації та кінцевої точки, і може бути застосована при проектуванні або аудиті систем віддаленого доступу в корпоративному середовищі.

Література

1. Souppaya M., Scarfone K. Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security. *NIST Special Publication 800-46 Rev. 2*. National Institute of Standards and Technology, 2016. URL: https://doi.org/10.6028/NIST.SP.800-46r2

2. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. *NIST Special Publication 800-207*. National Institute of Standards and Technology, 2020. URL: https://doi.org/10.6028/NIST.SP.800-207

3. OWASP Foundation. Threat Modeling Cheat Sheet. *OWASP Cheat Sheet Series* URL: https://cheatsheetseries.owasp.org/cheatsheets/Threat_Modeling_Cheat_Sheet.html

4. Rathnayake D. An Overview of the OSI Model and its Security Threats. *Tripwire: The State of Security*. 2021. URL: https://www.tripwire.com/state-of-security/overview-osi-model-and-its-security-threats

5. SANS Institute. Understanding Security Using the OSI Model. *SANS Reading Room*. URL:

6. https://www.sans.org/reading-room/whitepapers/protocols/understanding-security-osi-model-377

АНАЛІЗ СУЧАСНИХ ВЕКТОРІВ АТАК НА ХМАРНІ ТЕХНОЛОГІЇ В КОРПОРАТИВНОМУ СЕРЕДОВИЩІ ТА РОЗРОБКА КОМПЛЕКСНИХ ЗАСОБІВ ЗАХИСТУ

Легомінова С. В., д-р. екон. наук, професор

Лугін М. О.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

Хмарні технології вже стали фундаментальною частиною роботи українського бізнесу. Прискорення переходу компаній до AWS, Azure, Google Cloud та спеціалізованих платформ на кшталт Snowflake обумовлено відповіддю на виклики війни. Однак, за даними CERT-UA, у 2025 році кількість кіберінцидентів зросла на 37,4 % порівняно з попереднім роком, і значна їх частина спрямована саме проти корпоративних хмарних середовищ. Звіт Cloud Security Alliance (CSA) Top Threats to Cloud Computing Deep Dive 2025 чітко показує, що більшість успішних атак відбувається не через вразливості самої

інфраструктури провайдера, а через порушення моделі спільної відповідальності (Shared Responsibility Model) з боку клієнтів.

Теоретичним підгрунтям дослідження безпеки хмарних обчислень є аналіз моделей розгортання (IaaS, PaaS, SaaS, гібридні та мультихмарні середовища) та вивчення можливостей застосування стандартів NIST, ISO/IEC 27017, CSA CCM v4.1, українського законодавства у галузіі кібербезпеки.

Аналіз ключових інцидентів 2023–2025 років, де визначено найпоширеніші вектори атак на корпоративні хмари, що спонукає до розробки комплексних моделей захисту за принципами Zero Trust з урахуванням специфіки українських компаній (обмежені ресурси, віддалена робота, швидка міграція без повного аудиту безпеки), із частковою інтеграцією сучасних інструментів моніторингу та контролю безпеки (CASB, CSPM, CNAPP у провідних хмарних платформах).

Топ-загрози, визначені у CSA Deep Dive 2025, дозволяють більш конкректно спрямувати зусилля на протидію сучасним та кібератакам,. суттєво знизити ризики В таблиці 1 представлено топ-загроз хмарній безпеці.

Таблиця 1

Топ-загрози хмарній безпеці за частотою в 8 реальних інцидентах 2023–2025 рр. (з урахуванням наслідків)

Ранг за частотою	**Загроза(ТТ)**	**Кількість появ у кейсах**	**Приклади інцидентів**
1	TT2 – Identity and Access Management (IAM)	7	Snowflake UNC5537, Microsoft 2024
2	TT1 – Misconfiguration and Inadequate Change Control	5	Snowflake, Football Australia
3	TT6 – Insecure Software Development	4	CrowdStrike outage, Retool
4	TT3 – Insecure Interfaces and APIs	3	Retool & Fortress
5	TT5 – Insecure Third-Party Resources (supply chain)	2-3	Toyota, Retool

Поетапне впровадження принципів Zero Trust: обов’язкова MFA, умовний доступ, CSPM-інструменти, мережеві політики PrivateLink, регулярна

ротація ключів та DLP-моніторинг дозволить українським компаніям значно підвищити рівень захисту хмарних середовищ навіть за обмежених ресурсів.

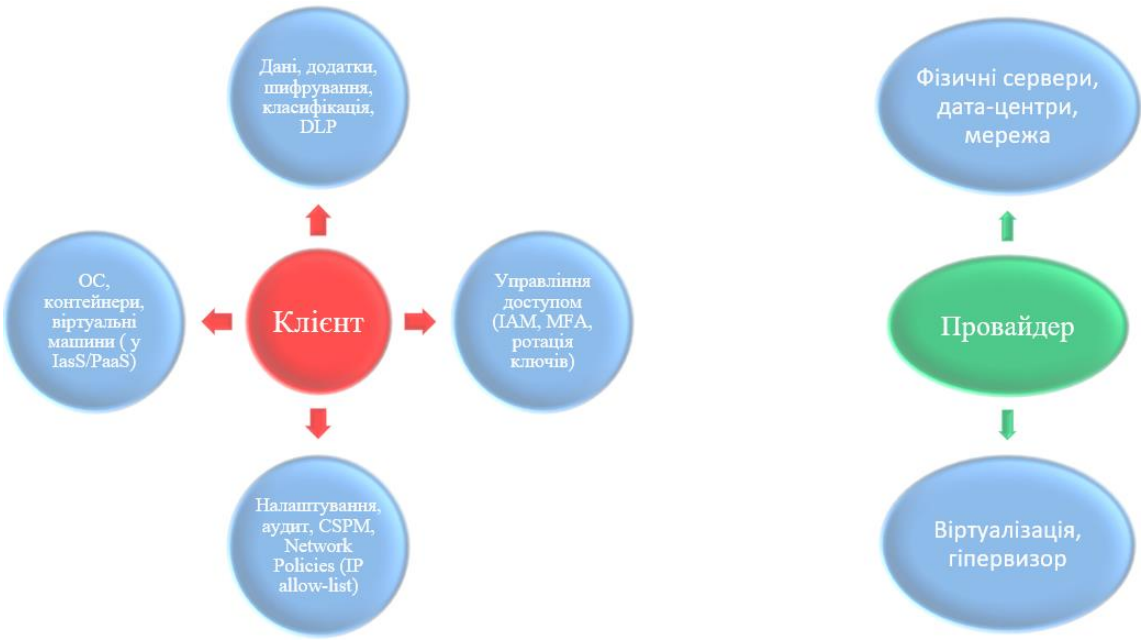

Рис. 1. Модель спільної відповідальності (Shared Responsibility Model)

Отже, аналізуючи сучасні загрози, які аналізуються у звітах відомих компаній з кібербезпеки, існує вірогідність створити модель захисту максимально прикладною, яку можна застосовувати у державному секторі, банківській сфері, рітейлі.

Література

1. Cloud Security Alliance. Top Threats to Cloud Computing – Deep Dive 2025. April 2025. URL: https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-2025

2. CERT-UA. Звіт за 2025 рік (5927 інцидентів, +37,4 %). URL: https://cip.gov.ua/ua/news/cert-ua-u-2025-roci-opracyuvala-maizhe-6000-kiberincidentiv-kilkist-vorozhikh-atak-zrosla-na-37

3. Mandiant. UNC5537 Targets Snowflake... 2024 URL: https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion

СУЧАСНІ ЗАСОБИ МЕРЕЖЕВОЇ ТА ОПЕРАЦІЙНОЇ БЕЗПЕКИ КОРПОРАТИВНОЇ ІНФРАСТРУКТУРИ

Лукашенко В. Д.
Державний університет інформаційно-комунікаційних технологій
м. Київ, Україна

В умовах стрімкої цифровізації бізнес-процесів та переходу до гібридних моделей роботи, класичний периметровий захист корпоративних мереж втрачає свою ультимативну ефективність. Сучасна парадигма кібербезпеки вимагає комплексного підходу, що поєднує засоби мережевої безпеки (Network Security), операційної безпеки (Operational/Endpoint Security) та організаційні заходи впливу. Метою даної роботи є аналіз сучасних програмно-апаратних засобів та політик, що забезпечують цілісність, конфіденційність та доступність корпоративної інфраструктури.

Засоби мережевої безпеки. Мережева безпека формує перший ешелон захисту (Defense in Depth) і відповідає за фільтрацію трафіку, захист каналів зв'язку та протидію зовнішнім атакам. Фундаментом мережевого захисту є міжмережеві екрани нового покоління (NGFW), наприклад, рішення від Checkpoint, які здійснюють не лише L3/L4 фільтрацію, але й глибоку інспекцію пакетів (DPI) на прикладному рівні моделі OSI [1, с. 45].

Для забезпечення стійкості інфраструктури критично важливим є використання спеціалізованих систем протидії DDoS-атакам (наприклад, Arbor Networks), які аналізують аномалії трафіку та здійснюють його очищення (scrubbing).

Окремим, але вкрай важливим вектором мережевої безпеки є захист бездротових мереж (Wi-Fi). Специфіка радіоканалу унеможливлює фізичний контроль доступу до середовища передачі. Поширена практика приховування ідентифікатора мережі (SSID) не забезпечує реального захисту, оскільки аналізатори трафіку легко перехоплюють MAC-адреси та параметри

підключення під час легітимних сесій. Тому надійним підходом є використання сучасних стандартів шифрування (WPA3) у поєднанні з корпоративною аутентифікацією за стандартом 802.1X, що гарантує підключення лише авторизованих пристроїв.

Безпека передачі даних та адміністрування забезпечується шляхом використання VPN з надійними алгоритмами шифрування (IPsec, OpenVPN), доступу через протокол SSH версії 2 та відмови від застарілих протоколів, що передають дані у відкритому вигляді (заміна TFTP на SFTP або SCP) [2].

Операційна безпека, людський фактор та комунікації. Операційна безпека охоплює процеси управління доступом, захисту електронної пошти та моніторингу кінцевих пристроїв (Endpoint Protection). Оскільки електронна пошта залишається головним вектором поширення фішингу та шкідливого ПЗ, впровадження спеціалізованих шлюзів безпеки (наприклад, FortiMail) є обов'язковим для фільтрації спаму, антивірусного захисту та запобігання витоку даних (DLP). На рівні робочих станцій базовими вимогами є встановлення EDR-систем, а також суворий контроль за регулярним оновленням ОС та прикладного ПЗ.

Відповідно, операційна безпека розширюється і на мобільні пристрої співробітників через впровадження систем MDM/UEM (Mobile Device Management) та Mobile Endpoint Protection, що дозволяє дистанційно блокувати пристрій при втраті, шифрувати корпоративний контейнер даних та контролювати цілісність мобільної ОС.

Проте одним із найслабших місць будь-якої інфраструктури залишається людський фактор та компрометація облікових даних. Зловмисники часто обходять складні технічні системи завдяки методам соціальної інженерії. Саме тому критично важливо регулярно проводити тренінги з кібергігієни (Security Awareness) для персоналу, а також впроваджувати чіткі, зрозумілі для звичайних співробітників політики та покрокові інструкції з інформаційної безпеки.

Для математичної оцінки стійкості парольних політик до атак типу Brute Force використовується розрахунок інформаційної ентропії пароля за формулою Шеннона:

$$H = L \cdot log_2(N), \quad (1)$$

де H – ентропія пароля (в бітах); L – довжина пароля (кількість символів); N – потужність алфавіту (кількість можливих символів, що використовуються).

Для нівелювання ризиків, пов'язаних із низькою ентропією паролів та людськими помилками, обов'язковим є впровадження багатофакторної аутентифікації (MFA).

Централізація моніторингу та управління доступом. Для забезпечення безперервної роботи (High Availability) та прозорості подій безпеки критично важливим є розгортання систем комплексного моніторингу. Для контролю стану мережевого обладнання, серверів та доступності сервісів стандартом є використання систем моніторингу інфраструктури, таких як Zabbix. Водночас для агрегації логів з NGFW, VPN, поштових шлюзів та кінцевих точок впроваджуються системи класу SIEM (Security Information and Event Management) [3, с. 112]. Синергія Zabbix (моніторинг працездатності та навантаження) та SIEM (кореляція інцидентів безпеки) дозволяє оперативно виявляти як технічні збої, так і складні вектори атак у режимі реального часу.

Сучасним трендом управління є використання систем привілейованого доступу (PAM). Інноваційним рішенням у цій сфері є продукти класу Excalibur, що реалізують підхід Passwordless аутентифікації, перетворюючи смартфон користувача на апаратний токен і унеможливлюючи перехоплення паролів.

Таблиця 1

Класифікація засобів захисту корпоративної інфраструктури

Рівень	Основні завдання	Типові рішення, технології та заходи
Мережевий (Network)	Фільтрація трафіку, протидія DDoS, захист Wi-Fi	Checkpoint NGFW, Arbor, VPN, 802.1X/WPA3
Операційний (Operational)	Захист хостів/мобільних пристроїв, фільтрація пошти	FortiMail, EDR, MDM, MFA
Управлінський (Management)	Кореляція подій, моніторинг інфраструктури, контроль сесій	SIEM, Zabbix, PAM (Excalibur)
Організаційний (Human)	Підвищення обізнаності, регламентація дій	Тренінги Security Awareness, політики, інструкції

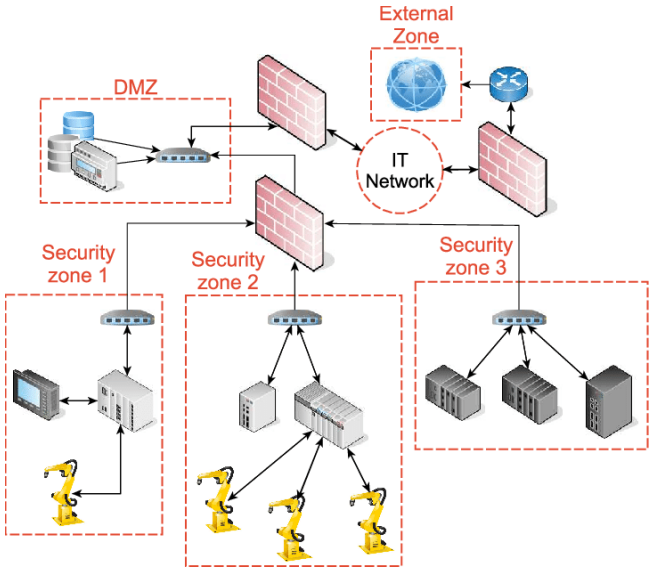

Рис. 1. Схема інтеграції засобів мережевої та операційної безпеки в корпоративну інфраструктуру

Висновки. Отже, ефективний захист корпоративної інфраструктури неможливий без інтеграції мережевих, операційних та організаційних заходів. Впровадження рішень периметрового захисту (NGFW, Anti-DDoS, 802.1X) у поєднанні із суворим контролем корпоративних та мобільних пристроїв (EDR, MDM), захистом комунікацій (FortiMail) та сучасним контролем доступу (PAM-системи типу Excalibur) формує міцний технологічний фундамент. Водночас для підтримання життєздатності цієї системи абсолютно необхідним є безперервний моніторинг інфраструктури та подій безпеки (Zabbix, SIEM), а

також регулярне навчання персоналу і впровадження зрозумілих інструкцій для мінімізації ризиків, пов'язаних із людським фактором.

Література

1. Stallings, W. (2020). *Cryptography and Network Security: Principles and Practice* (8th ed.). Pearson.

2. Національний інститут стандартів і технологій США (NIST). (2021). *NIST Special Publication 800-46 Rev. 2. Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security*.

3. Бурячок, В. Л., Толюпа, С. В., & Семченко, В. О. (2018). *Інформаційна та кібербезпека: соціотехнічний аспект*. Київ: ДУТ.

4. Orebaugh, A., Ramirez, G., & Beale, J. (2022). *Wi-Fi Security and Enterprise Email Protection Strategies*. Syngress.

АНАЛІЗ ТА ВИЯВЛЕННЯ АНОМАЛІЙ У МЕРЕЖЕВОМУ ТРАФІКУ ЯК ІНСТРУМЕНТ ПРОТИДІЇ КІБЕРЗАГРОЗАМ

Марченко М. В.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

В умовах стрімкої цифровізації економіки кіберзагрози набувають дедалі більшої складності та масштабності. За даними звіту IBM Cost of a Data Breach 2025, середня вартість витоку даних у світі сягнула 4,45 млн доларів США — найвищого показника за всю історію досліджень [1]. Одним із ключових векторів атак залишається мережева інфраструктура підприємств, тому виявлення аномалій у мережевому трафіку є критично важливою складовою системи кіберзахисту.

Мережевий трафік як джерело даних. Мережевий трафік є безперервним потоком даних, що містить інформацію про поведінку користувачів, застосунків та пристроїв. Аномалією вважається відхилення від встановленого нормального профілю поведінки, яке може свідчити про несанкціоновану активність або атаку. Виявлення аномалій (anomaly detection) поділяють на три основні парадигми:

- точкові аномалії — окремі спостереження, що різко відрізняються від норми (наприклад, аномальний обсяг трафіку до одного хосту);
- контекстуальні аномалії — відхилення, характерні лише у певному контексті (нічний трафік у бізнес-мережі);
- колективні аномалії — набір спостережень, що разом формують підозрілий патерн (розподілена атака DDoS).

Методи виявлення аномалій. Сучасні системи виявлення вторгнень (IDS) використовують різні підходи до аналізу трафіку [3]. Порівняльну характеристику основних методів представлено у таблиці 1.

Таблиця 1

Порівняльна характеристика методів виявлення аномалій у мережевому трафіку

Метод	Точність	Швидкість	Потреба у розмічених даних
Statistical (порогові)	Середня	Висока	Ні
Machine Learning (ML)	Висока	Середня	Частково
Deep Learning (DL)	Дуже висока	Низька	Так (частково)
Signature-based	Дуже висока*	Висока	Так

*лише для відомих сигнатур атак

Методи машинного навчання (ML) демонструють високу ефективність завдяки здатності виявляти раніше невідомі загрози. Серед найпоширеніших алгоритмів — Isolation Forest (ефективний для виявлення аномалій у веб-трафіку [3]), One-Class SVM, Autoencoder та LSTM для часових рядів трафіку. Для IoT-мереж особливо перспективним є поєднання Sparse Autoencoder (SAE) та CNN, що забезпечує точну бінарну класифікацію аномалій [2]. Навчання без

учителя є особливо цінним, оскільки не вимагає попереднього розмічення даних про атаки.

Ключові характеристики (ознаки), що використовуються для аналізу: тривалість сесії, кількість байт та пакетів, протокол, IP-адреси джерела та призначення, розподіл портів, частота з'єднань, флаги TCP-протоколу. Датасети CICIDS-2017 та NSL-KDD є стандартними бенчмарками для оцінювання алгоритмів виявлення аномалій.

Практична реалізація. Сучасний стек технологій для аналізу мережевого трафіку в реальному часі включає: інструменти захоплення трафіку (Zeek, Wireshark, ntopng), системи обробки потоків даних (Apache Kafka, Apache Flink), платформи машинного навчання (Python scikit-learn, TensorFlow) та засоби візуалізації (Kibana, Grafana, Power BI). Інтеграція цих компонентів дозволяє побудувати повноцінний конвеєр виявлення загроз у режимі реального часу.

Особливої уваги заслуговує підхід XAI (Explainable AI) — інтерпретовне штучне навчання, яке дозволяє пояснити рішення моделі аналітикам безпеки. Методи SHAP та LIME стають стандартом у виявленні аномалій, оскільки підвищують довіру до автоматизованих рішень і зменшують кількість хибних спрацювань.

Висновки. Аналіз та виявлення аномалій у мережевому трафіку є ефективним і перспективним інструментом протидії сучасним кіберзагрозам. Гібридні підходи, що поєднують статистичні методи, ML/DL-алгоритми та сигнатурний аналіз, забезпечують найвищу точність за прийнятного рівня хибних спрацювань [4]. Перспективами подальших досліджень є розробка адаптивних моделей, здатних навчатися в режимі реального часу та протистояти adversarial-атакам на самі системи виявлення вторгнень.

Література

1. IBM Security. (2025). Cost of a Data Breach Report 2025. IBM Corporation. https://www.ibm.com/reports/data-breach

2. Alsoufi, M. A., Siraj, M. M., Ghaleb, F. A., Al-Razgan, M., Al-Asaly, M. S., Alfakih, T., & Saeed, F. (2024). Anomaly-based intrusion detection model using deep learning for IoT networks. Computer Modeling in Engineering & Sciences, 141(1), 823–845. https://doi.org/10.32604/cmes.2024.052112

3. Chua, W., Pajas, A. L. D., Castro, C. S., Panganiban, S. P., Pasuquin, A. J., Purganan, M. J., Malupeng, R., Pingad, D. J., Orolfo, J. P., Lua, H. H., & Velasco, L. C. (2024). Web traffic anomaly detection using Isolation Forest. Informatics, 11(4), 83. https://doi.org/10.3390/informatics11040083

4. Almuhanna, R., & Dardouri, S. (2025). A deep learning/machine learning approach for anomaly based network intrusion detection. Frontiers in Artificial Intelligence, 8, 1625891. https://doi.org/10.3389/frai.2025.1625891

ФОРМАЛІЗАЦІЯ ТА ОПТИМІЗАЦІЯ МОДЕЛЕЙ УПРАВЛІННЯ ДОСТУПОМ В ІНФОРМАЦІЙНИХ СИСТЕМАХ НА ОСНОВІ КОНЦЕПЦІЇ ZERO TRUST

Примаченко Д. В.,

Григоренко В. Р.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

Інформаційні системи характеризуються високою динамічністю, розподіленістю ресурсів та інтеграцією з хмарними сервісами. Класичні периметрові підходи до забезпечення інформаційної безпеки, які передбачають наявність «довіреної внутрішньої мережі» та «недовіреного зовнішнього середовища», втрачають ефективність через зростання кількості мобільних користувачів, використання віддаленого доступу та постійні кіберзагрози. Концепція Zero Trust, запропонована John Kindervag та стандартизована National Institute of Standards and Technology у документі NIST SP 800-207,

набуває особливої актуальності як методологічна основа побудови сучасних систем управління доступом.

Zero Trust ґрунтується на фундаментальному принципі відсутності довіри за замовчуванням до будь-якого суб'єкта чи пристрою незалежно від їх розташування у мережі. Кожен запит на доступ до ресурсу розглядається як потенційно небезпечний і підлягає багаторівневій перевірці. Такий підхід передбачає безперервну автентифікацію, авторизацію та моніторинг поведінки суб'єктів доступу. Відповідно, управління доступом у межах Zero Trust повинно бути динамічним, контекстно-орієнтованим та ризик-адаптивним.

Аналіз існуючих моделей управління доступом свідчить, що рольова модель RBAC, формалізована у працях David Ferraiolo та D. Richard Kuhn, забезпечує структуроване розмежування прав доступу через ієрархію ролей, однак має обмежену гнучкість у динамічних середовищах [1]. Вона ефективна для стабільних організаційних структур, проте складно адаптується до змін контексту, поведінки користувачів або рівня ризику. Атрибутивна модель ABAC, описана у рекомендаціях National Institute of Standards and Technology (SP 800-162), дозволяє враховувати множину характеристик суб'єкта, об'єкта та середовища, що забезпечує більш тонке налаштування політик доступу. Проте ABAC вимагає формалізації складних логічних правил та ефективних механізмів обробки атрибутів у реальному часі.

У межах запропонованого дослідження розглядається інтегрована модель управління доступом, яка поєднує структурованість RBAC із гнучкістю ABAC у рамках архітектури Zero Trust. Формально модель можна представити у вигляді множин S — суб'єкти, O — об'єкти, A — дії, C — контекстні параметри, R — ролі, P — політики доступу. Функція прийняття рішення щодо доступу визначається як $D: S \times O \times A \times C \rightarrow \{allow, deny\}$. Політика доступу описується предикатною формулою, що враховує атрибути суб'єкта (ідентичність, належність до ролі, рівень довіри), характеристики об'єкта (класифікація, критичність) та параметри середовища (час, геолокація, стан пристрою, показники ризику) [2].

Ключовим елементом моделі є механізм оцінювання ризику, який інтегрується в процес авторизації. Рівень ризику Rrisk визначається як функція від поведінкових індикаторів, історії доступів, аномалій активності та стану пристрою. За умови перевищення порогового значення ризику політика автоматично модифікується шляхом обмеження або відкликання привілеїв. Таким чином реалізується принцип мінімальних привілеїв та адаптивного контролю доступу.

Важливу роль у забезпеченні Zero Trust відіграє мікросегментація ресурсів, що передбачає поділ інформаційної системи на ізольовані логічні сегменти з окремими політиками доступу. Це мінімізує горизонтальне поширення загроз у разі компрометації одного з вузлів. Додатково впроваджується багатофакторна автентифікація, яка підвищує достовірність ідентифікації суб’єкта. У сукупності ці механізми формують багаторівневу систему контролю доступу, орієнтовану на безперервну перевірку довіри.

Порівняльний аналіз показує, що класична RBAC-модель має нижчу складність реалізації, проте поступається інтегрованій Zero Trust-моделі за критеріями адаптивності, масштабованості та стійкості до інсайдерських загроз. ABAC забезпечує більш гнучке управління політиками, однак без інтеграції з механізмами оцінювання ризику не гарантує достатнього рівня захисту в умовах складних атак. Запропонована модель, що поєднує атрибутивний підхід із динамічним аналізом ризику, дозволяє мінімізувати ймовірність несанкціонованого доступу навіть у разі компрометації облікових даних, оскільки рішення про доступ приймається на основі сукупності параметрів, а не лише статичної ролі користувача.

Отже, формалізація моделей управління доступом на основі Zero Trust створює теоретичне підґрунтя для побудови адаптивних, контекстно-чутливих систем захисту інформації. Практична реалізація такої моделі сприятиме підвищенню рівня кіберстійкості організацій, зменшенню площини атаки та забезпеченню відповідності сучасним стандартам інформаційної безпеки. Подальші дослідження можуть бути спрямовані на оптимізацію алгоритмів

оцінювання ризику та використання методів машинного навчання для прогнозування аномальної поведінки суб’єктів доступу.

Література

1. Garbis J., Chapman J. W. Intrusion detection and prevention systems. Zero trust security. Berkeley, CA, 2021. P. 117–126. URL: https://doi.org/10.1007/978-1-4842-6702-8_8

2. Mankovskyi B., Dovbniak V., Opirskyy I. Research on the feasibility of implementing the zero trust concept in iot systems. Cybersecurity: education, science, technique. 2025. Vol. 1, no. 29. P. 73–91. URL: https://doi.org/10.28925/2663-4023.2025.29.864

СИСТЕМА ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ВПРОВАДЖЕНИХ ТЕХНІЧНИХ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ МЕТРИК РЕЗУЛЬТАТИВНОСТІ

Тарасенко Б. Р.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

У сучасних умовах стрімкого розвитку інформаційних технологій та зростання кількості кіберзагроз ефективність захисту інформації стає критичним фактором забезпечення конфіденційності, цілісності та доступності даних. Впровадження технічних засобів захисту інформації (ТЗЗІ), таких як міжмережеві екрани, системи виявлення та запобігання вторгнень (IDS/IPS), антивірусне програмне забезпечення, системи контролю доступу, шифрування даних та рішення класу DLP, не гарантує автоматичного досягнення цілей безпеки. Навіть найсучасніші технічні рішення вимагають постійної оцінки їх результативності, щоб своєчасно виявляти недоліки, оптимізувати витрати на

безпеку та забезпечувати відповідність вимогам як міжнародних стандартів, так і національного законодавства України.

Актуальність теми зумовлена жорсткими вимогами нормативної бази щодо моніторингу та вимірювання ефективності систем інформаційної безпеки. Міжнародні стандарти, зокрема ISO/IEC 27004:2016 [1], наголошують на необхідності переходу від якісних оцінок до кількісних показників, що дозволяє приймати обґрунтовані управлінські рішення на основі даних. Аналогічні підходи закріплені в NIST Special Publication 800-55 Volume 1 (2024)[2], де надано детальний посібник з вимірювання ефективності заходів інформаційної безпеки. В Україні ці вимоги конкретизуються в НД ТЗІ 2.3-025-24 [3], який визначає методику оцінювання заходів захисту інформації для інформаційних систем, а також у ДСТУ 3396.0-9 [4] та ДСТУ ISO/IEC 27001:2015 [5], що встановлюють основні принципи технічного захисту та управління системою інформаційної безпеки.

Метою даної роботи є формування концепції системи оцінювання ефективності впроваджених технічних засобів захисту інформації на основі метрик результативності. Для досягнення цієї мети передбачається проаналізувати основні категорії ТЗЗІ, визначити ключові метрики, описати структуру та процеси функціонування такої системи, а також сформулювати практичні рекомендації щодо її впровадження.

Технічні засоби захисту інформації класифікуються за функціональним призначенням: засоби запобігання (міжмережеві екрани, системи контролю доступу), виявлення (IDS/IPS, SIEM-системи), реагування (антивірусне ПЗ, DLP) та відновлення (резервне копіювання, шифрування). Відповідно до ДСТУ 3396.0-96, технічний захист інформації спрямований на блокування каналів витоку, запобігання несанкціонованому доступу та спеціальним видам впливу. У сучасній практиці ці засоби інтегруються в єдину систему, часто з використанням SIEM для централізованого моніторингу та аналізу. Ефективність таких комплексних рішень залежить не лише від правильного

впровадження, але й від постійної адаптації до еволюції загроз, як це підкреслюється в NIST SP 800-55v1.

Метрики результативності поділяються на дві основні групи: метрики продуктивності (performance measures), що відображають ступінь впровадження контролю (наприклад, відсоток систем з увімкненою багатофакторною аутентифікацією), та метрики ефективності (effectiveness measures), що оцінюють досягнення поставленої мети (наприклад, зниження кількості інцидентів). Згідно з ISO/IEC 27004:2016, серед ключових показників виділяються MTTD (Mean Time to Detect) – середній час виявлення загрози, MTTR (Mean Time to Respond) – середній час реагування на інцидент, а також MTTC (Mean Time to Contain) – середній час локалізації інциденту. Для конкретних ТЗЗІ прикладами можуть слугувати: для міжмережевого екрана – відсоток заблокованих несанкціонованих спроб доступу та частота оновлення правил; для IDS/IPS – кількість виявлених вторгнень та рівень хибних спрацювань; для антивірусного ПЗ – відсоток систем з актуальними сигнатурами та час усунення шкідливого ПЗ; для систем контролю доступу – відсоток облікових записів з MFA та кількість невдалих спроб; для шифрування – відсоток зашифрованих даних у спокої та частота ротації ключів. Додаткові метрики включають загальну кількість інцидентів за період, відсоток вразливостей, усунених у встановлений термін, та рівень покриття тестуванням на проникнення. У національній практиці, зокрема згідно з НД ТЗІ 2.3-025-24, оцінювання ефективності проводиться за критеріями повноти реалізації заходів, відсутності критичних вразливостей та економічної доцільності, з використанням Каталогу заходів захисту (класи AA–SR).

Система оцінювання ефективності ТЗЗІ базується на циклі PDCA (Plan-Do-Check-Act) і включає послідовні етапи: визначення інформаційних потреб з урахуванням бізнес-цілей та ризиків; розробку та валідацію метрик за принципом SMART (Specific, Measurable, Achievable, Relevant, Time-bound) з чіткою формулою, джерелом даних та цільовими значеннями; автоматизований або ручний збір даних (з логів SIEM, сканерів вразливостей, аудитів); аналіз за

допомогою статистичних методів (середнє, регресія, часові ряди) та порівняння з цільовими показниками; формування звітів, дашбордів та рекомендацій для вдосконалення. Відповідно до НД ТЗІ 2.3-025-24 , процес передбачає підготовку плану, виділення груп заходів, аналіз документації, співбесіди та тестування, з фіксацією результатів у звіті та посиланнями на докази. Оцінювання проводиться періодично (щоквартально або після значних змін) з забезпеченням незалежності оцінювача.

Практичне застосування такої системи дозволяє, наприклад, для організації з впровадженим firewall та IDS моніторити метрику «відсоток заблокованих атак» як (кількість заблокованих / загальна кількість спроб) × 100. Якщо значення падає нижче 95 %, це сигналізує про необхідність аналізу та оновлення правил, що може суттєво скоротити MTTD з кількох діб до кількох годин.

Таким чином, система оцінювання ефективності впроваджених технічних засобів захисту інформації на основі метрик результативності є потужним інструментом переходу від реактивного до проактивного управління ризиками. Вона сприяє підвищенню рівня захищеності, оптимізації ресурсів, зменшенню фінансових втрат від інцидентів та забезпеченню відповідності вимогам ДСТУ ISO/IEC 27001, ISO/IEC 27004, NIST SP 800-55 та національних нормативних документів. Перспективним напрямком розвитку є інтеграція з автоматизованими платформами на базі штучного інтелекту для аналізу метрик у реальному часі.

Література

1. ISO/IEC 27004:2016 Information technology — Security techniques — Information security management—Monitoring, measurement, analysis and evaluation
URL:https://cdn.standards.iteh.ai/samples/64120/53f9a1b766474aaf8c26c4aaccd91356/ISO-IEC-27004-2016.pdf

2. NIST Special Publication 800-55 Volume 1: Measurement Guide for Information Security(2024)URL:https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-55v1.pdf

3. НД ТЗІ 2.3-025-24 Методика оцінювання заходів захисту інформації… (Держспецзв'язку України) URL:https://cip.gov.ua/services/cm/api/attachment/download?id=66113

4. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення URL:https://tzi.com.ua/downloads/DSTU%203396.0-96.pdf

5. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги URL: https://www.assistem.kiev.ua/doc/dstu_ISO-IEC_27001_2015.pdf

6. SecurityScorecard. 20 Cybersecurity Metrics & KPIs to Track in 2025 (2024) URL: https://securityscorecard.com/blog/9-cybersecurity-metrics-kpis-to-track

ЗАСОБИ МЕРЕЖЕВОЇ ТА ОПЕРАЦІЙНОЇ БЕЗПЕКИ: CORTEX XDR ЯК КОМПЛЕКСНА ПЛАТФОРМА ВИЯВЛЕННЯ ТА РЕАГУВАННЯ

Грущинський Ю. Ю.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

Сучасні кібератаки дедалі частіше мають характер більш комплексний, маючи декілька стадій ланцюга ураження, поєднують компрометацію кінцевих точок, викрадення облікових даних, горизонтальне переміщення в мережі та встановлення каналів керування. За таких умов інструменти, що обмежуються лише одним рівнем спостереження (виключно мережевим або виключно рівнем кінцевих точок), підвищують навантаження на аналітика: для відновлення

«ланцюга атаки» необхідні ручні переходи між консолями, розрізнені запити до журналів і повторювана кореляція подій, що збільшує час реакції та ризик пропуску подій низької критичності [2, с. 3–5]. Додатковим чинником є кадровий тиск на центри моніторингу безпеки: у матеріалах ISC2 (попередній огляд дослідження 2024 року) підкреслено масштабність дефіциту фахівців і вплив обмежень бюджету на здатність організацій розвивати необхідні навички та процеси реагування [12]. У сукупності це формує запит на засоби, що одночасно розширюють видимість та зменшують «ручну» складову виявлення й реагування.

У настанові NIST SP 800-61 Rev. 3 реагування на інциденти розглядається як складова управління кіберризиками та інтегрована діяльність, що має підвищувати ефективність і результативність виявлення, реагування та відновлення [7]. Отже, технологічне рішення, придатне для мережевої й операційної площини, має поєднувати технічні механізми контролю/блокування з операційними механізмами кореляції, пріоритезації та керованого виконання дій реагування.

Cortex XDR описується як платформа, що корелює події безпеки в інцидент-орієнтовану модель розслідування та реагування, зменшуючи витрати ресурсу на аналіз подій [1, с. 3–4]. На рівні кінцевих точок агент Cortex XDR збирає детальну телеметрію поведінки (зокрема ланцюги виконання процесів, командні рядки, події файлової системи/реєстру тощо) та підтримує дії запобігання і реагування, що є критичним для виявлення безфайлових технік і зловживання легітимними утилітами ОС [1, с. 11–12]. Паралельно офіційні матеріали вказують, що рішення не обмежується даними з кінцевих точок, а орієнтоване на багатоджерельну кореляцію в межах «єдиного аналітичного поля» [3; 4].

Функціонально Cortex XDR можна описати за трьома групами:

1) Захист кінцевих точок у Cortex XDR реалізується через єдиний агент, що поєднує EPP/NGAV та EDR: багаторівнева превенція (блокування експлойтів, шкідливого ПЗ та програм-вимагачів до виконання), захист пам'яті процесів, поведінковий аналіз у реальному часі; залежно від модулів —

локальний брандмауер, контроль пристроїв, шифрування дисків. Агент збирає високодеталізовану телеметрію. Аналітична підсистема базується на єдиному Data Lake, куди надходять дані з кінцевих точок, мережі, хмари та систем ідентифікації; тисячі ШІ-детекторів виявляють аномалії у реальному часі, а Causality Analysis Engine (CAE) автоматично встановлює причинно-наслідкові зв'язки між подіями, формуючи повний ланцюг атаки.

2) Операційна ефективність SOC забезпечується через інцидент-орієнтований підхід: усі пов'язані події автоматично групуються в єдиний інцидент із присвоєнням оцінки ризику для пріоритезації; аналітики отримують інструменти проактивного полювання на загрози через мову запитів XQL, вбудовані плейбуки автоматизації реагування, швидкі дії (ізоляція хоста, завершення процесу, видалення файлу) та інтеграцію з XSOAR для оркестрації складних сценаріїв. Управління поверхнею атаки реалізується через інтеграцію з Xpanse для виявлення неінвентаризованих активів; збагачення даних про загрози забезпечується через Unit 42 Threat Intelligence з автоматичним оновленням превентивних механізмів на основі актуальних індикаторів.

3) Мережева безпека в Cortex XDR реалізується переважно через нативну інтеграцію з екосистемою PAN-OS: аналітик може безпосередньо з консолі додавати індикатори компрометації до External Dynamic Lists (EDL) для негайного блокування на рівні мережі — скорочуючи шлях від виявлення до блокування до мінімуму. Водночас EDL є виключно нативним механізмом PAN-OS, і пряма інтеграція зі сторонніми рішеннями не підтримується; у гетерогенних середовищах аналогічний контур блокування потребує альтернативних шляхів — зокрема через SOAR-механізми. Єдина консоль охоплює Windows, macOS, Linux, Android та iOS, забезпечуючи уніфікований захист усього парку пристроїв організації.

З позиції операційної безпеки, ключова вимога — скорочення часу від виявлення до стримування за збереження керованості та аудиту. NIST SP 800-61 Rev. 3 підкреслює інтеграцію реагування на інциденти в управління кіберризиками та необхідність підвищувати ефективність заходів виявлення,

реагування та відновлення [7]. Для цього важлива автоматизація повторюваних процедур. У матеріалах Cortex XDR (Cornerstone) вказуються можливості автоматизації та оркестрації [1, с. 37–38]. Palo Alto Networks також наголошує на готовому контенті, який покликаний забезпечити «покриття від першого дня» та зменшити навантаження на SOC [6]. З точки зору академічної свідомості, важливо підкреслити: такі твердження є частиною позиціонування постачальника й потребують валідації в конкретному середовищі, оскільки ці твердження є частиною маркетингової стратегії.

Оцінювання ефективності XDR-рішень доцільно розглядати через призму публічних програм. Однією з таких програм є MITRE ATT&CK Evaluations, особисто наголошую на незалежності та об'єктивності підходу цієї програми, а також на тому, що оцінювання не призначене для «ранжування» вендорів, а має допомогти організаціям зробити висновки щодо відповідності їхнім потребам [9]. В рамках випробувань, Palo Alto Networks має високі результати. Cortex XDR у MITRE ATT&CK Enterprise Evaluations 2024 демонструє 100% виявлень на рівні технік без змін конфігурації чи затримок [10].

Cortex XDR демонструє тенденцію злиття мережевої та операційної безпеки у межах єдиного циклу обробки інцидентів. Платформа поєднує деталізовану телеметрію з кінцевих точок та механізми реагування з можливістю мережевих маніпуляцій через PAN-OS (зокрема EDL-механізми), що потенційно зменшує затрати на розслідування і пришвидшує стійкість до багатостадійних атак [1, с. 12–13; 8; 11]. Водночас інтеграційні обмеження (наприклад, відсутність еквівалентної підтримки EDL від сторонніх розробників) та необхідність управлінського підходу до автоматизації мають бути відображені в проєктуванні впровадження [5; 7].

Література

1. Palo Alto Networks. Cortex XDR Cornerstone: *Technical Depth of the Demo*. 2025. 45 с.

2. Palo Alto Networks. *The Essential Guide to XDR*. 2022. 25 с.

3. Palo Alto Networks. Cortex XDR *At-A-Glance*. URL: https://www.paloaltonetworks.com/resources/whitepapers/cortex-xdr-at-a-glance

4. Palo Alto Networks. Cortex XDR URL: https://www.paloaltonetworks.com/cortex/cortex-xdr.

5. Palo Alto Networks LIVEcommunity. *Can I integrate EDL into Cortex XDR with other firewall brands?* URL: https://live.paloaltonetworks.com/t5/cortex-xdr-discussions/can-i-integrate-edl-into-cortex-xdr-with-other-firewall-brands/td-p/573071.

6. Palo Alto Networks. *SIEM Replacement Made Easy (Yes, Really!)* URL: https://www.paloaltonetworks.com/blog/security-operations/siem-replacement-made-easy-yes-really/

7. NIST. SP 800-61 Rev. 3*: Incident Response Recommendations and Considerations for Cybersecurity Risk Management*: A CSF 2.0 Community Profile. 2025.

8. Palo Alto Networks. Cortex XDR 2.4: *One Small Step for Cortex XDR, One Giant Leap for SecOps URL*: https://www.paloaltonetworks.com/blog/2020/06/cortex-xdr-2-4/

9. MITRE. *New Round of MITRE Engenuity's ATT&CK Evaluations Calls for Participation for Enterprise Cybersecurity Solutions*. URL: https://www.mitre.org/news-insights/news-release/new-round-mitre-engenuitys-attack-evaluations-calls-participation

10. Palo Alto Networks. *Cortex XDR Delivers Unmatched 100% Detection in MITRE Evals 202*4. URL: https://www.paloaltonetworks.com/blog/2024/12/historic-results-in-the-2024-mitre-attck-enterprise-evaluations/

11. Palo Alto Networks TechDocs (PAN-OS). *Policy Object: External Dynamic Lists*

12. ISC2. *Growth of Cybersecurity Workforce Slows in 2024 as Economic Uncertainty Persists (First Look)*. URL: https://www.isc2.org/Insights/2024/09/ISC2-Publishes-2024-Cybersecurity-Workforce-Study-First-Look

РОЗРОБКА ТА ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ КОМПЛЕКСНОЇ СИСТЕМИ МЕРЕЖЕВОЇ ТА ОПЕРАЦІЙНОЇ БЕЗПЕКИ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

Онопрієнко М. Ю.
Державний університет інформаційно-комунікаційних технологій
м. Київ, Україна

У сучасних умовах цифрової трансформації економіки стабільність функціонування підприємств безпосередньо залежить від надійності їх корпоративних інформаційних систем. Більшість управлінських, фінансових, виробничих та комунікаційних процесів здійснюється із використанням інформаційно-комунікаційних технологій. Така залежність від цифрової інфраструктури суттєво підвищує вимоги до забезпечення її безпеки. Порушення роботи інформаційної системи може призвести не лише до тимчасових збоїв, а й до значних фінансових втрат, витоку конфіденційної інформації та репутаційних ризиків.

Останніми роками спостерігається зростання кількості кіберінцидентів, спрямованих на корпоративні мережі та серверну інфраструктуру. Сучасні атаки характеризуються складністю, багаторівневістю та використанням комбінацій різних методів впливу. Зловмисники активно експлуатують як мережеві вразливості, так і недоліки конфігурації операційних систем, служб автентифікації та програмного забезпечення. У таких умовах забезпечення безпеки лише на одному рівні є недостатнім, оскільки атака може реалізовуватися через ланцюг взаємопов’язаних вразливостей.

На практиці більшість підприємств впроваджують окремі засоби захисту, зокрема міжмережеві екрани, антивірусні рішення, системи виявлення вторгнень, засоби резервного копіювання та механізми контролю доступу. Проте їх використання без комплексної інтеграції та централізованого моніторингу не дозволяє досягти максимальної ефективності. Фрагментарний

підхід до побудови системи безпеки призводить до ситуації, коли окремі елементи працюють ізольовано, що ускладнює своєчасне виявлення складних атак і збільшує час реагування на інциденти.

У зв’язку з цим актуальним є формування комплексної системи мережевої та операційної безпеки, яка передбачає узгоджену взаємодію різних механізмів захисту. Такий підхід базується на принципі багаторівневого захисту, відповідно до якого безпека забезпечується одночасно на мережевому, системному та прикладному рівнях. Особливу роль при цьому відіграє централізований моніторинг подій інформаційної безпеки та можливість оперативного реагування на виявлені загрози.

Метою дослідження є розробка комплексної системи мережевої та операційної безпеки корпоративної інформаційної системи та оцінювання її ефективності в умовах моделювання типових кіберзагроз. У межах роботи проведено аналіз сучасних підходів до забезпечення інформаційної безпеки, розглянуто актуальні загрози та визначено їх потенційний вплив на функціонування корпоративної інфраструктури.

На основі проведеного аналізу сформовано модель загроз для умовної корпоративної інформаційної системи, яка включає серверний сегмент, робочі станції користувачів та мережеву інфраструктуру. Враховано як зовнішні, так і внутрішні джерела загроз, зокрема спроби несанкціонованого доступу, використання шкідливого програмного забезпечення, експлуатацію вразливостей операційних систем, а також помилки конфігурації.

Запропонована архітектура комплексної системи безпеки передбачає впровадження механізмів мережевої фільтрації трафіку, сегментацію мережі, використання систем виявлення вторгнень, контроль прав доступу до ресурсів та централізований збір і аналіз журналів подій. Важливою складовою є забезпечення взаємодії між компонентами системи з метою формування єдиного інформаційного простору безпеки.

Для перевірки ефективності запропонованих рішень створено тестове середовище, у якому моделюються типові сценарії атак. Зокрема, імітуються

спроби мережевого сканування, підбору облікових даних, несанкціонованого доступу до ресурсів, а також експлуатація відомих вразливостей операційних систем. Оцінювання результатів здійснюється на основі кількісних показників, таких як рівень виявлення інцидентів, час реагування на загрозу та зменшення ризику її успішної реалізації.

Отримані результати свідчать про доцільність інтеграції мережевих і операційних механізмів захисту в єдину систему з централізованим управлінням. Комплексний підхід дозволяє підвищити рівень стійкості інформаційної інфраструктури підприємства, зменшити ймовірність реалізації кіберзагроз та забезпечити більш ефективний контроль за станом безпеки.

Таким чином, розробка та дослідження ефективності комплексної системи мережевої та операційної безпеки є актуальним напрямом у сфері інформаційної та кібернетичної безпеки. Запропоновані рішення можуть бути використані для вдосконалення практики побудови систем захисту в організаціях різного масштабу та профілю діяльності.

Література

1. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Geneva: ISO, 2022.

2. NIST. Security and Privacy Controls for Information Systems and Organizations (SP 800-53 Rev. 5). Gaithersburg, MD, 2020.

3. Stallings W. Computer Security: Principles and Practice. 4th ed. Pearson, 2018.

4. Anderson R. Security Engineering. 2nd ed. Wiley, 2020.

5. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII.

МЕТОДИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ API КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ ТА СЕРВІСІВ

Цюпак Н. Ю.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

Сучасні корпоративні інформаційні системи широко використовують програмні інтерфейси додатків (API) для інтеграції програмних компонентів, обміну даними та реалізації мікросервісної архітектури. Використання API забезпечує гнучку взаємодію між сервісами, підвищує масштабованість програмних систем та спрощує інтеграцію різних інформаційних ресурсів [1].

Разом із розвитком мікросервісної архітектури зростає і кількість потенційних загроз безпеці інформаційних систем. Збільшення кількості взаємодій між сервісами через API розширює поверхню атаки системи та створює додаткові ризики несанкціонованого доступу до інформаційних ресурсів [2]. Наукові дослідження показують, що найбільш поширеними загрозами для API є помилки автентифікації, недостатній контроль авторизації, а також витік конфіденційних даних під час передачі інформації [3].

Ефективний захист API корпоративних інформаційних систем передбачає використання комплексу механізмів безпеки. Одним із ключових елементів є автентифікація користувачів і сервісів, яка дозволяє перевіряти достовірність суб’єктів, що здійснюють доступ до ресурсів системи. У сучасних інформаційних системах для цього застосовуються стандартизовані механізми автентифікації та токени доступу.

Іншим важливим механізмом забезпечення безпеки є авторизація доступу до ресурсів системи, яка дозволяє обмежувати доступ до API відповідно до ролей користувачів. Для цього застосовуються моделі контролю доступу, які забезпечують гнучке управління правами користувачів і запобігають несанкціонованому використанню інформаційних ресурсів [4].

Важливим компонентом забезпечення безпеки API є захист передачі даних між компонентами інформаційної системи. Для цього використовуються криптографічні протоколи захисту мережевих з'єднань, які забезпечують конфіденційність та цілісність інформації під час її передачі. У сучасних інформаційних системах також широко застосовуються централізовані механізми контролю доступу до API, зокрема API Gateway, які виконують функції автентифікації, фільтрації запитів та моніторингу активності користувачів.

Додатковими заходами забезпечення безпеки є обмеження частоти запитів, ведення журналів доступу та використання систем виявлення аномальної активності. Основні загрози безпеці API та відповідні методи їх усунення узагальнено у табл. 1.

Таблиця 1

Основні загрози безпеці API та методи їх усунення

Загроза безпеці API	Опис загрози	Метод захисту
Несанкціонований доступ	Доступ до API без належної автентифікації	Використання механізмів автентифікації (OAuth 2.0, JWT)
Недостатній контроль авторизації	Отримання доступу до ресурсів без відповідних прав	Використання моделей контролю доступу RBAC або ABAC
Перехоплення даних	Передача даних може бути перехоплена під час мережевої взаємодії	Використання протоколів шифрування TLS
Перевантаження API	Надмірна кількість запитів може призвести до відмови в обслуговуванні	Обмеження частоти запитів (Rate limiting)
Аномальна активність	Підозрілі або шкідливі запити до API	Моніторинг запитів та системи виявлення аномалій

Комплексне застосування зазначених методів дозволяє значно підвищити рівень безпеки корпоративних інформаційних систем та зменшити ризик несанкціонованого доступу до інформаційних ресурсів.

Література

1. Chen L. Microservices: Architecting for Continuous Delivery and DevOps. *IEEE Software*. 2018. Vol. 35, no. 3. P. 52–60. URL: https://doi.org/10.1109/MS.2018.2141039

2. Rahman A., Williams L., Parnin C. Characterizing the Security of Microservice-Based Systems. *Proceedings of the IEEE International Conference on Software Architecture*. 2019. P. 195–206. URL: https://doi.org/10.1109/ICSA.2019.00018

3. Zhang Q., Chen M., Li L. Security Analysis of API-Based Cloud Services. *Future Generation Computer Systems*. 2020. Vol. 108. P. 1078–1090. URL: https://doi.org/10.1016/j.future.2019.09.059

4. Rahman M., Hossain M., Islam S. API Security in Cloud Computing: A Comprehensive Review. *Journal of Network and Computer Applications*. 2021. Vol. 178. URL: https://doi.org/10.1016/j.jnca.2020.102948

5. Nayak R., Padhy N. Security Issues in Microservices Architecture: A Systematic Literature Review. *Journal of Systems and Software*. 2022. Vol. 188. URL: https://doi.org/10.1016/j.jss.2022.111245

СЕКЦІЯ 5. ПРОТИДІЯ КІБЕРАТАКАМ НА СИСТЕМИ І БІЗНЕС-СЕРВІСИ КОМПАНІЇ

ПОБУДОВА МОЗКОПОДІБНИХ НЕЙРОННИХ МЕРЕЖ ДЛЯ ЗАДАЧ КЛАСИФІКАЦІЇ ТА ДЕТЕКЦІЇ АНОМАЛІЙ У БІЗНЕС-СЕРВІСАХ

Архипов О. О.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

Сьогодні традиційні методи глибокого навчання (ANN) стикаються з проблемою високої обчислювальної складності та неспроможності ефективно виявляти атаки типу "Zero-day" у реальному часі. Ця теза пропонує переосмислення підходів до інтелектуального захисту через використання нейроморфних (мозкоподібних) архітектур, зокрема імпульсних нейронних мереж (SNN).

Ключова ідея полягає у використанні часової динаміки обробки сигналів. На відміну від класичних моделей, запропонована система базується на моделі нейрона LIF (Leaky Integrate-and-Fire). Це дозволяє мережі не просто аналізувати дані, а "відчувати" ритм вхідного трафіку, автоматично фільтруючи випадковий шум (через механізм витоку) та накопичуючи інформацію про потенційні загрози в часі.

Для забезпечення автономності системи я планую використати біо інспірований механізм навчання STDP (Spike-Timing-Dependent Plasticity). Це дасть змогу системі навчатися "без вчителя", адаптуючись до специфічного профілю нормальної роботи бізнес-сервісів компанії. Такий підхід робить систему стійкою до складних атак типу "Low and Slow" та дозволяє виявляти аномалії без наявності попередньо розмічених баз атак. Механізм: STDP — це біологічний закон навчання: вага зв'язку (синапса) між

нейронами змінюється залежно від того, коли вони збудилися відносно один одного.

Логіка механізму (правила Хебба):

1. Потенціювання (LTP): Якщо вхідний сигнал (пресинаптичний спайк) прийшов за мить до того, як нейрон «вистрілив», система вважає, що цей сигнал був причиною збудження. Вага цього зв’язку збільшується.

2. Депресія (LTD): Якщо сигнал прийшов після збудження нейрона або занадто пізно, вага зв'язку зменшується.

У традиційних нейронних мережах інформація передається як статичне число (вага). У мозок-подібних (імпульсних) мережах важливо не тільки «що» прийшло, а й «коли» воно прийшло. Аномалія в кібербезпеці — це майже завжди порушення часового ритму (наприклад, занадто швидкі запити до бази даних або нетипові інтервали між пакетами).

Для моделювання цього процесу використовується модель LIF (Leaky Integrate-and-Fire). Це математичне спрощення того, як працює біологічний нейрон.

$$\tau_m \frac{dV_m(t)}{dt} = -(V_m(t) - V_{rest}) + RI(t)$$

1. $V_m(t)$ (Membrane Potential): Це «рівень напруги» або «рівень підозри» нейрона в момент часу t. Якщо цей рівень досягає певного порогу (V_{th}), нейрон «стріляє» (генерує спайк) — це і є момент детекції аномалії.

2. $\frac{dV_m(t)}{dt}$: Швидкість зміни цього потенціалу. Вона показує, як швидко накопичуються ознаки атаки.

3. $-(V_m(t) - V_{rest})$ (Leaky — «витік»): Це ключова частина. Якщо на вхід довгий час нічого не надходить, потенціал нейрона поступово повертається до стану спокою (V_{rest}). Це захист від хибних спрацювань. Поодинокі підозрілі пакети, розтягнуті в часі, «забуваються» системою і не викликають тривоги.

4. τ_m (Time Constant): Параметр, що визначає, як швидко нейрон «забуває» минулі події. Це налаштування чутливості вашого детектора

5. *RI*(t) (Input): Вхідний сигнал. Тут $I(t)$ — це потік даних з вашого бізнес-сервісу (наприклад, кількість з'єднань або розмір пакетів), а *R* — опір (коефіцієнт посилення сигналу).

За допомогою моделі LIF, нейрон накопичує інформацію про вхідний трафік. Якщо підозрілі події відбуваються часто і щільно, потенціал нейрона V_m швидко зростає і пробиває поріг — ми фіксуємо аномалію. Якщо ж підозрілі події трапляються рідко, нейрон "скидає" напругу через механізм витоку (Leak), розуміючи, що це, швидше за все, випадковий шум, а не спланована атака. Це дозволяє нам ідентифікувати складні Zero-day атаки, які намагаються мімікрувати під нормальний трафік, розтягуючи свої дії в час. Проблема «Low and Slow» атак та їх рішення:

Якщо хакер надсилає по одному підозрілому пакету раз на годину, потенціал V_m одного LIF-нейрона справді буде встигати «стікати» (leak) до нуля. Система сприйматиме це як випадковий шум. Зловмисники використовують це, щоб обійти стандартні пороги захисту (Thresholds).

В мозку немає одного нейрона на всі випадки життя. Існує популяція нейронів.

- Одні нейрони мають малу τ_m: вони «швидкі», миттєво реагують на лавиноподібні атаки (наприклад, Flood DDoS), але швидко забувають.
- Інші нейрони мають велику τ_m: вони «повільні», їхній потенціал стікає дуже повільно (годинами або днями). Вони накопичують інформацію про ті самі поодинокі пакети.

Крім потенціалу нейрона (V_m), який швидко зникає, є ще вага зв'язку (синапса).

- Навіть якщо V_m впав до нуля, сам факт проходження підозрілого сигналу може трохи змінити вагу зв'язку.

● При повторенні «поодинокого пакета» через годину, система вже реагуватиме на нього сильніше, бо синапс «запам'ятав» попередню подію

Література

1. Gerstner, W., & Kistler, W. M. (2002). *Spiking Neuron Models: Single Neurons, Populations, Plasticity.* Cambridge University Press.

2. Cordone, L., et al. (2022). *Spiking Neural Networks for Network Intrusion Detection.* (IEEE/ACM Transactions).

СИСТЕМА АНАЛІЗУ ТА КЛАСИФІКАЦІЇ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ З ВИКОРИСТАННЯМ МЕТОДІВ МАШИННОГО НАВЧАННЯ

Лозова І. Л., канд. техн. наук,

Афанасьєв І. О.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

Зростання кількості шкідливого програмного забезпечення (ШПЗ) стає все більшою загрозою для інформаційної безпеки. Традиційні сигнатурні методи виявлення часто не є ефективними у випадках нових або змінених зразків ШПЗ. Використання машинного навчання дозволяє автоматизувати аналіз, підвищити точність класифікації та зворотній відгук на загрози.

Сучасні зразки шкідливого програмного забезпечення часто застосовують такі техніки, як обфускація коду, шифрування, поліформізм, динамічна зміна поведінки. Через це їх виявлення за допомогою традиційних методів стає неабияк складним. Відтак, особливо актуальним стає застосування інтелектуальних методів аналізу ШПЗ, зокрема алгоритмів машинного

навчання, які здатні знаходити приховані закономірності у великих обсягах даних та пристосовуватися до нових загроз.

Метою роботи є розробка системи розпізнавання і класифікації шкідливого програмного забезпечення на основі технологій машинного навчання для покращення ефективності виявлення кіберзагроз.

Сучасні напрямки досліджень з кібербезпеки все активніше зосереджуються на можливостях застосування машинного навчання. Так, Saxe і Sanders у своїй роботі [1] представили концепцію виявлення шкідливого коду, яка базується на принципах data science і використанні моделей класифікації. У статті [2] описується застосування нейронних мереж для розпізнавання різних типів мережевих атак, що є черговим підтвердженням ефективності глибоких моделей у кіберзахисті. У дослідженні [3] наведено основні характеристики систем виявлення атак та можливі напрямки їхньої побудови, що може слугувати теоретичною базою для формування ознак у задачах аналізу ШПЗ.

Проте, навіть за умови широкої бази досліджень, проблеми інтеграції статичного та динамічного аналізу, підвищення узагальнювальної здатності моделей, а також їхньої адаптації до нових видів загроз залишаються відкритими.

Для підвищення об’єктивності оцінки моделей застосовувалися методи попередньої обробки даних, нормалізації ознак, відбору найбільш інформативних характеристик та кросвалідації. Виконано порівняльний аналіз ефективності різних алгоритмів машинного навчання з метою визначення найбільш підходящого для задачі класифікації шкідливого програмного забезпечення. Результати можна використовувати для підвищення точності та швидкості виявлення шкідливого програмного забезпечення, зниження залежності від сигнатурних методів, а також для автоматизації процесів в кібербезпеці, зокрема у розпізнаванні нових типів атак.

Отримані результати свідчать про те, що методи машинного навчання дійсно можуть ефективно застосовуватись у задачах аналізу і класифікації шкідливого ПЗ. Комплексний підхід дозволяє не лише підвищувати точність виявлення загроз, а й забезпечувати адаптивність системи до нових типів

кіберзагроз. Результати можуть використовуватися у SOC-центрах, антивірусних системах, системах моніторингу безпеки, sandbox-середовищах, а також для навчання фахівців із кібербезпеки.

В подальшому є можливості для розвитку досліджень у напрямі застосування методів глибокого навчання, автоматичного виділення ознак, використання онлайн-навчання, а також інтеграції розробленої системи у хмарні середи та системи безперервного моніторингу безпеки.

Література

1. Saxe J., Sanders H. Malware Data Science: Attack Detection and Attribution. No Starch Press, 2018.

2. Складанний, П., Костюк, Ю., Рзаєва, С., Самойленко, Ю., Савченко, Т. Розробка модульних нейронних мереж для виявлення різних класів мережевих атак. Кібербезпека: освіта, наука, техніка. 2025. No 3(27), с. 534–548.

3. Толюпа С. В., Штаненко С. С., Берестовенко Г. Класифікаційні ознаки систем виявлення атак та напрямки їх побудови. 2018. Збірник наукових праць Військового інституту телекомунікацій та інформатизації імені Героїв Крут. Вип. № 3. с. 56–66.

СИСТЕМА МОНІТОРИНГУ ТА АНАЛІЗУ АНОМАЛЬНОЇ ПОВЕДІНКИ КОРИСТУВАЧІВ У КОРПОРАТИВНИХ МЕРЕЖАХ НА ОСНОВІ SYTECA UAM

Гавришенко Д. С.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

Зростання кількості інцидентів інформаційної безпеки за участі внутрішніх користувачів вимагає впровадження систем, які не лише фіксують

події, а й аналізують зміни в поведінці користувачів у корпоративному середовищі [1]. Традиційне журналювання не дозволяє швидко виявити підготовчі етапи інсайдерських загроз. Тому актуально використовувати системи класу UAM (User Activity Monitoring) разом з поведінковою аналітикою [2].

У роботі розглянуто платформу Syteca UAM як інструмент для моніторингу та аналізу аномальної активності користувачів у корпоративних мережах [3].

Аналіз інтерфейсу системи показав, що моніторинг здійснюється через кілька рівнів відображення даних. На рівні Activity Chart відображається візуалізація часу використання окремих процесів (cmd.exe, explorer.exe, chrome.exe, msedge.exe). Це дозволяє визначити основні сценарії роботи користувача та виявити відхилення від типової поведінки (рис. 1). Наприклад, значне зростання часу роботи з командним рядком або адміністративними утилітами може свідчити про підозрілу активність [2].

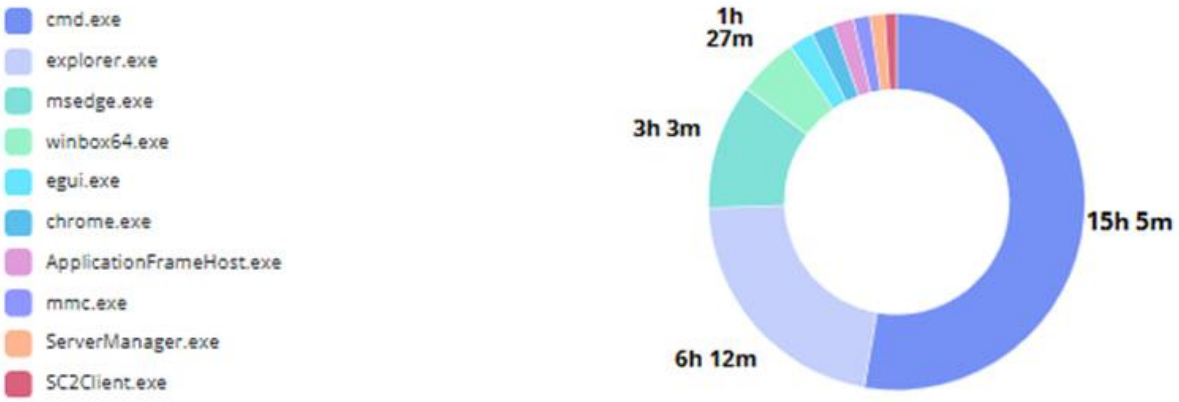

Рис. 1. Виявлено інцидент запуску розважального ПЗ (SC2Client.exe)

Графічний модуль ризикових категорій показує події за рівнем критичності (Normal, High, Critical) (рис. 2). Активність типу usb-plug-in з високим рівнем ризику демонструє можливість контролю використання зовнішніх носіїв інформації — одного з найбільш поширених шляхів витоку даних [1].

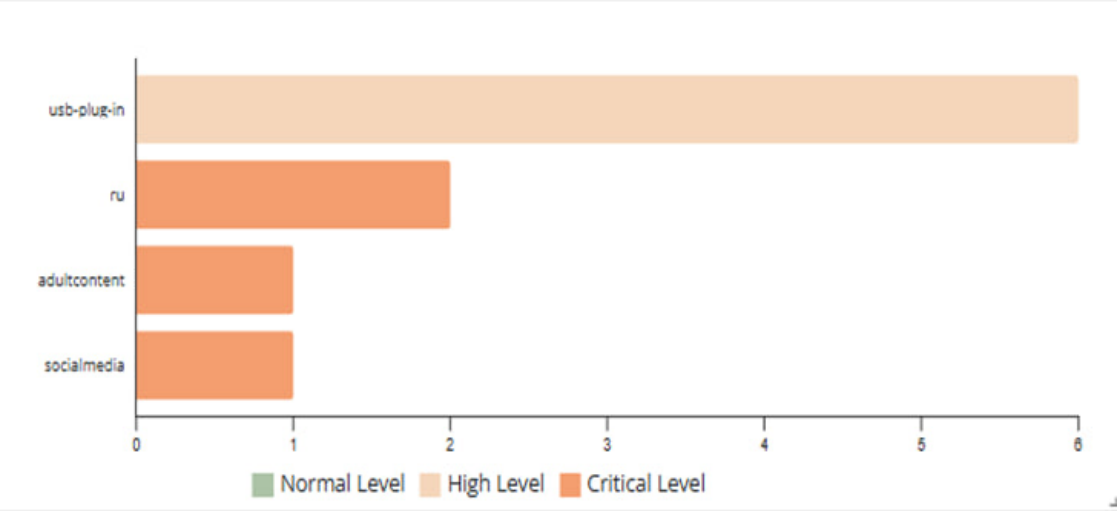

Рис. 2. Топ спрацювань порушень політик безпеки

У журналі подій (Detailed Activity Grid) відображаються конкретні дії користувача: запуск процесів, підключення USB-пристроїв, відкриття директорій, контекстні операції (рис.3). Часові мітки та ідентифікація процесів дозволяють відновити повну послідовність дій у межах робочої сесії, що є важливим для проведення аудиту або розслідування інцидентів інформаційної безпеки [2].

Activity Ti...	Activity Ti...	Applicatio...	URL	Text Data	Alert/USB
15:21:07	Program Manager	explorer.exe			
15:21:23	Program Manager	explorer.exe			
15:21:23	Program Manager	explorer.exe			usb-plug-in
15:21:24	Сповіщення - ESE...	egui.exe			
15:21:25	Флешка 8 Гб (D:)	explorer.exe			
15:21:25	USBStorage - D:\ - ...	[Monitoring event]			
15:21:25	Program Manager	explorer.exe			
15:21:29	Контекстне меню	explorer.exe			

Рис. 3. Лог подій сесії користувача із тригерами порушення

Система звітності Syteca UAM містить різні способи представлення інформації (Alert Grid, Session Grid, Clipboard Grid, Overtime Work Grid тощо) (рис. 4). Це забезпечує гнучкість аналізу залежно від задачі — оперативного реагування, аудиту або цифрової експертизи.

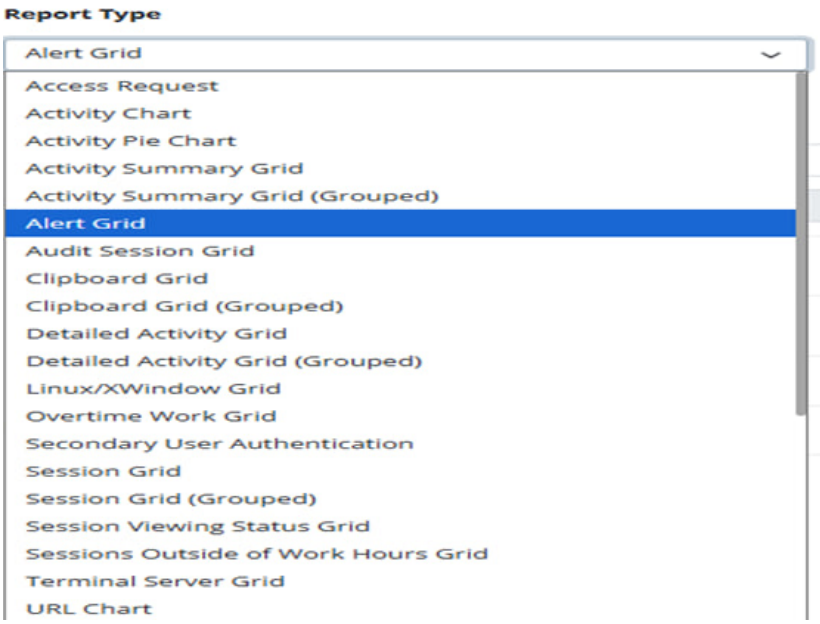

Рис. 4. Вибір звітності

На основі дослідження функціоналу створено узагальнений алгоритм виявлення аномалій поведінки користувача:

1. Збір телеметричних даних агентами системи;

2. Нормалізація та класифікація подій;

3. Формування базової поведінкової моделі користувача;

4. Виявлення відхилень за часовими, кількісними та контекстними параметрами.

5. Призначення індексу ризику та генерація сповіщення.

Практичне значення роботи полягає у створенні структурованої моделі моніторингу активності користувача. Вона дозволяє своєчасно виявляти:

- масове копіювання або переміщення файлів;
- використання нетипових програм;
- підключення змінних носіїв;
- активність у неробочий час;
- зловживання адміністративними інструментами.

Таким чином, використання Syteca UAM дозволяє перейти від реактивного аналізу журналів подій до проактивного контролю поведінкових ризиків. Це підвищує рівень захищеності корпоративної мережі.

Література

1. Bishop M. Computer Security: Art and Science. – Boston: Addison-Wesley, 2018 URL: https://www.pearson.com/en-us/subject-catalog/p/computer-security-art-and-science/P200000000134/9780321712332.
2. Behl A., Behl K. Cybersecurity and Cyberwar: What Everyone Needs to Know. – Oxford University Press, 2020 URL: https://www.syteca.com/en/product/user-activity-monitoring.
3. Syteca. User Activity Monitoring System – Official Documentation. – 2025 URL: https://www.syteca.com/docs.

МЕТОДОЛОГІЧНІ АСПЕКТИ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ ТИПУ PROMPT INJECTION У СИСТЕМАХ З ІНТЕГРОВАНИМ ШТУЧНИМ ІНТЕЛЕКТОМ

Гапелик Д. О.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

Сучасний етап розвитку веб-технологій характеризується стрімкою інтеграцією великих мовних моделей (Large Language Models, LLM) у клієнт-серверну архітектуру веб-застосунків. Використання генеративного штучного інтелекту (ШІ) дозволяє автоматизувати обробку «живої» мови, створення контенту та взаємодію з користувачами. Однак, поява нового компонента в системі неминуче призводить до розширення поверхні атак та виникненню нових загроз та ризиків.

Традиційні засоби захисту, такі як Web Application Firewalls (WAF), орієнтовані на блокування відомих сигнатур у запитах користувача (наприклад, SQL Injection або XSS) [1]. Натомість атаки на LLM, зокрема маніпуляція

вхідними інструкціями (Prompt Injection), базуються на семантичному рівні взаємодії, де межа між керуючими командами та даними користувача є розмитою. Це робить класичні методи фільтрації вводу користувача неефективними та вимагає розробки спеціалізованих методологічних аспектів до проведення тестування на проникнення.

Основним завданням дослідження є аналіз механізмів виникнення вразливостей типу Prompt Injection та розробка методологічного базису для їх ідентифікації в системах з інтегрованим ШІ. Необхідно враховувати як прямі вприскування інструкцій через інтерфейс користувача, так і непрямі (Indirect Prompt Injection), де шкідливий контент надходить із зовнішніх джерел даних (інших веб-застосунків, бази даних, файлів), що обробляються моделлю [2]. Адаптація стандартного процесу пентесту під ці загрози є важливою для забезпечення комплексного підходу та повного покриття веб-додатків перевірками.

Для досягнення мети дослідження необхідно вирішити наступні підзадачі:

1. Класифікація вводу**:** диференціація прямих атак (через форми введення користувача) та непрямих ін'єкцій (Indirect Prompt Injection), коли шкідливі інструкції потрапляють до моделі через сторонні джерела - веб-сторінки, файли або API-відповіді, які LLM використовує як контекст [2].

2. Аналіз механізмів обходу фільтрів: дослідження технік обфускації промптів, таких як зміна рольової моделі (role-play), переклад інструкцій на малопоширені мови (які гірше сприймаються моделлю) або використання спеціальних токенів для скидання попереднього контексту.

3. Визначення наслідків експлуатації: оцінка ризиків, пов'язаних із «надмірними повноваженнями» (Excessive Agency), коли успішна ін'єкція дозволяє моделі несанкціоновано викликати внутрішні функції системи або розголошувати конфіденційні дані зловмисику[3].

Адаптація стандартного життєвого циклу пентесту до цих специфічних загроз є важливою для переходу від реактивного захисту до проактивної моделі безпеки веб-застосунків.

У ході дослідження було визначено, що традиційний життєвий цикл тестування на проникнення потребує адаптації через нелінійну природу відповідей LLM. Запропонований методологічний підхід до виявлення вразливостей типу Prompt Injection базується на трьох ключових етапах:

1. Семантичний аналіз векторів вводу. На відміну від пошуку спецсимволів (як у SQLi), аудит LLM-систем передбачає тестування вразливості моделі до технік «втечі з контексту» (Context Escape). Це включає використання багатомовних запитів (Multi-lingual Jailbreaking) та методів кодування (Base64, Leetspeak) для обходу вбудованих контент-фільтрів [4].

2. Тестування системних обмежень (System Prompt Extraction). Важливим аспектом є перевірка можливості вилучення прихованих інструкцій розробника. Успішна атака на цьому етапі дозволяє зловмиснику зрозуміти логіку роботи бекенд-системи та підготувати підґрунтя для складніших сценаріїв експлуатації.

3. Аудит інтегрованих інструментів та плагінів. Найбільш критичним вектором є перевірка здатності моделі до виконання несанкціонованих дій у зовнішніх системах через механізм Function Calling. Досліджено, що через Prompt Injection можливо змусити модель сформувати легітимний, з точки зору API, запит на видалення даних або розсилку спаму, що фактично нівелює захист на рівні мережевих екранів (WAF) [1].

Результати практичних експериментів показують, що ефективність ідентифікації таких вразливостей суттєво підвищується при використанні стратегії «адаптивного пентесту», де кожен наступний запит до моделі генерується на основі аналізу її попередніх відповідей, імітуючи дії зловмисника.

Проведене дослідження підтверджує, що інтеграція великих мовних моделей у веб-застосунки створює специфічний клас загроз, які не можуть бути повноцінно усунені класичними методами фільтрації трафіку. Розроблена методологія, що фокусується на семантичному аналізі та аудиті повноважень моделі, дозволяє виявляти критичні недоліки в архітектурі захисту систем з ШІ. Подальші дослідження будуть спрямовані на автоматизацію процесів виявлення

Prompt Injection за допомогою спеціалізованих агентів тестування, що дозволить інтегрувати перевірки безпеки в CI/CD цикли розробки інтелектуальних систем.

Література

1. What is penetration testing | CLOUDFLARE. URL: https://www.cloudflare.com/learning/security/glossary/what-is-penetration-testing/ (дата звернення: 20.02.2025).

2. OWASP Top 10 for LLM Applications | OWASP Foundation. URL: https://owasp.org/www-project-top-10-for-large-language-model-applications/ (дата звернення: 22.02.2025).

3. Greshake K. et al. Not What You've Signed Up For: Compromising Real-World LLM-Integrated Applications with Indirect Prompt Injection. URL: https://arxiv.org/abs/2302.12173 (дата звернення: 24.02.2025).

4. Liu Y. et al. Jailbreaking ChatGPT via Prompt Engineering: An Empirical Study. URL: https://arxiv.org/abs/2305.13860 (дата звернення: 24.02.2025).

АНАЛІЗ ПІДХОДІВ ПРОТИДІЇ СОЦІОІНЖЕНЕРНИМ ЗАГРОЗАМ В ОРГАНІЗАЦІЯХ ТА УСТАНОВАХ

Горбач Н. О.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

Соціальна інженерія є одним із найбільш поширених та небезпечних інструментів реалізації кіберзагроз в організаціях. На відміну від технічних атак, соціоінженерні методи спрямовані на експлуатацію людського фактора шляхом маніпуляції, психологічного впливу та введення в оману працівників. За статистикою міжнародних досліджень у сфері кібербезпеки, значна частина

інцидентів інформаційної безпеки пов’язана саме з помилками персоналу та успішною реалізацією фішингових кампаній [1].

Основними видами соціоінженерних атак є фішинг (у тому числі spear phishing та whaling), вішинг, смишинг, претекстинг, baiting та фізичне проникнення (tailgating). Найбільш поширеним каналом залишається електронна пошта, через яку зловмисники здійснюють масові або таргетовані атаки з метою отримання конфіденційної інформації, облікових даних або фінансових ресурсів організації.

Ефективна протидія соціоінженерним загрозам повинна базуватися на комплексному підході, що поєднує організаційні, технічні та освітні заходи. До організаційних методів належать розробка політик інформаційної безпеки, впровадження принципу мінімальних привілеїв та чітка регламентація доступу до інформаційних ресурсів. Технічні засоби включають використання багатофакторної автентифікації (MFA), систем фільтрації електронної пошти, SIEM- та DLP-рішень. Водночас ключову роль відіграє підвищення рівня обізнаності персоналу через регулярні тренінги та проведення імітаційних фішингових кампаній [2].

Важливим елементом є оцінювання ризиків соціоінженерних атак відповідно до міжнародних стандартів (ISO/IEC 27001, NIST). Це дозволяє визначити критичні активи, оцінити ймовірність реалізації загроз та мінімізувати потенційні збитки. Інтеграція заходів протидії в систему управління інформаційною безпекою організації забезпечує системність та безперервність процесу захисту [3].

Ефективна система протидії соціоінженерним загрозам повинна базуватися на комплексному підході, що поєднує організаційні, технічні та освітні заходи, а також постійний процес оцінювання ризиків. Взаємозв’язок зазначених складових формує цілісну модель захисту організації від маніпулятивних впливів на персонал. Узагальнену структуру такої моделі наведено на рис. 1.

Рис. 1. Комплексна модель протидії соціоінженерним загрозам

Як видно з рис. 1, центральним елементом моделі є система протидії соціоінженерним загрозам, що формується під впливом чотирьох основних складових: оцінки ризиків, організаційних заходів, технічних засобів та освітніх програм. Взаємодія цих елементів забезпечує багаторівневий захист організації та мінімізує ймовірність успішної реалізації соціоінженерних атак.

Таким чином, протидія соціоінженерним загрозам потребує формування культури кібербезпеки в організації, поєднання сучасних технологічних рішень із належною підготовкою персоналу та постійного вдосконалення механізмів управління ризиками.

Література

1. Edwards L., Iqbal M. Z., Hassan M. *A multi-layered security model to counter social engineering attacks: a learning-based approach. International Cybersecurity Law Review*, 2024. DOI:10.1365/s43439-024-00119-z

2. Li T., Song C., Pang Q. *Defending against social engineering attacks: A security pattern-based analysis framework. IET Information Security*, Vol. 17, No. 4, 2023. DOI:10.1049/ise2.12125

3. Waelchli S., Walter Y. *Reducing the risk of social engineering attacks using SOAR measures in a real world environment: A case study. Computers & Security*, Vol. 148, 2025. DOI:10.1016/j.cose.2024.104137

СИСТЕМА АВТОМАТИЗОВАНОГО АНАЛІЗУ ЦИФРОВИХ АРТЕФАКТІВ ІЗ ВИКОРИСТАННЯМ ІСНУЮЧИХ FORENSIC-ІНСТРУМЕНТІВ

Лозова І. Л., канд. техн. наук,

Косинський О. О.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

Стрімке зростання кількості кіберінцидентів в Україні та світі, зокрема в умовах гібридної війни, актуалізує потребу в ефективних інструментах цифрової криміналістики. За даними звіту ENISA Threat Landscape 2025, кількість атак на критичну інфраструктуру зросла на 34% порівняно з попереднім роком [1]. Традиційний підхід до аналізу цифрових артефактів передбачає ручне застосування розрізнених forensic-інструментів, що є трудомістким і не дозволяє масштабувати розслідування.

Метою роботи є розробка архітектури системи автоматизованого аналізу цифрових артефактів, яка інтегрує наявні forensic-інструменти у єдиний конвеєр обробки даних.

Цифровий артефакт – будь-який об'єкт або фрагмент даних на цифровому носії, що може містити доказову інформацію: файли, записи реєстру, журнали подій, дампи пам'яті, мережеві пакети, метадані файлової системи. Аналіз

артефактів є ключовим етапом Digital Forensics and Incident Response (DFIR). Сучасна практика DFIR спирається на такі інструменти: Autopsy/The Sleuth Kit – аналіз файлових систем; Volatility 3 – аналіз дампів оперативної пам'яті; Wireshark/tshark – аналіз мережевого трафіку; Plaso/log2timeline – побудова хронології подій; YARA – сигнатурне виявлення шкідливого коду [2]. Попри потужність кожного з них, відсутність єдиного інтерфейсу керування та стандартизованих форматів виведення результатів суттєво ускладнює їх спільне використання.

Запропонована архітектура системи базується на мікросервісному підході та складається з таких компонентів: (1) Task Manager – приймає артефакти та розподіляє завдання між модулями; (2) Adapter Layer – набір уніфікованих обгорток для кожного forensic-інструменту, що нормалізують вихідні дані до спільного JSON-формату; (3) Message Broker (RabbitMQ) – забезпечує асинхронну передачу даних між компонентами; (4) Aggregator – об'єднує результати різних інструментів та будує хронологію подій; (5) Reporter – генерує структуровані звіти у форматах PDF та HTML. Ключовою особливістю є «Plugin Architecture»: кожен інструмент підключається через стандартизований інтерфейс, що дозволяє додавати нові модулі без зміни ядра системи [3].

Прототип системи розгорнуто у контейнеризованому середовищі Docker Compose та протестовано на наборі тестових образів дисків і дампів пам'яті з репозиторію Digital Corpora. Підхід узгоджується з рекомендаціями NIST SP 800-86 щодо інтеграції forensic-процесів у систему реагування на інциденти [4].

Розроблена система автоматизованого аналізу цифрових артефактів підтверджує ефективність оркестрації наявних forensic-інструментів через уніфіковані адаптери. Модульна архітектура забезпечує гнучкість і масштабованість, а стандартизація вихідних даних прискорює кореляцію результатів. Перспективою подальших досліджень є інтеграція модулів машинного навчання для автоматичної класифікації артефактів та виявлення аномалій на основі поведінкового аналізу.

Література

1. Chabot Y., Bertaux A., Nicolle C., Kechadi T. A complete formalized knowledge representation model for advanced digital forensics timeline analysis. Digital Investigation. Vol. 44. ISSN: 2666-2817 2023.
2. Du X. Le-Khac N.-A. Scanlon M. Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service. IFIP Advances in Information and Communication Technology. 701st ed. 2024. 81 p.
3. ENISA Threat Landscape 2023 | ENISA. *Home* | *ENISA*. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023(date of access: 24.02.2026).
4. Kent K., Chevalier S., Grance T., Dang H. Guide to Integrating Forensic Techniques into Incident Response. NIST SP 800-86. National Institute of Standards and Technology. *Home Page*. URL: https://doi.org/10.6028/NIST.SP.800-86(date of access: 24.02.2026).

МОДУЛЬ ПІДТРИМКИ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ ШЛЯХОМ ІНТЕГРАЦІЇ SIEM ТА SOAR-РІШЕНЬ

Лозова І. Л., канд. техн. наук,

Савицький А. О.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

В умовах зростання кількості складних кіберзагроз актуальним є підвищення ефективності реагування на кіберінциденти. Системи моніторингу інформаційної безпеки (SIEM) забезпечують централізований збір, нормалізацію та кореляцію подій безпеки, однак процес реагування часто залишається частково ручним, що збільшує час обробки інцидентів та навантаження на аналітиків SOC [2]. Платформи SOAR (Security Orchestration,

Automation and Response) дозволяють автоматизувати ці процеси, стандартизувати реакцію на інциденти та інтегрувати SIEM із засобами захисту.

Метою роботи є розробка модуля підтримки реагування на кіберінциденти шляхом інтеграції SIEM та SOAR-рішень для підвищення оперативності, узгодженості та рівня автоматизації процесів кіберзахисту.

У роботі проаналізовано сучасні підходи до побудови центрів моніторингу безпеки та функціональних можливостей SIEM і SOAR-платформ. Зокрема, розглянуто такі рішення, як Splunk Enterprise Security і Splunk SOAR (раніше Phantom) – для централізованого журналювання подій та автоматизації реагування; IBM QRadar SIEM у поєднанні з IBM Resilient SOAR – для кореляції подій, збагачення контекстом загроз і запуску автоматичних плейбуків; а також Cortex XSOAR від Palo Alto Networks – для оркестрації дій між різними компонентами захисту та інтегрованого керування інцидентами [3].

Запропоновано архітектуру інтеграції SIEM і SOAR-рішень, що включає компоненти збору даних, механізми нормалізації подій, модуль класифікації інцидентів та набір автоматичних сценаріїв реагування залежно від рівня критичності події. Розроблений модуль передбачає реалізацію стандартизованих плейбуків, які автоматично виконують такі дії: збагачення подій інформацією з Threat Intel, ізоляцію компрометованих хостів, блокування облікових записів та створення завдань у сервіс-десках. При цьому рішення адаптовано до вимог локального законодавства та рекомендацій з управління інцидентами [1, 2].

Очікуваним результатом впровадження запропонованого модуля є скорочення часу реагування на інциденти, зниження впливу людського фактора, зменшення навантаження на фахівців SOC та підвищення загального рівня інформаційної безпеки організації.

Запропоноване рішення може бути використане в корпоративних SOC, банківських установах і державних органах. Перспективами подальших досліджень є розробка методів машинного навчання для прогнозування складності інцидентів на основі історичних даних SIEM, оптимізація наборів

сценаріїв реагування для різних класів загроз і оцінювання впливу інтегрованих рішень на показники SOC у тривалому вимірі.

Література

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 24.02.2026).

2. Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки : ДСТУ ISO/IEC 27035:2018. Київ : ДП «УкрНДНЦ», 2018. 32 с.

3. Методичні рекомендації щодо організації заходів із кіберзахисту в банківській системі України / Національний банк України. Київ, 2020. URL: https://bank.gov.ua (дата звернення: 24.02.2026).

СУЧАСНІ ВЕКТОРИ ОТРИМАННЯ ПЕРВИННОГО ДОСТУПУ ДО КОРПОРАТИВНОЇ МЕРЕЖІ В РАМКАХ RED TEAMING

Скрипка О. В.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

В умовах стрімкої цифровізації та переходу до гібридних моделей роботи, забезпечення кіберстійкості стає фундаментальною умовою безперервності бізнесу. Традиційні методи оцінки захищеності, такі як сканування вразливостей або класичне тестування на проникнення (Penetration Testing), часто фокусуються на пошуку технічних помилок, не враховуючи складні ланцюги атак та людський фактор. Натомість методологія Red Teaming пропонує цілісний підхід до емуляції дій реальних зловмисників, де одним із ключових етапів є отримання первинного доступу (Initial Access).

Згідно з фреймворком MITRE ATT&CK, тактика Initial Access (TA0001) є відправною точкою для будь-якої операції [1]. У рамках Red Teaming операцій за 2025-2026 роки виділяються три основні вектори отримання доступу: соціальна інженерія з використанням AI, атаки на інфраструктуру ідентичності та експлуатація критичних вразливостей веб-застосунків.

Традиційний фішинг еволюціонує завдяки Generative AI. Дослідження показують, що AI-агенти, які використовуються для створення фішингових кампаній, перевершують результативність команд людей-операторів на 55% [2]. Використання великих мовних моделей (LLM) дозволяє автоматизувати створення контекстно-залежних листів (Spear Phishing), які важко відрізнити від легітимного ділового листування.

Окремим вектором, що набув популярності, є QR-фішинг або "Quishing". Зловмисники вбудовують шкідливі посилання у QR-коди, часто у форматі PDF або зображень, що дозволяє обходити традиційні шлюзи безпеки електронної пошти, оскільки аналіз графічного вмісту вимагає значних ресурсів [3]. Атака переносить вектор загрози з захищеного корпоративного комп'ютера на мобільний пристрій співробітника, який зазвичай менш контрольований службою безпеки.

Впровадження багатофакторної аутентифікації (MFA) змусило атакуючих адаптувати свої інструменти. Найбільш небезпечним методом на сьогодні є атаки типу Adversary-in-the-Middle (AiTM). Використовуючи інструментарій на кшталт Evilginx, оператори Red Team створюють проксі-сторінки, які перехоплюють не лише логін та пароль, а й сесійні токени автентифікації [4]. Це дозволяє отримати доступ до хмарних середовищ (Microsoft 365, Google Workspace) навіть за увімкненої MFA, не викликаючи підозри у користувача.

Також актуальним залишається метод Password Spraying — "розпилення" паролів, коли зловмисники перевіряють декілька найпоширеніших паролів проти великої кількості облікових записів, щоб уникнути блокування [5].

Попри акцент на людському факторі, технічна експлуатація вразливостей зовнішнього периметру компанії залишається ефективним методом входу. У

2025 році значний резонанс викликала вразливість CVE-2025-55182 (React2Shell), що дозволяє віддалене виконання коду (RCE) у компонентах React Server Components [6]. Такі вразливості дозволяють Red Team отримати контроль над сервером без взаємодії з користувачем, що є критичним для сценаріїв, де соціальна інженерія заборонена правилами проведення Red Teaming (Rules of Engagement).

Підсумовуючи, сучасна методологія Red Teaming вимагає від спеціалістів глибокого розуміння не лише технічних аспектів вразливостей, але й психології користувачів та принципів роботи сучасних засобів захисту ідентичності. Для протидії описаним векторам організаціям рекомендується проводити регулярні навчання персоналу з урахуванням новітніх трендів AI-фішингу, впровадження надійних політик парольної безпеки, а також проведення регулярних оцінок захищеності методами тестування проникнення, Red Teaming та соціальної інженерії.

Література

1. MITRE ATT&CK Framework. Initial Access Tactic. URL: https://attack.mitre.org/tactics/TA0001

2. AI-Powered Phishing Outperforms Elite Red Teams in 2025. Hoxhunt. URL: https://hoxhunt.com/blog/ai-powered-phishing-vs-humans

3. Phishing on the Edge of the Web and Mobile Using QR Codes. Unit 42. URL: https://unit42.paloaltonetworks.com/qr-codes-as-attack-vector

4. Cybercriminals Use Evilginx to Bypass MFA: Gmail, Outlook, and Yahoo. Abnormal AI. URL: https://abnormal.ai/blog/cybercriminals-evilginx-mfa-bypass

5. Password Spraying Attack: What You Need to Know and How to Prevent It. Infisign. URL: https://www.infisign.ai/blog/what-is-password-spraying-attack

6. CVE-2025-55182: React2Shell Analysis, Proof-of-Concept Chaos, and In-the-Wild Exploitation. Trend Micro. URL:https://www.trendmicro.com/ru_ru/research/25/l/CVE-2025-55182-analysis-poc-itw.html

МЕТОДИ ВИЯВЛЕННЯ ТА ПРОТИДІЇ АТАКАМ НА ІНФРАСТРУКТУРУ ЕЛЕКТРОННОЇ ПОШТИ ОРГАНІЗАЦІЇ

Сулима Б. В.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

Актуальність теми зумовлена зростанням ролі електронної пошти як базового бізнес-сервісу та відповідністю напрямам конференції, зокрема протидії кібератакам на системи і бізнес-сервіси компаній [1]. Інфраструктура електронної пошти організації є постійною ціллю фішингу, спуфінгу, компрометації облікових записів і сценаріїв Business Email Compromise (BEC), що можуть призводити до фінансових втрат, витоку даних і порушення безперервності бізнес-процесів.

Базовий рівень протидії формується через впровадження механізмів автентифікації домену відправника SPF, DKIM та DMARC. Згідно з NIST, ці технології є ключовими для підвищення довіри до електронної пошти та мають використовуватися в комплексі разом із захистом передавання (TLS) і належним адмініструванням [2]. SPF дозволяє домену визначити дозволені вузли надсилання [3], DKIM забезпечує перевірку цілісності та відповідальності домену через криптографічний підпис [4], а DMARC задає політику обробки повідомлень, що не проходять перевірку автентифікації, та підтримує звітність [5].

Для виявлення складніших атак доцільно поєднувати контентну та поведінкову аналітику: фільтрацію фішингових ознак у темі й тілі листа, аналіз вкладень і URL, моніторинг журналів подій поштових серверів, поштових шлюзів і систем автентифікації. Практичну ефективність також підвищують багатофакторна автентифікація, контроль привілеїв, сегментація доступу та інтеграція поштової інфраструктури з SIEM для оперативного сповіщення про аномалії.

Окрему увагу слід приділяти організаційним заходам: навчанню персоналу, перевірці фінансових і критичних запитів через незалежний канал зв'язку, а також регламентам реагування на інциденти BEC. IC3 та FBI

рекомендують використовувати вторинні канали підтвердження, уважно перевіряти адресу відправника та візуалізувати повні розширення файлів у листах. Отже, стійкість поштової інфраструктури забезпечується лише комплексним поєднанням технічних, організаційних та процесних засобів.

Рис. 1. Комплексна схема методів виявлення та протидії атакам на інфраструктуру електронної пошти

Таблиця 1

Методи виявлення атак та заходи протидії в поштовій інфраструктурі

Метод / засіб	Тип загрози	Що виявляє	Заходи протидії
SPF, DKIM, DMARC	Спуфінг домену, підміна відправника	Невідповідність домену, провал автентифікації	Політики DMARC (quarantine/reject), коректний DNS-запис, звітність
Антиспам/антифішинг, аналіз URL і вкладень	Фішинг, шкідливі вкладення	Ознаки соціальної інженерії, підозрілі посилання, макроси, архіви	Карантин листів, sandbox, блокування доменів/URL
MFA, моніторинг логів, навчання персоналу	BEC, компрометація акаунтів, несанкціонований доступ	Аномальні входи, нетипові дії, ризикові запити на платежі	MFA, вторинна перевірка запитів, регламенти реагування

Література

1. Rose S., Nightingale J. S., Garfinkel S. et al. Trustworthy Email (NIST SP 800-177 Rev. 1). National Institute of Standards and Technology, 2019. URL: https://csrc.nist.gov/pubs/sp/800/177/r1/final (дата звернення: 24.02.2026).
2. Kitterman S. Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1. RFC 7208, 2014. DOI: 10.17487/RFC7208. URL: https://www.rfc-editor.org/info/rfc7208 (дата звернення: 24.02.2026).
3. Crocker D., Hansen T., Kucherawy M. DomainKeys Identified Mail (DKIM) Signatures. RFC 6376 (STD 76), 2011. DOI: 10.17487/RFC6376. URL: https://www.rfc-editor.org/info/rfc6376 (дата звернення: 24.02.2026).
4. Kucherawy M., Zwicky E. Domain-based Message Authentication, Reporting, and Conformance (DMARC). RFC 7489, 2015. DOI: 10.17487/RFC7489. URL: https://www.rfc-editor.org/info/rfc7489 (дата звернення: 24.02.2026).
5. IC3 (Internet Crime Complaint Center). Business Email Compromise (BEC): опис загрози та рекомендації захисту. URL: https://www.ic3.gov/CrimeInfo/BEC (дата звернення: 24.02.2026).

ВАЖЛИВІСТЬ ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ЖУРНАЛІВ ПОДІЙ ТА ДОКАЗОВОЇ БАЗИ В СИСТЕМАХ КІБЕБЕЗПЕКИ ОРГАНІЗАЦІЙ

Юрчишин О.М.

Державний університет інформаційно-комунікаційних технологій

м.Київ, Україна

Стрімка цифровізація та перехід до складних розподілених інфраструктур зумовили зростання кількості кіберзагроз. У цьому контексті системи моніторінгу та управління подіями інформаційної безпеки стали центральним елементом захисту. Основою для цих систем є журнали подій – автоматизовані записи, що фіксують стан системи, дії користувачів, мережевий трафік та зміни конфігурації

[1]. Цінність будь-якої аналітичної системи дорівнює якості даних, які вона обробляє. Одним з найперших завдань зловмисника після отримання несанкціонованого доступу є приховування слідів своєї активності. І коли організація не здатна забезпечити цілісність своїх логів, вона втрачає не лише можливість оперативно зупинити атаку, але і здатність відновити хронологію подій.

Роль журналів подій у криміналістиці неможливо перебільшити. Фундаментальним поняттям у розслідуванні кіберзлочинів є ланцюжок збереження доказів (Chain of Custody). Цей юридичний та процедурний концепт вимагає безперервного документування життєвого циклу від моменту генерації та вилучення до моменту представлення в суді [4]. Щоб цифровий слід мав юридичну потрібно довести його автентичність й цілісність. Якщо ж архітектура системи дозволяє відкрити текстовий файл журналу і непомітно видалити кілька рядків, вся база логів на цьому сервері вважається скомпрометованою і не може використовуватись як доказ. Тому забезпечення цілісності вимагає впровадження механізмів що роблять будь яку модифікацію очевидною. Використання криптографічного хешування, цифрових підписів та систем типу WORM дозволяє гарантувати, що з моменту фіксації дані не зазнали змін. Інакше вони можуть бути легко оскарженні в суді або під час внутрішніх аудитів.

Також важливим питанням є операційна цінність для Security Operations Center (SOC). З точки зору щоденних операцій з кібербезпеки, цілісність логів є питанням видимості інфраструктури. Коли зловмисник отримує доступ до системи та знищує локальні журнали, для аналітиків виникає сліпа зона [2]. Втрата цілісності журналів подій унеможливлює відповіді на критичні питання:

1) Initial Access (Точка входу): Як саме зловмисник проник у мережу? За допомогою фішингу, експлуатації вразливості або скомпроментовані облікові данні?

2) Lateral Movement (Горизонтальне переміщення): Які ще вузли мережі були заражені або скомпроментовані після проникнення?

3) Data Exfiltration (Витік данних): Чи була скопійована конфіденційна інформація і в якому обсязі?

4) Persistence (Закріплення) Які бекдори або шкідливі сервіси були залишені в системі?

Сучасна інфраструктура зазнає значних викликів забезпечення цілісності. Особливого значення проблема набуває з переходом до мікросервісних архітектури, контейнеризації та систем оркестрації. Традиційні сервери роками могли накопичувати дані на локальних жорстких диска в той час як життєвий цикл робочого вузла може тривати від кількох секунд до кількох годин. Якщо контейнер знищується усі локільні дані безповоротно втрачаються. Ця особливість активно використовується. Зловмиснику достатньо ініціювати завершення роботи контейнера. Якщо система не забезпечує потокове пересилання логів до зовнішнього захищеного середовища, доказова база буде повністю знищена. Це робить впровадження централізованого логування критичною необхідністю для забезпечення кіберстійкості [5].

Також важливість цілісності журналів подій підкріплюється жорсткими нормативно правовими вимогами. Міжнародні та національні стандарти розглядають надійне логування як базовий мінімум:

- PCI DSS (стандарт безпеки індустрії платіжних карток) вимагає не лише збору логів транзакцій та доступу до систем, але й створення механізмів, що унеможливлюють їх підробку зі строком зберігання не менше року [3].
- GDPR (загальний регламент захисту ЄС) зобов’язує компанії протягом 72 годин повідомляти про витоки персональних даних.
- Директива NIS2 на рівні ЄС встановлює суворі вимоги до операторів критичної інфраструктури щодо безперервності бізнесу та управління інцидентами, де логування є ключовим інструментом доказування відповідності.

Неможливість надати цілісні, незмінні журнали подій розцінюється як грубе порушення політик безпеки і тягне за собою фінансові та репутаційні втрати. Забезпечення цілісності журналів подій є критичною умовою для розслідування інцидентів та формування доказової бази. Що вимагає впровадження комплексних криптографічних та апаратних засобів захисту, особливо у вразливих до втрат ефемерних контейнеризованих середовищах.

Література

1. Souppaya, M., & Kent, K. (2006). *Guide to Computer Security Log Management* (NIST Special Publication 800-92). National Institute of Standards and Technology. URL: https://doi.org/10.6028/NIST.SP.800-92

2. Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (3rd ed.). Academic Press.

3. Вимоги стандарту PCI DSS (Payment Card Industry Data Security Standard) v4.0. Домен 10: Логування та моніторинг доступу до систем.

4. ISO/IEC 27043:2015. *Information technology — Security techniques — Incident investigation principles and processes*. International Organization for Standardization.

5. Вуд, Дж. (2022). *Безпека мікросервісів та контейнерних середовищ: виклики оркестрації*. Journal of Cloud Computing and Cybersecurity, 12(4), 112-128.

ПРОТИДІЯ КІБЕРАТАКАМ НА СИСТЕМИ І БІЗНЕС-СЕРВІСИ КОМПАНІЇ

Ярмоленко Б. В.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

Сучасні компанії активно використовують інформаційні технології для забезпечення бізнес-процесів, зберігання даних клієнтів, фінансових операцій та взаємодії з партнерами. Перехід до цифрової економіки, впровадження хмарних сервісів, CRM-систем, електронної комерції та віддаленої роботи значно підвищили ефективність діяльності підприємств, однак одночасно збільшили кількість кіберзагроз. Будь-який бізнес-сервіс, підключений до мережі Інтернет, стає потенційною ціллю для кібератак [1]. У результаті

інцидентів кібербезпеки компанії можуть зазнати фінансових втрат, втрати репутації та зупинки операційної діяльності.

Однією з найбільш поширених загроз для бізнес-сервісів є DDoS-атаки, які спрямовані на перевантаження серверів і виведення системи з ладу. У разі недоступності веб-сайту або онлайн-сервісу компанія втрачає клієнтів і прибуток. Особливо небезпечними такі атаки є для інтернет-магазинів, банківських систем та сервісів електронних платежів, де навіть короткочасна відмова в роботі призводить до значних збитків. Крім того, DDoS-атаки часто використовуються як відволікаючий маневр для проведення більш складних вторгнень у систему.

Не менш небезпечною загрозою є фішинг та соціальна інженерія. Зловмисники отримують доступ до корпоративних систем шляхом обману співробітників. Підроблені електронні листи, фальшиві сторінки авторизації та повідомлення від імені керівництва змушують працівників вводити паролі або відкривати шкідливі вкладення. Таким чином відбувається компрометація облікових записів, що дозволяє атакуючим отримати доступ до внутрішніх ресурсів компанії. Значна частина інцидентів кібербезпеки пов’язана саме з людським фактором, а не технічними вразливостями [2].

Окрему категорію становлять шкідливі програми, зокрема ransomware. Після проникнення в корпоративну мережу шкідливе програмне забезпечення шифрує файли та вимагає викуп за їх відновлення. У разі відсутності резервних копій компанія може повністю втратити критично важливі дані. Часто такі атаки супроводжуються викраденням інформації з подальшим шантажем її публікацією. Це створює не лише фінансові, але й юридичні наслідки через порушення вимог щодо захисту персональних даних [3].

Загрози також виникають через експлуатацію вразливостей програмного забезпечення. Несвоєчасне оновлення систем, використання застарілих протоколів і помилки конфігурації відкривають можливість несанкціонованого доступу до серверів. Автоматизовані сканери мереж постійно шукають такі слабкі місця, тому навіть невелика компанія може стати жертвою атаки без прямої цілеспрямованості.

Для ефективної протидії кібератакам необхідно застосовувати комплексний підхід до кіберзахисту. Одним із ключових принципів є багаторівнева система безпеки. Вона передбачає використання міжмережевих екранів, систем виявлення вторгнень, антивірусного захисту, сегментації мережі та багатофакторної автентифікації. Навіть у разі компрометації одного рівня захисту інші механізми дозволяють зупинити поширення атаки.

Важливу роль відіграє моніторинг подій інформаційної безпеки. Використання систем централізованого журналювання та аналізу дозволяє своєчасно виявляти підозрілу активність. Аналіз поведінки користувачів допомагає визначити аномалії, що можуть свідчити про злом облікового запису. Чим раніше виявлено інцидент, тим меншими будуть наслідки для бізнесу.

Необхідним елементом захисту є резервне копіювання даних та план аварійного відновлення. Регулярне створення резервних копій забезпечує можливість швидкого відновлення роботи після кібератаки або технічного збою. Копії повинні зберігатися ізольовано від основної мережі, інакше шкідливе програмне забезпечення може зашифрувати їх разом з основними даними.

Організаційні заходи є не менш важливими за технічні. Навчання співробітників правилам кібергігієни значно зменшує ризик фішингових атак. Працівники повинні вміти розпізнавати підозрілі листи, не використовувати прості паролі та дотримуватись політик доступу. Регулярні інструктажі та тестові атаки дозволяють підтримувати належний рівень обізнаності персоналу.

Сучасною тенденцією у сфері кібербезпеки є впровадження концепції Zero Trust, яка передбачає перевірку кожного запиту незалежно від місця розташування користувача. Доступ до ресурсів надається лише після підтвердження особи та перевірки пристрою. Такий підхід значно зменшує ризик поширення атаки всередині мережі [4].

Отже, кібератаки становлять серйозну загрозу для функціонування бізнес-сервісів компанії. Найбільш небезпечними є DDoS-атаки, фішинг, шкідливе програмне забезпечення та експлуатація вразливостей. Ефективна протидія можлива лише за умови поєднання технічних засобів захисту, організаційних

заходів і підготовки персоналу. Забезпечення кіберстійкості повинно розглядатися як безперервний процес, що є складовою стратегічного управління компанією та запорукою стабільної роботи в умовах цифрового середовища.

Література

1. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems Requirements.

2. Конахович Г.Ф., Козловський В.А. Основи інформаційної безпеки. Київ: КПІ ім. Ігоря Сікорського, 2020. 316 с.

3. NIST Special Publication 800-61r2. Computer Security Incident Handling Guide. National Institute of Standards and Technology, 2019.

4.Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. NIST SP 800-207. NIST, 2020.

ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ У ФІНАНСОВИХ ТЕХНОЛОГІЯХ (FINTECH): СУЧАСНІ ВИКЛИКИ ТА МЕХАНІЗМИ ЗАХИСТУ

Асмолов С. О.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

У цифровій трансформації економіки фінансові технології (FinTech) є ключовим драйвером. Вони забезпечують швидкий доступ до фінансових послуг і автоматизацію процесів, що знижує витрати та підвищує конкуренцію на ринку.

Водночас FinTech-бізнеси дедалі більше залежать від надійності інформаційних систем. Збої чи кібератаки можуть спричинити переривання сервісів, фінансові втрати та втрату довіри клієнтів, тому безперервність бізнесу стає критичною.

Показовим прикладом є WeChat Pay (рис 1), який трансформував підхід до цифрових платежів і посилює конкуренцію. Разом із новими можливостями для компаній і споживачів зростає і кількість кіберзагроз. Для систематизації ключових аспектів впливу кібербезпеки на FinTech-сектор доцільно узагальнити їх у структурованому вигляді.

За цих умов кібербезпека виходить за межі технічного питання і набуває стратегічного значення для фінансових організацій. Захист інформаційних систем є необхідною умовою стійкості та довіри до FinTech у цифровій економіці[1].

Фінтех є важливим для безперервності бізнесу, автоматизуючи фінансові процеси, забезпечуючи доступність послуг і дозволяючи здійснювати платіжні процеси швидким способом.

Цифрові платформи працюють у режимі 24/7 і забезпечують безперервний доступ компаній до клієнтів. Це зменшує їхню залежність від фізичної інфраструктури та офлайн-каналів.

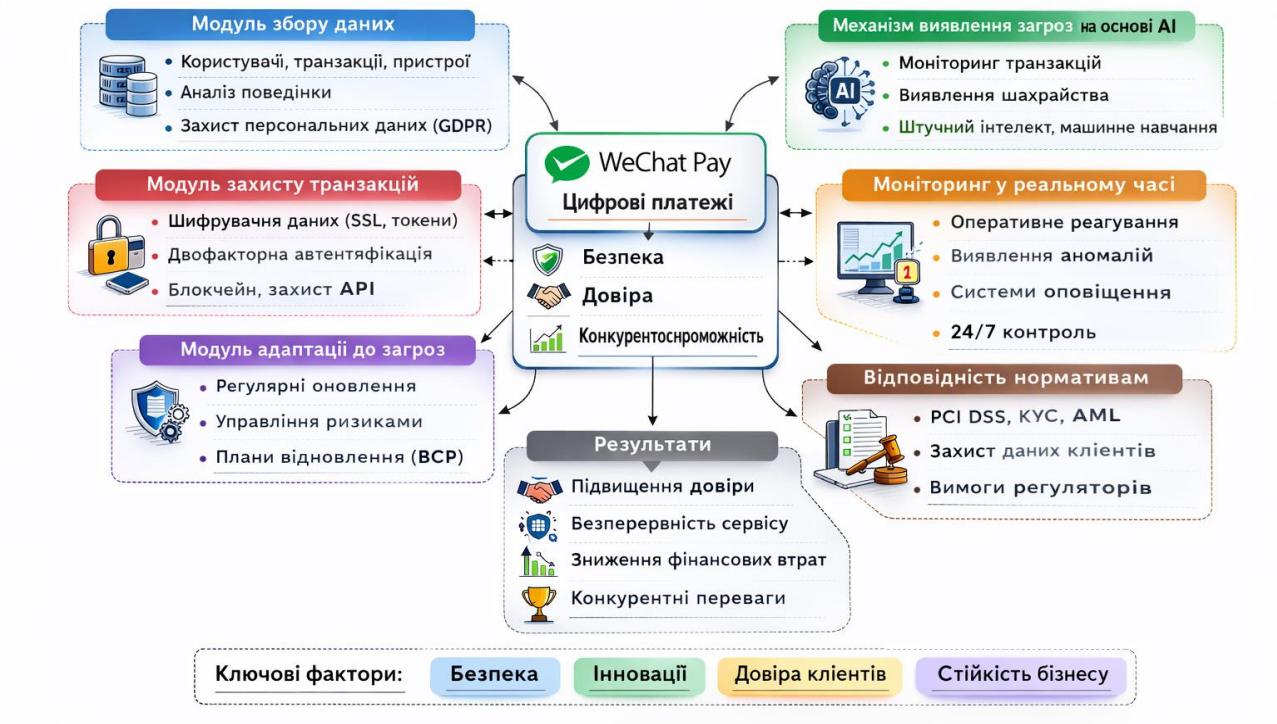

Рис.1. WeChat Pay

Фінтех-компанії впроваджують плани безперервності бізнесу (BCP) — проводять аналіз ризиків, резервне копіювання даних і сценарії реагування на кризові ситуації.

Це зміцнює операційну стійкість і дозволяє швидше відновлювати основні види діяльності. Використання хмарних сервісів, аналітики великих даних і моніторингу ліквідності в реальному часі дозволяє швидко реагувати на фінансові збої та мінімізувати можливість збитків. Кібербезпека має стратегічну цінність.

Безпека цифрових послуг і довіра клієнтів зміцнюються за допомогою криптографічного захисту транзакцій, двофакторної аутентифікації та виявлення аномалій за допомогою штучного інтелекту. Регулятори також хочуть бачити продемонстровані плани безперервності для захисту споживачів і забезпечення стабільності ринку.

Таким чином, фінтех підвищує гнучкість компаній, знижує операційні ризики та посилює конкурентну силу в кризових ситуаціях. Зростаюча автоматизація, безпека та ефективність фінансових рішень, що забезпечуються штучним інтелектом, блокчейном і хмарними обчисленнями, розширюють доступність фінансових послуг [2,3].

В українських FinTech-компаніях чат-боти стали важливим елементом цифрової взаємодії з клієнтами. Вони дозволяють автоматизувати комунікаційні процеси, скоротити час обробки звернень та оптимізувати витрати на підтримку сервісів. Ключові функціональні можливості чат-ботів у фінансовому секторі див (див. табл. 1) [4, с 5-6].

Таблиця 1

Функціональні можливості чат-ботів у FinTech

Функціональний напрям	**Практичний ефект для компанії**
Автоматизована обробка запитів клієнтів	Скорочення часу відповіді та підвищення швидкості обслуговування
Інформаційний супровід транзакцій	Зменшення операційного навантаження на персонал
Персоналізовані консультації	Підвищення рівня задоволеності та лояльності користувачів
Інтеграція з CRM та платіжними сервісами	Оптимізація внутрішніх бізнес-процесів і покращення управління даними

Таким чином, інтеграція чат-ботів у FinTech-секторі сприяє підвищенню операційної ефективності та конкурентоспроможності компаній.

Виклики обробки великих даних, персоналізації послуг та кібербезпеки стають у фокусі у банківському та технологічному секторах. Забезпечення кібербезпеки є ключовим для збереження довіри клієнтів та конкурентоспроможності традиційних банків у змаганні з FinTech-компаніями [5].

У галузі фінансових технологій (FinTech) зростає значення кібербезпеки через збільшення онлайн-операцій, тому компанії повинні посилити заходи безпеки даних та співпрацювати зі спеціалізованими компаніями для забезпечення надійності та довіри.

Література

1. Семенець М. О. FinTech та кібербезпека в е-банкінгу. URL: http://essuir.sumdu.edu.ua/handle/123456789/57306

2. What is FinTech? STFalcon. URL: https://stfalcon.com/uk/blog/post/what-is-fintech

3. Фінтех: інновації у галузі фінансів та у сфері технологій. URL: https://news.dtkt.ua/finance/other/90055-fintex-innovaciyi-u-galuzi-finansiv-ta-v-sferi-texnologii

4. Демчишак Н. Б., Гудима Р. П. Розвиток фінтеху в Україні та світі на основі використання технологій блокчейну і штучного інтелекту. Львівський національний університет імені Івана Франка. 2021. Р. 10.

5. FinTech: інновації у фінансовому секторі. Економічна правда. URL: https://www.epravda.com.ua/projects/fintech/2018/12/5/641431/#7

КІБЕРСТІЙКІСТЬ ДЕЦЕНТРАЛІЗОВАНИХ ФІНАНСОВИХ СИСТЕМ: ВИЯВЛЕННЯ ТА ПРОТИДІЯ КРИПТОЗЛОЧИНАМ І DeFi-ШАХРАЙСТВУ

Конкін В. О.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

За останні роки сектор криптовалют і децентралізованих фінансів (DeFi) зазнав значного зростання: кількість активів у DeFi-протоколах вимірюється десятками мільярдів доларів, а ринок криптовалют став невід'ємною частиною глобального фінансового ландшафту. Проте разом із цим стрімким розвитком зросла і кількість шахрайських схем, що спрямовані на експлуатацію характеристик блокчейну — анонімності, швидкості транзакцій та відсутності централізованого контролю. Такі кіберзагрози не лише завдають прямого фінансового збитку користувачам, але й підривають довіру до технологій, що вимагає ефективних підходів до управління ризиками та побудови кіберстійких систем [1].

Сучасні криптовалютні шахрайства представлені широким спектром типів. Згідно з даними TRM Labs, найпоширенішими з них є: романтичні шахрайства і схеми типу «pig butchering»; фейкові інвестиційні проекти і ICO з нереальними обіцянками прибутку; rug pull та exit-схеми — ліквідація ліквідності протоколу після збору коштів; фішинг і drainware-атаки — шахрайські сайти або контракти, що крадуть активи користувачів; помпи-і-зливи та фінансові піраміди[1]. Такі схеми є проявом системних слабкостей децентралізованого фінансового середовища.

Хоч DeFi і має на меті ліквідацію посередників, саме його архітектура створює унікальні ризики. Складність смарт-контрактів робить їх вразливими: будь-який логічний недолік може бути експлуатований зловмисниками. Псевдонімні транзакції ускладнюють ідентифікацію зловмисників та правову

відповідальність. Децентралізація нерідко означає відсутність правил щодо захисту інвесторів і вимог до аудиту безпеки коду. Це створює вакуум, що дозволяє шахрайським структурам розвиватись без належного нагляду [2].

Для підвищення кіберстійкості DeFi-систем ключову роль відіграють інструменти аналізу blockchain-даних та форензики. Аналітика транзакцій дозволяє виявляти аномальні патерни — величезні або часті переміщення токенів, що можуть свідчити про шахрайську діяльність. Кластеризація гаманців допомагає пов'язувати адреси зі спільними характеристиками і ідентифікувати мережі шахраїв навіть в умовах псевдонімності. Аудити коду смарт-контрактів дозволяють виявляти вразливості до атак, що можуть використовуватись у rug pull чи інших схемах. Машинне навчання на основі моделей поведінки дозволяє автоматично і в реальному часі виявляти потенційні загрози до їх реалізації [1].

Загальний висновок полягає в тому, що захист DeFi-екосистем потребує мультидисциплінарного підходу, що включає технічні інструменти, освіту користувачів та розвиток нормативної бази. Необхідне впровадження систем автоматичного моніторингу транзакцій, обов'язкові аудити смарт-контрактів перед запуском, підвищення цифрової грамотності інвесторів та розроблення правових механізмів реагування на криптозлочини - це заходи, що сприятимуть безперервності бізнесу і підвищуватимуть кіберстійкість цифрових фінансових продуктів [2].

Література

1. Crypto Scam Types and How Blockchain Forensics Helps Detect and Disrupt URL: https://www.trmlabs.com/resources/blog/14-crypto-scam-types-and-how-blockchain-forensics-helps-detect-and-disrupt-them

2. Cybersecurity in Telecom Industry. URL:https://searchinform.com/articles/cybersecurity/industry/cybersecurity-in-telecom-industry/

РОЛЬ ПІДХОДУ DEVSECOPS У ПРОТИДІЇ КІБЕРАТАКАМ НА БІЗНЕС-СЕРВІСИ КОМПАНІЇ

Кухарчук В. В.
Державний університет інформаційно-комунікаційних технологій
м. Київ, Україна

Стрімка цифровізація бізнес-процесів та перехід до хмарних технологій зумовили безпрецедентне зростання кількості та складності кібератак на корпоративні системи. Сучасна інженерія програмного забезпечення вимагає високої швидкості постачання нових функцій (Time-to-Market), що часто призводить до конфлікту між швидкістю розробки та рівнем безпеки. Традиційні підходи, за яких тестування на вразливості відбувається на фінальних етапах життєвого циклу розробки програмного забезпечення (SDLC), виявилися неефективними. Виявлення критичних вразливостей після релізу або на етапі тестування перед розгортанням вимагає значних фінансових та часових ресурсів на їх усунення [1, с. 112].

Вирішенням цієї проблеми є впровадження методології DevSecOps (Development, Security, and Operations) – практики, що передбачає інтеграцію інструментів та процесів безпеки на кожному етапі конвеєра CI/CD (Continuous Integration / Continuous Deployment). Основною парадигмою DevSecOps є принцип "Shift-Left", який означає перенесення перевірок безпеки на якомога більш ранні етапи розробки: від етапу планування архітектури та написання коду до розгортання та моніторингу в середовищі експлуатації [2].

Для розуміння ефективності впровадження DevSecOps як стратегії протидії кібератакам, доцільно порівняти її з традиційним підходом до розробки (Табл. 1).

Економічну та ризик-орієнтовану доцільність переходу до DevSecOps можна обґрунтувати через зниження очікуваних фінансових втрат від

потенційних кіберинцидентів. В управлінні ризиками кібербезпеки ключовим показником є очікувана річна втрата (Annualized Loss Expectancy, ALE).

Таблиця 1

Порівняння традиційного підходу до безпеки ПЗ та методології DevSecOps

Характеристика	Традиційна безпека (Siloed Security)	Підхід DevSecOps
Етап перевірки	Наприкінці циклу розробки (перед релізом)	Безперервно на всіх етапах SDLC
Інструментарій	Ручне тестування на проникнення (Pen-testing)	Автоматизовані сканери (SAST, DAST, SCA)
Відповідальність	Виключно відділ інформаційної безпеки	Розподілена між розробниками, DevOps та безпековими інженерами
Вплив на швидкість	Затримує релізи, створює "вузькі місця"	Дозволяє підтримувати швидкий темп релізів завдяки автоматизації

Модифікувавши базову формулу оцінки ризиків, ефективність впровадження інструментів DevSecOps (E_{DSO}) можна розрахувати наступним чином:

$$ALE_{residual} = SLE * ARO * (1 - E_{DSO}) \quad (1)$$

де: $ALE_{residual}$ – залишковий фінансовий ризик (очікувані втрати) після впровадження засобів автоматизованої перевірки коду;

SLE (Single Loss Expectancy) – очікуваний розмір збитків від одного успішного кіберінциденту (наприклад, витоку бази даних користувачів);

ARO (Annualized Rate of Occurrence) – очікувана частота реалізації загрози протягом року;

E_{DSO} – коефіцієнт ефективності практик DevSecOps (значення від 0 до 1), який відображає відсоток вразливостей, автоматично заблокованих на етапі збирання та тестування коду (наприклад, за допомогою засобів Static Application Security Testing).

Завдяки впровадженню інструментів статичного (SAST) та динамічного аналізу (DAST), а також аналізу композиції програмного забезпечення (SCA), компанії отримують змогу блокувати атаки типу SQL Injection, Cross-Site

Scripting (XSS) та використання вразливих open-source бібліотек ще до того, як код потрапить на продуктивні сервери. Це безпосередньо впливає на показник E_{DSO}, наближаючи залишковий ризик до прийнятного рівня [3; 4].

Таким чином, у контексті сучасних кіберзагроз, забезпечення безперервності бізнес-сервісів неможливе без трансформації процесів розробки ПЗ. Впровадження методології DevSecOps виступає фундаментальною стратегією протидії кібератакам. Автоматизація перевірок безпеки та інтеграція їх у CI/CD процеси дозволяє не лише превентивно усувати критичні вразливості, але й оптимізувати витрати компанії на усунення наслідків інцидентів інформаційної безпеки, забезпечуючи при цьому кіберстійкість підприємства на архітектурному рівні.

Література

1. Корченко О. Г., Казмірчук С. В., Гнатюк С. О. Основи кібербезпеки: навчальний посібник. Київ: НАУ, 2019. 256 с.

2. Myrbakken H., Colomo-Palacios R. DevSecOps: A Multivocal Literature Review. Software Quality Journal. 2017. Vol. 25, No. 2. P. 125–150.

3. ДСТУ ISO/IEC 27005:2019 (ISO/IEC 27005:2018, IDT). Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки. Київ: ДП «УкрНДНЦ», 2020. 60 с.

4. DevSecOps: Integrating Security into the DevOps Cycle. OWASP Foundation. URL: https://owasp.org/www-project-devsecops/

СЕКЦІЯ 6. БЕЗПЕКА ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ КОМПАНІЇ

БЕЗПЕКА КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Берсим А. В.
Державний університет інформаційно-комунікаційних технологій
м. Київ, Україна

Забезпечення безпеки критичної інформаційної інфраструктури в умовах сучасних кіберзагроз вимагає комплексного підходу, що ґрунтується на детермінованих методах захисту. Відмова від використання неперевірених алгоритмів у стратегічно важливих вузлах дозволяє уникнути ризиків «чорної скриньки» та забезпечити повну прозорість процесів прийняття рішень щодо блокування трафіку. Замість нейронних мереж пропонується використовувати багаторівневу модель захисту, що базується на жорстких правилах фільтрації та сигнатурному аналізі відомих вразливостей.

Сигнатурний аналіз та антивірусний захист.

Метод перевірки контрольних сум (хешів) файлів та пошук специфічних послідовностей байтів, притаманних шкідливому ПЗ. Перевага у високій швидкісті обробки та відсутність хибних спрацювань на легітимне ПЗ. Неефективність проти атак «нульового дня» (0-day), які ще не внесені до баз.

Ешелонування мережі та міжмережеве екранування (Firewalling).

Використання міжмережевих екранів для контролю трафіку на рівнях L3-L4 та L7 (Application Layer). Створення «демілітаризованих зон» (DMZ) для зовнішніх сервісів. Найбільш критичні вузли (наприклад, системи управління енергомережами) не повинні мати жодного фізичного зв'язку з інтернетом.

Системи виявлення та запобігання вторгненням (IDS/IPS).

Аналізатор мережевого трафіку шукає аномалії, що відповідають

конкретним сценаріям атак, як-от спроби перебору паролів (brute-force) або SQL- ін'єкції. При виявленні підозрілої активності IPS автоматично розриває TCP- з’єднання або перенаправляє трафік у «пастку» (Honeypot).

Криптографічний захист та контроль цілісності.

Регулярне сканування системних файлів за допомогою утиліт (наприклад, Tripwire), які порівнюють поточні стани файлів з еталонними знімками. Використання лише сертифікованих державою алгоритмів для захисту каналів зв'язку між підрозділами.

Таблиця 1

Порівняння традиційних методів захисту

Метод захисту	Об'єкт захисту	Основний інструмент
Сигнатурний	Кінцеві точки (ПК, сервери)	Антивіруси, EDR
Мережевий	Периметр КІІ	Firewall, IDS/IPS
Організаційний	Персонал	Регламенти доступу, парольна політика
Криптографічний	Канали передачі даних	VPN (IPsec), TLS

Література

1. Про критичну інфраструктуру : Закон України від 16.11.2021 р. № 1882-IX. Редакція від 01.01.2026. URL: https://zakon.rada.gov.ua/laws/show/1882-20 (дата звернення: 24.02.2026).

2. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. Редакція від 20.05.2025. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 24.02.2026).

3. Çakır A. M. Conventional Methods in Cybersecurity Infrastructure. Human Computer Interaction. 2024.Vol.8,no. 1. P. 119. URL: https://doi.org/10.62802/jg7gge06

4. ДСТУ ISO/IEC 27001:2023. Інформаційні технології. Методи захисту. Системи менеджменту інформаційної безпеки. Вимоги (ISO/IEC 27001:2022, IDT). Київ : ДП «УкрНДНЦ», 2023. 32 с.

ВПЛИВ СУЧАСНИХ КІБЕРЗАГРОЗ НА РОЗВИТОК ТА ЗАХИСТ ІНФОРМАЦІЙНИХ СИСТЕМ ДЕРЖАВНИХ УСТАНОВ УКРАЇНИ

Коршиков О. В.

Державний університет інформаційно-комунікаційних технологій

Київ, Україна

Розвиток цифровізації державного управління в умовах воєнної агресії проти України стикнувся з проблемою забезпечення кібербезпеки державних інформаційних систем. Впровадження цифрових сервісів та інтеграція державних реєстрів значно підвищують ефективність функціонування органів влади, однак водночас збільшують площу для атаки кіберзловмисників. Розвиток цифрової екосистеми державних послуг, таких як платформа Дія чи Резерв+, зумовлює необхідність підвищення кіберстійкості всіх рівнів державних інформаційних систем. Сучасні кіберзагрози мають комплексний, багатовекторний характер і останнім часом спрямовані не стільки на отримання фінансової вигоди, скільки на дестабілізацію державного управління, порушення функціонування критичної інфраструктури та підрив довіри громадян до державних інституцій. З огляду на те, що кібервійна вже перейшла у фазу систематичного виснаження інфраструктури, сучасні кіберзагрози стали каталізатором і вимагають від держави радикальних змін у підходах до захисту та впровадження нових архітектурних рішень і глибокої міжнародної інтеграції.

Державні установи України є об’єктами постійних цілеспрямованих атак. Найбільш небезпечними серед них є Advanced Persistent Threats (APT), які представляють собою складні, довготривалі атаки, спрямовані на глибоке проникнення в урядові мережі з метою шпигунства, викрадення чутливих даних або критичного саботажу. Такі атаки зазвичай поєднують таргетовану соціальну інженерію, експлуатацію вразливостей нульового дня та маскування трафіку, що робить їх виявлення серйозним викликом для традиційних систем державного кіберзахисту. Особливо небезпечними залишаються деструктивні

атаки із застосуванням шкідливого програмного забезпечення типу Wiper, призначеного для безповоротного знищення даних. Метою таких операцій є максимальна дестабілізація, а не фінансова вигода. Характерним прикладом є діяльність угруповання Sandworm, яке пов'язують із підрозділами ГРУ РФ. Це угрупування здійснювало атаки на енергетичну інфраструктуру та державні інформаційні ресурси України, застосовуючи інструменти для повного виведення систем із ладу. За даними Держспецзв'язку та CERT-UA, кількість ворожих атак невпинно зростає: лише у 2025 році було опрацьовано майже 6000 кіберінцидентів (зростання на 37% порівняно з попереднім роком). Найбільшого удару зазнають місцеві органи влади (понад 35% інцидентів), урядові організації (близько 20%) та сектор безпеки і оборони [1]. Фішинг залишається ключовим вектором первинного доступу, що експлуатує людський фактор держслужбовців через маніпулятивні повідомлення, часто виступаючи першим етапом масштабної APT-атаки. Така тактика зловмисників, як масове розповсюдження шкідливого ПЗ через фішинг (кількість якого подвоїлася у 2025 році), стала основним інструментом проникнення [1]. Наочним прикладом наслідків таких загроз стала масштабна кібератака на бази Міністерства юстиції у грудні 2024 року, яка тимчасово заблокувала роботу близько 60 державних реєстрів (зокрема систему е-нотаріату та систему «Банкрутство і неплатоспроможність») і паралізувала надання послуг, пов'язаних з верифікацією даних [2].

Постійний тиск кіберзагроз став каталізатором модернізації державних інформаційних систем. Один із ключових напрямів трансформації — це перехід від периметрової моделі безпеки до концепції «Нульової довіри» (Zero Trust Architecture, ZTA). Цей підхід фокусується на захисті даних і передбачає мікросегментацію мереж, жорсткий контроль доступу та постійний поведінковий моніторинг (наприклад, виявлення нетипової активності користувачів у неробочий час чи необґрунтованих з'єднань із зовнішніми IP-адресами) [3][4]. Також зросла увага до створення та розвитку центрів моніторингу безпеки (SOC), впровадження систем управління інформаційною

безпекою (ISMS) і міжнародних стандартів, зокрема ISO/IEC 27001 та NIST-орієнтованих моделей. Також державні установи активно впроваджують багатофакторну автентифікацію, централізоване журналювання подій та інструменти виявлення вторгнень (IDS/IPS). Завдяки змінам у законодавстві щодо використання хмарних технологій державні органи отримали можливість розміщувати дані в закордонних дата-центрах провідних постачальників, зокрема Amazon Web Services, Microsoft Azure та Google Cloud. Це забезпечило фізичне збереження реєстрів у період ракетних атак та підвищило рівень географічного резервування. Одним із важливих елементів побудови кіберстійких інформаційних систем є створення внутрішніх підрозділів із кіберзахисту в державних установах. На виконання вимог закону «Про основні засади забезпечення кібербезпеки України» [8] Адміністрація Держспецзв'язку затвердила методичні рекомендації, які визначають типові вимоги до таких підрозділів і їх керівників. Вони охоплюють формування положень про підрозділ, завдання та функції, стандарти внутрішніх політик кібербезпеки, регламентів і інструкцій, а також контроль за їх виконанням і впровадженням планів кіберзахисту установи. Такий підрозділ має здійснювати оцінювання ризиків, визначати вимоги до захисту інформації і впроваджувати заходи з кіберзахисту відповідно до кращих практик міжнародних стандартів (NIST, ISO/IEC) і настанов регулятора. Важливо, що керівник підрозділу з кіберзахисту (CISO) повинен мати відповідні кваліфікаційні рівні та професійний досвід у сфері кібербезпеки і не може суміщати цю посаду з функціями цифрової трансформації чи цифрового розвитку органу влади. Це забезпечує профільну спрямованість функцій і незалежну оцінку безпекових ризиків.

Однією з критичних проблем в державному секторі все ще залишається нестача кваліфікованих фахівців із кібербезпеки, дефіцит яких згідно з оцінками може сягати сотень тисяч професіоналів. Це створює значні виклики для державних структур при формуванні ефективної системи захисту інформаційних систем. Для підвищення якості підготовки кадрів

Держспецзв’язку разом із Національним агентством із забезпечення якості вищої освіти впроваджує національні рамки професійних кваліфікацій у сфері кібербезпеки. Уже розроблено та затверджено нові професійні стандарти, які визначають кваліфікаційні вимоги та компетенції для окремих спеціалістів, таких як аналітики оцінювання ризиків, експерти з критичної інфраструктури та спеціалісти з забезпечення стійкості. Це дозволяє уніфікувати навчальні програми та встановити чіткі вимоги до сертифікації фахівців, здобутої як у вищій освіті, так і під час практичної підготовки.

Крім того, Україна активно гармонізує своє законодавство з європейськими стандартами кібербезпеки (зокрема з вимогами директиви ЄС NIS2). Завдяки новим законодавчим ініціативам (як-от Закону України №4336), розпочалося створення секторальних і регіональних команд реагування на кіберінциденти (CSIRT), що суттєво підвищує загальний рівень кіберстійкості держави та децентралізує захист [5]. Важливим кроком до розвитку державних ІТ-систем стала безпрецедентна міжнародна координація. З кінця 2023 року функціонує Талліннський механізм — коаліція з понад 10 країн-партнерів (зокрема США, Великої Британії, Естонії, Німеччини та ін.), що координує зусилля та фінансування для посилення цивільної кібербезпеки України [6]. Щоб зробити взаємодію ще ефективнішою, на початку 2026 року заплановано повноцінний запуск *Tallinn Mechanism Platform* — цифрової платформи, яка об'єднає донорів, державні інституції та приватний сектор (tech-бізнес) для реалізації спільних проєктів, участі в тендерах та швидкого впровадження інновацій у держсектор [7].

Попри позитивні тенденції модернізації, існує низка системних проблем. По-перше, значна частина державних установ експлуатує застарілу ІТ-інфраструктуру, що не відповідає сучасним вимогам безпеки. По-друге, нестача коштів гальмує впровадження сучасних технологій захисту та регулярні аудити безпеки. Не менш важливим чинником залишається людський фактор — недостатній рівень обізнаності персоналу щодо кібергігієни та правил безпечної роботи з інформаційними ресурсами.

Сучасні кіберзагрози суттєво трансформують підходи до розвитку та захисту інформаційних систем державних установ України, формуючи нові вимоги не лише до технологій, але й до організаційної структури та професійної підготовки кадрів. Створення підрозділів кіберзахисту, затвердження чітких вимог до їх функціонування та сертифікація фахівців виступають ключовими елементами підвищення кіберстійкості національної цифрової інфраструктури. Ефективна протидія кіберзагрозам потребує комплексного підходу, який об'єднає технічні рішення, управлінські механізми, нормативне забезпечення та системну освіту персоналу. У такому контексті кібербезпека стає невід'ємною частиною національної безпеки України.

Література

1. CERT-UA у 2025 році опрацювала майже 6000 кіберінцидентів: кількість ворожих атак зросла на 37% : звіт Держспецзв'язку. Січень 2026 р. URL: https://cip.gov.ua/ua/news/cert-ua-u-2025-roci-opracyuvala-maizhe-6000-kiberincidentiv-kilkist-vorozhikh-atak-zrosla-na-37

2. Кібератака на державні реєстри України (грудень 2024 р.) : Вікіпедія / Звіти щодо кіберінцидентів. URL: https://uk.wikipedia.org/wiki/Кібератака_на_державні_реєстри_України_(2024)

3. Атаки через ланцюжки постачань: формуючи стратегічну відповідь (Аналіз впровадження Zero Trust Architecture) : аналітична записка. Національний інститут стратегічних досліджень. 2025. URL: https://www.niss.gov.ua/sites/default/files/2022-06/ad_cyberresill_structure_var8_new_ed_01_gotove_0.pdf

4. Кібератаки в Україні: зростання на 70% та як захистити бізнес у 2025 році (Практика застосування ZTA) : аналітика Softlist. 2025. URL: ttps://softlist.ua/cases/cyberattacksinukraine

5. Фішинг, Zero Click-експлойти, AI-атаки: тенденції кіберзагроз в Україні у 2025 році (Про Закон №4336 та CSIRT) : звіт IT Ukraine Association.

2025. URL: https://itukraine.org.ua/fishing-zero-click-eksplojti-ai-ataki-tendentsiyi-kiberzagroz-v-ukrayini-u-2025-rotsi/

6. Два роки Талліннського механізму: системна міжнародна підтримка кіберстійкості України : офіційний портал КМУ / Мінцифри. Грудень 2025 р. URL: https://www.kmu.gov.ua/news/dva-roky-tallinnskoho-mekhanizmu-systemna-mizhnarodna-pidtrymka-kiberstiikosti-ukrainy

7. Талліннський механізм: два роки системної міжнародної підтримки (Анонс запуску Tallinn Mechanism Platform у 2026 році) : Digital State UA. 2026. URL: https://digitalstate.gov.ua/uk/news/govtech/tallinn-mechanism-two-years-of-coordinated-international-support-for-ukraines-cyber-resilience

8. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інфраструктури : Закон України від 27 берез. 2025 р. № 4336-IX. Офіційний портал Верховної Ради України. URL https://zakon.rada.gov.ua/laws/show/4336-20#Text

ФОРМУВАННЯ СТРАТЕГІЇ ІНФОРМАЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Кривов'яз І. Я.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

Забезпечення безпеки об'єктів критичної інфраструктури (далі – ОКІ) в умовах стрімкого розвитку цифрових технологій та збільшення кількості та складності загроз є важливим елементом національної безпеки, оскільки безпосередньо впливає на стабільність економічної, соціальної та оборонної сфери. Процес формування дієвої стратегії інформаційної та кібербезпеки на рівні об'єкта не може бути ефективним без належного аналітичного підґрунтя,

яким виступають результати регулярних аудитів інформаційної безпеки та комплексного оцінювання ризиків інформаційної безпеки. Саме це дозволяє трансформувати загальні вимоги у конкретний, пріоритезований план заходів, адаптований до реальних загроз та технічного стану ОКІ.

Формування стратегії на рівні об’єкта починається з чіткого дотримання нормативних вимог, які за останні роки зазнали суттєвих змін. Базовим документом, що регламентує технічні та організаційні аспекти, є Постанова Кабінету Міністрів України від 19 червня 2019 р. № 518 «Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури». Проте, враховуючи динаміку загроз, у листопаді 2025 року було прийнято Постанову № 1470 «Про внесення змін до постанови Кабінету Міністрів України від 19 червня 2019 р. № 518», яка виклала ці вимоги у новій редакції, акцентуючи увагу на обов'язковому управлінні ризиками кібербезпеки та забезпечені безперервного моніторингу.

При формуванні стратегії інформаційної та кібербезпеки оператори ОКІ орієнтуються на глобальні стандарти, зокрема на оновлений у 2024 році NIST Cybersecurity Framework (далі – NIST CSF) 2.0. Головною особливістю нової версії є її універсальність та додання функції «Govern», яка тепер пронизує всі аспекти кіберзахисту.

Функція «Управління» (Govern) є центральною, оскільки вона визначає політику та стратегію управління ризиками, в той час як класична для попередньої версії фреймфорку функція «Ідентифікація» (Identefication) дозволяє зрозуміти поточні ризики для бізнес-процесів, активів та даних. У цьому контексті аудит безпеки виступає одним з основних методів збору об'єктивних даних про наявні активи, їх вразливості та релевантні загрозі, а також реальний стан захищеності ОКІ.

Без глибокого розуміння поточного стану інформаційної безпеки, отриманого в ході аудиту, процес формування стратегії неминуче перетворюється на формальне виконання нормативних вимог. Такий підхід створює ілюзію безпеки на папері, але не забезпечує реальної стійкості ОКІ. Саме результати аудиту дозволяють побудувати «Поточний профіль» та

визначити «Цільовий профіль», що є основою для формування стратегії з акцентом на слабких місцях які вона має усунути в першу чергу.

Не менш важливим аспектом формування стратегії інформаційної та кібербезпеки є оцінка ризиків. Сучасна методологія пропонує два основні підходи до оцінки: кількісний та якісний. Кількісні методи (quantitative) базуються на використанні конкретних числових значень, фінансових показників потенційних втрат та математичних розрахунках ймовірності. Проте для ОКІ, де наслідки інциденту часто виходять за межі економічних показників і торкаються національної безпеки, застосування чисто кількісних моделей може бути ускладненим.

Натомість якісний підхід (qualitative) орієнтований на використання порядкових шкал (від «дуже низький» до «дуже високий») та експертних оцінок. Саме якісна методика є найбільш гнучкою та адаптивною для ОКІ, оскільки вона дозволяє оперативно реагувати на зміни у ландшафті загроз в умовах невизначеності та воєнного стану. Вона дає змогу врахувати не лише ймовірність і вплив, а й складніші фактори, такі як цінність активу, рейтинг загрози та вразливість системи, не вимагаючи при цьому надлишкових статистичних даних, які можуть бути недоступними.

Завдяки використанню комплексного підходу, аудит і оцінка ризиків перетворюються з формальних заходів контролю на динамічний інструмент управління стійкістю. Якщо аудит визначає фактичні межі «Поточного профілю», то якісна оцінка ризиків виступає фільтром, що дозволяє визначити черговість кроків до «Цільового профілю». Це забезпечує формування чіткої стратегії, де ресурси інвестуються не у випадкові технології, а в цілеспрямоване усунення найбільш небезпечних прогалин у захисті.

Література

1. Закон України «Про критичну інфраструктуру» від 16.11.2021 р. № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20

2. NIST Cybersecurity Framework (CSF) 2.0. URL: https://www.nist.gov/cyberframework

3. Постанова КМУ від 19.06.2019 № 518 (в редакції від 13.11.2025 № 1470). URL: https://ips.ligazakon.net/document/MN030699

4. Наказ Адміністрації Держспецзв'язку від 14.01.2025 № 17 «Про затвердження Методики та Критеріїв і показників оцінки стану захищеності об'єктів критичної інфраструктури». URL: https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-14-sichnya-2025-roku-17-pro-zatverdzhennya-metodiki-ta-kriteriyiv-i-pokaznikiv-ocinki-stanu-zakhishenosti-ob-yektiv-kritichnoyi-infrastrukturi

МЕТОДИ ЗАСТОСУВАННЯ СТАНДАРТУ ISO/IEC 27001 В ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Лоза О. Д.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

Інформаційна безпека є критично важливим аспектом функціонування сучасних організацій. Одним із найефективніших інструментів для забезпечення безпеки даних є стандарт ISO/IEC 27001, який встановлює вимоги до системи управління інформаційною безпекою (СУІБ) [1]. Для об'єктів критичної інфраструктури (ОКІ) застосування цього стандарту вимагає специфічних методів, що враховують високі ризики порушення доступності сервісів та цілісності технологічних процесів. СУІБ дозволяє створити системний підхід, де технології, процеси та персонал працюють як єдиний захисний контур.

Ризик-орієнтований метод управління безпекою ОКІ. В основі стандарту ISO/IEC 27001 лежить процес оцінки та обробки ризиків. Для об'єктів критичної інфраструктури застосовуються наступні методичні підходи:

- Ідентифікація критичних активів: визначення інформаційних систем та технологічних мереж (ОТ), вихід з ладу яких може спричинити техногенну або соціальну катастрофу.
- Метод оцінки впливу: аналіз ризиків проводиться не лише з точки зору фінансових втрат , а й з позиції національної безпеки та безперервності надання послуг [2].
- Пріоритезація заходів контролю: вибір засобів захисту із Додатка А стандарту, які в першу чергу забезпечують стійкість систем до кібератак.

Методи забезпечення технічної та експлуатаційної стійкості. Застосування стандарту на ОКІ передбачає інтеграцію технічних заходів у загальну систему управління:

- Контроль доступу та моніторинг: впровадження суворих політик управління доступами, зокрема принципу "найменшого необхідного доступу"[3].
- Керування вразливостями: регулярна оцінка захищеності мереж та використання оновлених баз даних про кіберзагрози (Threat Intelligence).
- Забезпечення безперервності бізнесу: розробка та тестування планів відновлення після інцидентів (Disaster Recovery) [4], що є обов'язковою вимогою для стабільної роботи критичних систем.

Стратегічне управління та культура безпеки. Ефективне впровадження СУІБ на стратегічних об'єктах неможливе без системного підходу до управління організаційними змінами:

- Лідерство та відповідальність: вище керівництво ОКІ має демонструвати важливість інформаційної безпеки для стабільності підприємства.
- Прозора комунікація: створення надійних механізмів для швидкого повідомлення про потенційні загрози та аномалії в роботі систем[5].
- Контроль ланцюга постачання: перевірка безпеки обладнання та програмного забезпечення від сторонніх постачальників згідно з вимогами оновленого стандарту 2022 року.

Література

1. ISO/IEC 27001:2022. Інформаційні технології – Методи забезпечення безпеки – Системи управління інформаційною безпекою – Вимоги. Женева: Міжнародна організація зі стандартизації, 2022. 40 с. URL:https://www.iso.org/standard/27001
2. Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX (зі змінами від 22.08.2024). Відомості Верховної Ради України. 2023. № 5. ст. 13. URL: https://zakon.rada.gov.ua/laws/show/1882-20
3. ISO/IEC 27002:2022. Інформаційні технології. Методи захисту. Кодекс практики для заходів інформаційної безпеки. Женева: ISO, 2022.
4. NIST Special Publication 800-82 Rev. 3. Guide to Operational Technology (OT) Security. Вашингтон: National Institute of Standards and Technology, 2023. URL: https://csrc.nist.gov/publications/detail/sp/800-82/rev-3/final
5. ENISA. Good Practices for Security of Critical Information Infrastructures. Афіни: European Union Agency for Cybersecurity, 2022. 85 с. URL: https://www.enisa.europa.eu/publications

МЕТОДИ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ПОДІЙ БЕЗПЕКИ ДЛЯ ПІДВИЩЕННЯ КІБЕРСТІЙКОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Наріжна І. В.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

Анотація. У тезах розглянуто застосування методів інтелектуального аналізу подій безпеки для підвищення кіберстійкості об'єктів критичної інформаційної інфраструктури. Запропоновано підхід, що поєднує кореляцію подій, виявлення аномалій і ризик-орієнтовану пріоритизацію інцидентів.

Показано, що використання такого підходу дає змогу підвищити якість виявлення кіберзагроз, зменшити кількість хибнопозитивних спрацювань і скоротити час реагування на інциденти.

Ключові слова: кіберстійкість, критична інформаційна інфраструктура, події безпеки, інтелектуальний аналіз, виявлення аномалій, кореляція подій, SIEM, кіберінцидент.

Актуальність теми зумовлена зростанням кількості та складності кібератак на об’єкти критичної інформаційної інфраструктури та необхідністю забезпечення безперервності функціонування критичних сервісів. Для таких об’єктів своєчасне виявлення та аналіз подій безпеки є ключовою умовою підвищення кіберстійкості, оскільки інциденти можуть призводити до порушення надання послуг, втрати даних і зростання операційних ризиків [1], [2].

Сучасні підходи до управління кіберризиками та реагування на інциденти орієнтують організації на побудову безперервного процесу виявлення, аналізу, реагування та відновлення. У цьому контексті важливими є рекомендації NIST CSF 2.0 і NIST SP 800-61 Rev. 3, які підкреслюють необхідність інтеграції моніторингу, контекстуалізації подій та ризик-орієнтованого прийняття рішень [3], [4]. Для опису поведінки зловмисників і побудови сценаріїв детектування доцільно використовувати матрицю MITRE ATT&CK [5].

Традиційні rule-based механізми SIEM ефективні для виявлення відомих сценаріїв атак, проте мають обмеження щодо багатокрокових, малопомітних та модифікованих технік. Тому перспективним є застосування методів інтелектуального аналізу подій безпеки, що поєднують статистичне профілювання, виявлення аномалій, кореляцію подій та пріоритизацію інцидентів. Такий підхід дає змогу зменшити кількість хибнопозитивних спрацювань і підвищити якість виявлення складних атак [4], [5], [7].

Запропонований підхід передбачає багаторівневу обробку подій безпеки: збір і нормалізацію телеметрії з різних джерел (мережеве обладнання, сервери, засоби захисту, журнали автентифікації, EDR/NDR), формування контексту події (критичність активу, роль користувача, сегмент мережі, відповідність технікам

ATT&CK), інтелектуальну кореляцію та виявлення аномалій, а також ризик-орієнтовану пріоритизацію інцидентів для передавання на реагування. Для оцінювання ефективності доцільно використовувати показники MTTD, MTTR, частку хибнопозитивних спрацювань і точність пріоритизації [3], [4], [6].

Отже, поєднання rule-based кореляції з методами інтелектуального аналізу подій безпеки є доцільним напрямом підвищення кіберстійкості об'єктів КІІ. Практична цінність підходу полягає у підвищенні якості детектування, зниженні навантаження на аналітиків та підтримці більш обґрунтованого реагування на кіберінциденти.

Таблиця 1

Методи інтелектуального аналізу подій безпеки та їх застосування для підвищення кіберстійкості

Метод / засіб	Тип загрози	Що виявляє	Заходи протидії
Rule-based кореляція (SIEM-правила)	Відомі техніки атак, порушення політик	Сигнатури, IOC, послідовності подій	Оновлення правил, use-cases, інтеграція ATT&CK
Виявлення аномалій (статистика/ML)	Невідомі або нетипові сценарії активності	Відхилення від базового профілю, аномальні входи/трафік	Тюнінг моделей, feedback аналітика, пороги ризику
Контекстна пріоритизація та скоринг інцидентів	Перевантаження SOC, хибнопозитивні спрацювання	Критичність активу, вплив, достовірність спрацювання	Risk-based triage, черговість реагування

Література

1. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1882-20

2. Деякі питання об'єктів критичної інформаційної інфраструктури : Постанова Кабінету Міністрів України від 09.10.2020 № 943 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF

3. NIST. The Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. 2024. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

4. NIST. Incident Response Recommendations and Considerations for Cybersecurity Risk Management (SP 800-61 Rev. 3). 2025. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf

5. MITRE ATT&CK. Enterprise Matrix (online resource). URL: https://attack.mitre.org/matrices/enterprise/

6. ENISA. 2024 Report on the State of Cybersecurity in the Union. 2024. URL: https://www.enisa.europa.eu/sites/default/files/2024-11/2024%20Report%20on%20the%20State%20of%20the%20Cybersecurity%20in%20the%20Union.pdf

7. Tendikov N. et al. Security Information Event Management data acquisition and machine learning methods for intrusion detection // Results in Engineering. 2024. URL: https://www.sciencedirect.com/science/article/pii/S2590123024005097

8. Sheeraz M. et al. Revolutionizing SIEM Security: An Innovative Correlation Engine and Attack Detection with ML // Sensors. 2024. URL: https://www.mdpi.com/1424-8220/24/15/4901

СЕКЦІЯ 7. ОСВІТА Й ОБІЗНАНІСТЬ, ФОРМУВАННЯ КУЛЬТУРИ КІБЕРБЕЗПЕКИ

ЛЮДСЬКИЙ ФАКТОР У КОНТЕКСТІ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ОРГАНІЗАЦІЇ

Бишук І. О.
Державний університет інформаційно-комунікаційних технологій
м. Київ, Україна

Майже всі коли-небудь вводили значення в неправильному полі форми, або робили просту помилку в обчисленнях, видаляли не той файл помилково. Всі припускаються помилок, і здебільшого просто приймаємо такі та подобні помилки як неминуче, а потім робимо все можливе, щоб виявити і усунути проблеми, поки ще не занадто пізно. Відносно контролю технічної безпеки, прості помилки конфігурації можуть залишити мережеві порти відкритими, брандмауери уразливими і системи повністю незахищеними. Насправді людська помилка, куди більш імовірно може привести до серйозних порушень безпеки, ніж технічні уразливості [1].

У рамках теорії організації інформаційної безпеки чітко визначено постулат, що організація інформаційної безпеки повинна враховувати не тільки складність техніко-технологічних складових системи, а й людський фактор. І відповідно, до цього вже на етапі проектування систем технічного та програмного захисту, необхідно враховувати не тільки технічний аспект а й кількісні та якісні індивідуальні характерологічні особливості персоналу. Наявність людського фактора має першорядне значення в теорії інформаційної безпеки. Головна, ключова роль у безпеці належить не машинам чи технологіям, а людині. Людський фактор, як такий залежить від багатьох, як внутрішніх так і зовнішніх, змінних а іноді може проявлятися у «ніби» нелогічних діях.

Навмисний відтік часто важко відрізнити від ненавмисного, але це не завжди необхідно, оскільки наслідки для підприємства в будь-якому з цих варіантів можуть бути катастрофічними.

Люди, які контролюють і використовують корпоративну мережу, є найбільш вразливою складовою цієї системи. Захист усієї системи часто перебуває в руках системного адміністратора. Якщо адміністратор не має достатнього рівня кваліфікації або вирішить стати на шлях злочину, то така система знаходиться в серйозній небезпеці.

Звичайних користувачів корпоративних мереж, операторів та інший персонал також можуть підкупити або змусити вчинити протиправні дії, що створює небезпечне середовище для захисту системи.

Категорія працівників, звільнених або понижених у посаді, особливо небезпечна. В комп'ютерній інформаційній діяльності ці працівники повинні перебувати під безпосереднім наглядом керівництва, особливо якщо персонал має право доступу до активного цінного інформаційного ресурсу. А у разі звільнення слід подбати, щоб особа більше не мала доступу до корпоративної інформації.

Основним захистом від внутрішніх ворогів є підтримка трудової дисципліни в колективі та встановлення особистого контакту між керівником та його підлеглими для подальшого вирішення проблем, а саме особистих конфліктів.

Найпоширенішими та найнебезпечнішими загрозами доступності є ненавмисні помилки звичайних користувачів, операторів, системних адміністраторів та інших, які користуються інформаційними системами чи їх обслуговують. Такі помилки зазвичай стають загрозами, іноді вони створюють вразливості, якими можуть скористатися зловмисники. Виходячи з цього, найрадикальнішим способом боротьби з ненавмисними помилками є максимальна автоматизація та суворий контроль [2].

Існує область науки, яка називається «Human Factors Engineering», вона прагне вирішити цю проблему. У деяких випадках, натискання «не тієї кнопки» може мати катастрофічні наслідки для безпеки. Є система блокування,

подвійне управління і автоматичні програмовані відгуки. Цілі групи моніторів стежать і постійно перевіряють систему, її операторів, і динамічний реагування на стані тривоги. Безпека критично важливих систем дуже важлива і досить надійна. І все ж, помилки все ще мають місце. Оператори електростанцій іноді натискають на неправильні кнопки, тим самим виключаючи системи, через що і відбуваються порушення в системах безпеки.

Підводячи підсумки, можна сказати, що інформаційна безпека є одночасно повністю людською та технологічною проблемою [1].

Література

1. Маслова Ю.Ю., Кушнір І.М. Інформаційна безпека і людський фактор. *ДУТ*. 2020.

URL: https://journals.dut.edu.ua/index.php/dataprotect/article/view/2462/2362

2. Заник О., Ткачук Р. Вплив людського фактору на системи організації інформаційної безпек. *ЛДУ БЖД*. 2020. URL: https://sci.ldubgd.edu.ua/jspui/bitstream/123456789/9704/1/7_Kon_2020.pdf

КІБЕРГІГІЄНА ТА ФОРМУВАННЯ КУЛЬТУРИ КІБЕРБЕЗПЕКИ СЕРЕД МОЛОДІ

Журавель А. В.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

Кібергігієна розглядається як щоденні прості дії для захисту персональних даних і пристроїв, яких слід дотримуватися кожному користувачу інтернету. Відсутність базових навичок безпечної поведінки онлайн значно підвищує ризик успішних кібератак. Так, експерти з CISA зазначають, що базова кібергігієна здатна запобігати до 98% кібератак, тому її

слід зробити звичкою, як чищення зубів або миття рук [1]. Водночас дослідження показують, що значна частина інцидентів пов’язана з соціальною інженерією та людською помилкою [2]. Це означає, що посилення обізнаності та навчання користувачів має стати першочерговою стратегією для безпеки, особливо серед молоді та студентів, які активно використовують цифрові технології [2, 3].

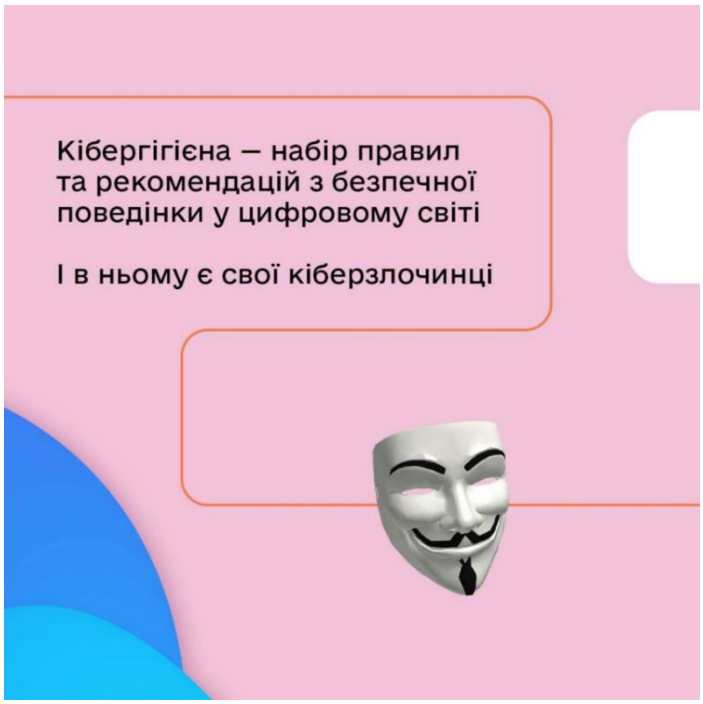

Рис 1. Визначення кібергігієни

На рис.1 показано, що кібергігієна – це “набір правил та рекомендацій з безпечної поведінки у цифровому світі”. Здобуття цих навичок має відбуватися через навчання та практичне застосування. Наразі в Україні запущено кілька національних інформаційно-освітніх кампаній з кібергігієни. Наприклад, у квітні 2024 року Міністерство освіти і науки разом з CRDF Global та партнерами розпочали всеукраїнську кампанію, що має на меті підвищити обізнаність громадян про онлайн-загрози та навчити основам кібергігієни [4]. Аналогічно, Дія.Освіта у вересні 2024 року анонсувала кампанію з кібергігієни за підтримки USAID, що охоплює підлітків, дорослих і літніх користувачів, і містить серіали-лекції та симулятори для закріплення знань [5].

1. Цілі та завдання кампанії

Основними цілями такої просвітницької кампанії є: формування правильної поведінки у цифровому середовищі, поширення навичок кібергігієни та створення базового рівня критичного мислення щодо онлайн-інформації. З одного боку, це захищає особисті дані студентів і працівників; з іншого – підвищує загальну кіберстійкість суспільства. Національний координаційний центр кібербезпеки при РНБО підкреслює, що кожен громадянин, незалежно від віку чи соціального статусу, повинен дбати про власну кібербезпеку, адже це напряму впливає на безпеку всієї країни [3]. Особливо актуальною ця тема є під час війни, коли підлітки часто довіряють інформації від російських блогерів і менш захищені від інтернет-шахрайств. Тому інформацію про кібербезпеку необхідно поширювати не лише в школах, але й у сім'ях та медіа [3].

До ключових завдань кампанії належать:

- Інформування – підвищити поінформованість про типові кіберзагрози (фішинг, шкідливе ПЗ, шахрайство) і шляхи їх уникнення.
- Навчання навичкам кібергігієни – сформувати такі практичні звички, як регулярна зміна паролів, перевірка надійності посилань і мережі Wi-Fi, оновлення програм і використання антивірусів [3, 5].
- Залучення молоді – розробити адаптовані освітні матеріали для школярів та студентів (пояснювальні відеосеріали, інтерактивні курси, симулятори інтернет-загроз) [5].
- Використання гейміфікації – мотивувати перевіряти знання через ігри та тести. Наприклад, на сайті кампанії доступна онлайн-гра-вікторина, що допомагає закріпити правила безпечної поведінки [4].

Реалізація включає мультиканальні підходи – лекції та тренінги в університетах і школах, дистанційні вебінари, соціальна реклама в мережах і ролики на телебаченні, а також інтерактивні серіали та симулятори. Дія.Освіта, зокрема, створила серіал «Кібергігієна для молоді», де на прикладах демонструють, чому важливо оновлювати ПЗ, використовувати антивіруси та двофакторну автентифікацію [5]. Для старших вікових груп розроблено окремі

серіали про захист мобільних пристроїв, безпечні онлайн-платежі і протидію фішингу. Крім того, у межах кампанії плануються серії соціальних відеороликів для різних аудиторій – від учнів до людей елегантного віку [5].

Управлінський аспект передбачає зобов'язання керівництва навчальних закладів і організацій: лідери повинні демонструвати важливість безпеки своїм прикладом, виділяти ресурси на тренінги та нагороджувати дотримання правил. Культура кібербезпеки будується «згори і знизу»: вісь зв'язок керівників і рядових користувачів, які розуміють, чому безпека є пріоритетом[6, 7]. Власне, професіонали радять регулярно оновлювати навчальні програми, практикувати симуляції кібератак (наприклад, фішинг-тести) і впроваджувати модель Zero Trust для мінімізації ризиків навіть у гібридному середовищі [7].

2. Основні правила кібергігієни

Головними рекомендаціями для учасників кампанії є формування таких звичок:

- Використання надійних паролів і MFA. Пароль має бути довгим, унікальним і містити цифри, літери різного регістру та символи. Двофакторна автентифікація (MFA) значно ускладнює несанкціонований доступ. Ці заходи критично важливі для захисту акаунтів [1].
- Регулярне оновлення ПЗ і антивірусний захист. Своєчасні оновлення закривають відомі вразливості систем. Антивірусні програми та брандмауери слід застосовувати як на комп'ютерах, так і на смартфонах і планшетах [5].
- Перевірка інформації. Перед тим як перейти за посиланням або ввести дані, необхідно перевіряти автентичність сайтів та повідомлень. Наприклад, фішингові листи можуть імітувати банки чи державні установи, тому важливо звертати увагу на адресу ресурсу і не довіряти підозрілим повідомленням [3, 5].
- Обережне використання Wi-Fi і публічних мереж. Під час роботи з конфіденційною інформацією небажано підключатися до незахищених відкритих мереж. Якщо необхідно користуватися публічним Wi-Fi, слід застосовувати віртуальні приватні мережі (VPN) або інші засоби шифрування [3].

- Освідомлене використання соцмереж і контенту. Молоді люди повинні усвідомлювати небезпеку завантаження невідомого програмного забезпечення та обмінюванняся даними з незнайомцями. Як відзначають в МОН, багато підлітків споживають інформацію з неперевірених російських джерел, що підвищує їхню вразливість до маніпуляцій [3].

Особливо важливо, щоб кампанія мала тривалий ефект: культура безпеки формується через постійне повторення меседжів. Власне, РНБО та партнери підкреслюють, що така інформаційна робота ведеться вже другий рік поспіль і постійно адаптується до нових загроз [3, 4]. Ключові матеріали доступні онлайн – всі правила і симулятори зібрані на порталі Дія.Освіта, що дозволяє кожному за бажання самостійно пройти навчання та перевірити знання [5].

Проведення просвітницької кампанії з елементами кібергігієни спрямоване на системне підвищення кіберстійкості суспільства через освіту. Фокус на молодь і студентів є особливо перспективним, адже саме вони формують майбутню культуру безпеки в Україні. Створення інтерактивних навчальних матеріалів, включення теми в шкільні та університетські курси, а також використання сучасних комунікаційних каналів дозволяють максимально захопити увагу аудиторії. Відповідно, системна кібергігієна поступово стає невід'ємною частиною щоденних звичок.

Отже, освітня кампанія з кібергігієни – це не разовий захід, а довготермінова інвестиція в цифрову грамотність суспільства.

Література

1. Association of Alaska School Boards (Patrick Massey, CISA). *Teaching Children to be Cyber Safe*. 2023. URL: https://aasb.org/commentary/teaching-children-to-be-cyber-safe/.

2. Armas, R., & Taherdoost, H. (2025). *Building a Cybersecurity Culture in Higher Education: Proposing a Cybersecurity Awareness Paradigm*. *Information*, 16(5), 336. URL: https://www.mdpi.com/2078-2489/16/5/336.

3. National Security and Defense Council of Ukraine. *Awareness-raising campaign to improve citizens' cyber hygiene launched in Ukraine*. 17.04.2024. URL: https://www.rnbo.gov.ua/en/Diialnist/6853.html.

4. Міністерство освіти і науки України. *Стартує інформаційно-освітня кампанія з кібергігієни*. 17.04.2024. URL: https://mon.gov.ua/news/startue-informatsiyno-osvitnya-kampaniya-z-kibergigieni.

5. Міністерство цифрової трансформації України. *Дія.Освіта та Проєкт USAID «Кібербезпека» запускають інформаційну кампанію з кібергігієни*. 16.09.2024. URL: https://thedigital.gov.ua/news/education/diyaosvita-ta-proekt-usaid-kiberbezpeka-zapuskayut-informatsiynu-kampaniyu-z-kibergigieni.

6. Lazarus Alliance. (2023). *Просування культури обізнаності про кібербезпеку у вашій організації*. 21.09.2023. URL: https://lazarusalliance.com/uk/promoting-a-culture-of-cybersecurity-awareness-in-your-organization/.

7. Smart Power. (2024). *Культура кібербезпеки*. 25.09.2024. URL: https://www.smartpower.com.ua/2024/09/25/kultura-kiberbezpeky/.

РОЛЬ КІБЕРГІГІЄНИ ТА БЕЗПЕРЕРВНОГО НАВЧАННЯ У ФОРМУВАННІ КОРПОРАТИВНОЇ КУЛЬТУРИ КІБЕРБЕЗПЕКИ

Курінний О. С.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

У сучасних умовах стрімкого розвитку цифрових технологій та зростання інтенсивності кібератак людський фактор залишається однією з найбільш критичних уразливостей у системі захисту будь-якої організації. Більшість успішних інцидентів інформаційної безпеки виникають не через відсутність технічних засобів захисту, а внаслідок ненавмисних помилок персоналу, що

підкреслює необхідність формування стійкої корпоративної культури кібербезпеки. Це зумовлено тим, що зловмисники все частіше фокусуються не на зламі програмного коду, а на психологічних маніпуляціях, намагаючись обійти технічні бар'єри через довіру або неуважність працівників. Основою такої культури є кібергігієна, яка передбачає систематичне дотримання працівниками базових правил цифрової безпеки, таких як використання складних паролів, обережне поводження з електронною поштою та розуміння складних механізмів сучасної соціальної інженерії [1].

Ефективне зміцнення кіберстійкості підприємства вимагає переходу від формальних разових інструктажів до концепції безперервного навчання. Практика свідчить, що регулярне оновлення знань у поєднанні з симуляціями фішингових атак дозволяє значно підвищити рівень обізнаності працівників та їхню здатність вчасно ідентифікувати загрози в реальному часі. Особливої уваги заслуговує впровадження гейміфікації в освітній процес, що дозволяє підвищити мотивацію персоналу та забезпечити краще засвоєння складного матеріалу через ігрові механіки, інтерактивні сценарії та квізи [2]. Такий підхід дозволяє інтегрувати безпеку в повсякденні бізнес-процеси, роблячи кожного співробітника активним учасником системи захисту периметра організації.

Окрім освітнього аспекту, важливим елементом культури кібербезпеки є створення середовища довіри, де працівники не бояться повідомляти про можливі інциденти або власні помилки. Психологічна готовність співробітника визнати випадкове натискання на підозріле посилання є критично важливою для компанії, адже приховування інциденту лише поглиблює ризики. Своєчасне інформування служби безпеки про підозрілу активність є ключовим чинником для швидкої локалізації загроз та мінімізації можливих збитків.

Таким чином, стратегічне управління ризиками, що базується на підвищенні обізнаності персоналу та впровадженні високих стандартів кібергігієни, є фундаментом забезпечення безперервності бізнесу в умовах постійних кіберзагроз [3].

Література

1. В. Є. Лучик, Д. Є. Власко. Фішингові атаки: як їх розпізнавати та уникати. URL: https://ibn.idsi.md/sites/default/files/imag_file/536-539_5.pdf?
2. Аналіз досвіду впровадження гейміфікації в освітній процес. Інститут цифровізації освіти НАПН України.
3. ENISA. Cyber Security Culture in organisations. Main requirements and model. URL: https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations

ПРОТИДІЯ КОГНІТИВНИМ ВИКРИВЛЕННЯМ ЯК ОСНОВА ФОРМУВАННЯ СУЧАСНОЇ КУЛЬТУРИ КІБЕРБЕЗПЕКИ

Кучерявенко Я. В.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

Когнітивні викривлення (cognitive biases) залишаються однією з головних причин успішних кібератак. За даними Verizon DBIR 2025 року, 74 % порушень безпеки, пов’язаних з соціальною інженерією, стали можливими саме через типові когнітивні упередження людей — confirmation bias, authority bias, urgency bias та anchoring effect [1].

Сучасні методи протидії цим викривленням виходять далеко за рамки традиційних тренінгів. Найефективнішими вважаються:

- дебайсинг-тренінги (structured debiasing training), які навчають розпізнавати власні упередження;
- nudging-техніки (поведінкові підказки), наприклад, автоматичні попередження «Ви впевнені, що хочете відкрити цей файл?»;
- gamification та імітаційні симуляції, де працівники в реальному часі бачать наслідки своїх когнітивних помилок.

Дослідження Ponemon Institute (2024) показало, що організації, які регулярно застосовують дебайсинг-програми, зменшують кількість успішних фішингових атак на 61 % порівняно з компаніями, що використовують лише стандартне навчання [2].

Формування сучасної культури кібербезпеки неможливе без системної роботи з когнітивними викривленнями персоналу. Культура безпеки — це не тільки правила та політики, а насамперед зміна мислення і поведінки людей.

Сьогодні передові компанії інтегрують протидію когнітивним викривленням у всі рівні корпоративної культури: від підбору персоналу (тести на когнітивну стійкість) до щоденних процесів (автоматичні поведінкові інтервенції). Особливо ефективним є поєднання психологічних методів з технічними рішеннями — так званий human firewall 2.0.

Відповідно до NIST Cybersecurity Framework 2.0 та рекомендацій ENISA, протидія когнітивним викривленням уже визнається одним із ключових елементів зрілої культури кібербезпеки [3]. Організації, які досягли високого рівня «bias awareness», демонструють значно вищу стійкість до соціальної інженерії та швидше відновлюються після інцидентів.

Протидія когнітивним викривленням є не додатковим заходом, а фундаментальною основою формування сучасної культури кібербезпеки. Перехід від традиційного «навчання правилам» до науково обґрунтованої роботи з когнітивними упередженнями дозволяє суттєво підвищити рівень захищеності організацій. У перспективі саме рівень зрілості систем протидії когнітивним викривленням стане одним із головних показників кіберзрілості компанії.

Література

1. Verizon. 2025 Data Breach Investigations Report [Електронний ресурс]. URL: https://www.verizon.com/business/resources/reports/dbir/ (дата звернення: 24.02.2026).

2. Ponemon Institute. 2024 Cost of a Data Breach Report [Електронний ресурс] / IBM Security. URL: https://www.ibm.com/security/data-breach (дата звернення: 24.02.2026).

3. National Institute of Standards and Technology. NIST Cybersecurity Framework 2.0 [Електронний ресурс]. Gaithersburg, 2024. URL: https://www.nist.gov/cyberframework (дата звернення: 24.02.2026).

ОСНОВНІ ЧИННИКИ ФОРМУВАННЯ КУЛЬТУРИ КІБЕРБЕЗПЕКИ ОРГАНІЗАЦІЇ

Легомінова С. В., д-р екон. наук, професор,
Мужанова Т. М., канд. наук з держ. упр., доцент,
Щавінський Ю. В., канд. техн. наук, доцент,
Родіонов В. Ю.
Державний університет інформаційно-комунікаційних технологій
м. Київ, Україна

В умовах динамічного ландшафту кіберзагроз та, як наслідок, значного зростання ризиків порушень кібербезпеки сучасні компанії постають перед викликом своєчасної реакції та швидкої адаптації своїх захисних стратегій. Для ефективної боротьби з цими кіберзагрозами компанії активно впроваджують передові технологічні рішення. Однак, для подолання негативного впливу людського чинника, який згідно з дослідженням компанії Verizon 2024-2025 років є причиною 74% кіберінцидентів [1], таких заходів недостатньо. Тому сьогодні все більше організацій починають усвідомлювати цінність сильної культури кібербезпеки, яка є ключовим інструментом людиноцентристських стратегій безпеки.

Концепція культури кібербезпеки базується на принципах організаційної культури й відповідно до визначення Європейського агентства з кібербезпеки

ENISA охоплює знання, переконання, сприйняття, ставлення, уявлення, норми й цінності людей щодо кібербезпеки та того, як вони проявляються в їх поводженні з інформаційним технологіями [2]. Культура кібербезпеки спрямована на те, щоб зробити питання кібербезпеки невід'ємною частиною роботи, звичок і поведінки працівників, вбудовуючи їх у їхні щоденні дії.

Культура кібербезпеки стосується колективного мислення, поведінки і практичної діяльності працівників в організації відповідно до вимог кібербезпеки. Високий рівень культури кібербезпеки проявляється у створенні корпоративного середовища, де кожен співробітник: від вищого керівництва до рядових працівників, – не тільки розуміє важливість кібербезпеки, але й активно допомагає захищати цифрові активи та інформацію організації від кіберзагроз, усвідомлюючи спільну відповідальність за належний кіберзахист.

Як показало дослідження, ключовими елементами, які сприяють сильній культурі кібербезпеки, є [2-4] (Рис. 1):

Рис. 1. Основні чинники формування культури кібербезпеки

- Відданість керівництва організації принципам культури кібербезпеки, яка проявляється у визнанні пріоритетності цього напряму, виділенні ресурсів на заходи кібербезпеки й демонстрації підтримки безпекових ініціатив.
- Формування усвідомленої відповідальності за кібербезпеку у всього персоналу і забезпечення підзвітності кожного працівника, що допомагає створити більш пильну робочу силу.
- Розробка чітких політик і процедур безпеки відповідно до кращих практик, зокрема щодо належної обробки даних, управління паролями і прийнятного використання технологій.
- Дотримання правил захисту даних і приватності, а також захист конфіденційної інформації організації як передумова забезпечення нормативної відповідності і високої культури кібербезпеки.
- Забезпечення обізнаності й регулярне навчання персоналу, що має вирішальне значення не тільки для розуміння працівниками важливості кібербезпеки, але й формування навичок розпізнавання кіберзагроз і належного реагування на інциденти.
- Підтримка постійної ефективної комунікації з питань кібербезпеки, зокрема щодо нових загроз і методів їх виявлення та протидії, а також мотивування персоналу інформувати про підозрілу діяльність або потенційні інциденти безпеки.
- Планування відповіді на інциденти і завчасний розподіл ролей у ході реагування, яка дозволяє персоналу діяти швидко і скоординовано відповідно до своїх повноважень.
- Заохочення культури постійного вдосконалення на основі уроків реагування на інциденти безпеки і підтримання постійної обізнаності про актуальні кіберзагрози і кращий галузевий досвід.

Пропагуючи ці принципи, організації можуть створити сильну культуру кібербезпеки, яка посилить їхню стійкість до кіберзагроз і сприятиме ефективному захисту інформаційних активів та ІКС.

Література

1. 2025 Data Breach Investigations Report. Executive Summary. 2025. *Verizon.* URL: https://www.verizon.com/business/resources/reports/2025-dbir-executive-summary.pdf

2. Cyber Security Culture in organisations November 2017. *ENISA.* URL: https://www.enisa.europa.eu/sites/default/files/publications/WP2017%20O-3-3-1%20Cyber%20Security%20Cultures%20in%20Organizations.pdf

3. Sutton A., Tompson L. Towards a cybersecurity culture-behaviour framework: A rapid evidence review. *Computers & Security.* 2025. Volume 148. URL: https://www.sciencedirect.com/science/article/pii/S0167404824004152#tbl0001

4. Sahli M. Creating a Cybersecurity Culture in the Workplace. 2024. *Adnovum*. URL: https://www.adnovum.com/blog/cybersecurity-culture

РОЛЬ ЛЮДСЬКОГО ФАКТОРА У ЗАБЕЗПЕЧЕННІ КІБЕРСТІЙКОСТІ ПІДПРИЄМСТВА: ПРАКТИЧНІ РІШЕННЯ

Старкова О. В., д-р техн. наук, професор,

Кисельова Я. О.

Харківський національний економічний університет імені Семена Кузнеця

м. Харків, Україна

Звіт Verizon DBIR за 2024 рік показав, що навіть у сучасній архітектурі захисту людина все одно залишається найбільш вразливим компонентом системи. Відтак, близько 68% інцидентів виникають через людський фактор [1, с. 8].

На основі вищесказаного, метою роботи є представлення комплексу практичних заходів щодо трансформації персоналу з об'єкта атаки на активного участника інфраструктури безпеки.

Для захисту бізнесу від недбалості персоналу пропонується

впровадження моделі «Активної обізнаності»:

1. Моделювання фішингових атак. Однієї теорії може виявитися недостатньо, але у поєднанні з регулярними перевірками набуті теоретичні знання дозволять виявити групи ризику. За результатами проведення симуляції, Працівник, який допустив помилку, отримує миттєве мікро-навчання (Micro-learning) за конкретним сценарієм атаки.

2. Принцип «Zero Trust» (Нульова довіра). Принцип базується на обмеженні прав доступу користувачів відповідно до мінімально необхідних привілеїв. Це слугує гарантом запобігання компрометації всієї мережі через випадкову помилку одного співробітника.

3. Впровадження технічних запобіжників. Застосування обов'язкової мультифакторної автентифікації (MFA) [2, с.1] для всіх корпоративних сервісів та використання систем запобігання витоку даних (DLP) задля контролю за рухом конфіденційної інформації.

4. Практика швидкого звітування. Користуючись інтегрованим технічним інструментарією миттєвого повідомлення IT-служби про підозрілу активність, Персонал нарешті отримує можливість зайняти проактивну позицію та скоротити час виявлення (Mean Time to Detect) загрози.

Як зазначають професор Г. І. Гайдур та доцент С. О. Гахов у своїх дослідженнях механізму функціонування цілісної інформаційної системи в умовах кібернетичного впливу: «Інформаційна система (ІС) – це складна система, для опису якої необхідно застосовувати системний підхід» [3, с. 22].

Практичний кейс імплементації та механізм дії, наведені нижче, демонструють роботу розробленої моделі на практиці. Процес реалізації рекомендацій вибудовується як цілісний кейс з трьох послідовних етапів.

Етап 1: Діагностика та адаптивне навчання.

Підприємство запускає симуляцію атаки, імітуючи запит на зміну пароля від системного адміністратора [4, с. 2-4]. Працівники, які проігнорували базові правила кібергігієни з будь-якої причини, негайно переходять до проходження інтерактивного тренінгу. Створюється миттєвий психологічний зв'язок між

помилкою та знанням, що сприяє формуванню стійкої пильності.

Етап 2: Технічна мінімізація радіуса ураження.

У разі, якщо зловмисник все ж таки зміг отримати доступ до корпоративної пошти працівника, спрацьовує модель Zero Trust. Оскільки права користувача обмежені (принцип «мінімальних привілеїв»), зловмисник не може отримати доступ до фінансової бази або серверів розробки. MFA блокує спроби входу з підозрілих локацій, локалізуючи інцидент на початковій стадії.

Етап 3: Формування колективного захисту.

Ключовим моментом стане реакція «навченого» персоналу. Коли «навчений» співробітник отримує аналогічний фішинговий лист, тепер він вже буде використовувати інструмент швидкого звітування. IT-служба миттєво отримує зразок шкідливого посилання та блокує його на рівні шлюзу для всього підприємства. Таким чином, одна пильна людина захищає весь колектив.

Як показує аналіз, такий підхід до вирішення висвітленої прооблеми корелює з рекомендаціями Держспецзв'язку України та міжнародним стандартом ISO/IEC 27001 [5, с. 6]. Так, вдалося здійснити перехід від статичного переліку навчальних тем до динамічного циклу «перевірка-обмеження-звітність», аби створити систему захисту, яка здатна до самонавчання.

Новизна підходу полягає у переході від пасивного інструктажу до створення екосистеми, де технічні обмеження (Zero Trust) працюють у симбіозі з високою обізнаністю персоналу. Результатом стане забезпечення практичної кіберстійкості підприємства та безперервності бізнес-процесів.

Література

1. 2024 Data Breach Investigations Report. 2024. С. 1-100. URL: https://www.verizon.com/business/resources/reports/dbir/

2. Рекомендації з кібергігієни для працівників державних органів та приватного сектору. 2024. С. 1-3. URL: https://cip.gov.ua/ua/docs/nakaz-administraciyi-derzhspeczv-yazku-vid-21-10-2025-661-pro-zatverdzhennya-

metodichnikh-rekomendacii-shodo-provedennya-instruktazhiv-i-treningiv-shodo-kibergigiyeni-na-period-priznachennya-na-posadi-derzhavnikh-sluzhbovciv-pracivnikiv-organiv-derzhavnoyi-vladi-ta-inshikh-derzhavnikh-organiv-viiskovosluzhbovciv-kerivnikiv-ta-pracivnikiv-derzhavnikh-pidpriyemstv-ustanov-ta-organizacii

3. Гайдур Г. І., Гахов С. О. Механізм функціонування цілісної інформаційної системи в умовах кібернетичного впливу. *Сучасний захист інформації* 2019. С. 22-26. URL: https://journals.dut.edu.ua/index.php/dataprotect/article/view/2353/2253

4. Hadlington L. Human factors in cybersecurity: examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. 2017. С. 1-18. URL: file:///C:/Users/Admin/Downloads/Human_factors_in_cybersecurity_examining_the_link_.pdf

5. ISO/IEC 27001:2022. 2022. С. 1-20. URL: https://www.exactls.com/wp-content/uploads/2025/02/ISO_IEC-270012022-ed.3.pdf

ПЕРЕВАГИ СИМУЛЯЦІЙНОГО НАВЧАННЯ ФАХІВЦІВ З КІБЕРБЕЗПЕКИ

Ушаков В. А.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

У сучасних умовах швидкої еволюції кіберзагроз і потреби у своєчасній адаптації до них систем кіберзахисту нагальним завданням стає постійне оновлення знань і навичок фахівців з кібербезпеки. З огляду на те, що традиційні методи підвищення кваліфікації кіберспеціалістів поступово втрачають свою актуальність, на перший план виходять методи симуляційного

навчання, які підвищують результативність і забезпечують практичну спрямованість навчання.

Симуляційне навчання з кібербезпеки – це спосіб точно відтворити корпоративну IT-систему і перевірити, наскільки якісно і швидко кіберкоманда реагує на змодельовані кібератаки [1].

Навчання було і залишається обов'язковим елементом багатьох стратегій кібербезпеки, однак сьогодні постає завдання щодо розширення його обсягів і підвищення ефективності. Так, користувачі по всій організації, а не лише фахівці з IT, повинні знати, що робити у разі кібератаки, а правильне реагування на кіберзагрозу в потрібний час може запобігти реалізації деструктивних сценаріїв.

Розглянемо основні переваги симуляційного навчання у кібербезпеці.

Однією з головних переваг імітаційних середовищ є їхня здатність відтворювати реалістичні умови інформаційних систем і мереж завдяки використанню віртуалізації, емуляції мережевих протоколів і сервісів, а також інтеграції з реальними інструментами безпеки.

Такий підхід дозволяє фахівцям набути навичок відпрацювання сценаріїв з різними типами атак, зокрема DDoS, фішинг, SQL-ін'єкції, соціоінженерні атаки тощо. Сучасні імітаційні середовища дозволяють не лише моделювати атаки, але й відпрацьовувати стратегії захисту, налаштовувати системи виявлення вторгнень/захищень, брандмауери та системи моніторингу й аналізу мережевого трафіку. Це забезпечує комплексний підхід до навчання, дозволяючи зрозуміти тактику й методи зловмисників, а також методи ефективного захисту [2].

Навчання, що базується на практичному досвіді в максимально наближеному до реального середовищі, сприяє не тільки підвищенню кваліфікації фахівців з кібербезпеки і забезпеченню їх практичної підготовки до роботи, підвищенню ефективності навчання, але і зменшенню витрат на безпеку.

Симуляційне навчання є ефективним засобом безпечного тестування нових стратегій чи інноваційних засобів кібербезпеки, впровадження яких у діючі корпоративні мережі може викликати значні ризики безпеці. Аналогічно симуляційні технології можуть бути успішно використані у процесі перевірки кваліфікації кандидатів на зайняття посад з кібербезпеки в організації.

Крім цього, симуляційне навчання, яке відтворює реальне IT-середовище організації, надає широкі можливості для збору важливої інформації не лише для покращення та спрямування навчання, але й для розуміння прогалин у системі захисту і перспективних напрямів інвестування в кібербезпеку [1].

Завдяки практичному навчанню на основі симуляційних технологій працівники організації незалежно від посади і важливості їхнього внеску в забезпечення кібербезпеки можуть краще зрозуміти вимоги кібербезпеки й освоїти основні кібернавички для використання на своєму робочому місці.

Отже, використання симуляційного навчання для підготовки спеціалістів з кібербезпеки сприяє підвищенню ефективності й практичної спрямованості навчання, дозволяє безпечно апробувати нові технології безпеки, а також є джерелом корисної інформації про недоліки і перспективні напрями кіберзахисту.

Література

1. Cyber Security Simulation Training. *Cloudshare*. URL: https://www.cloudshare.com/virtual-it-labs-glossary/cyber-security-simulation

2. Tymoshchuk D., Yatskiv V., Tymoshchuk V., Yatskiv N. Interactive Cybersecurity Training System Based on Simulation Environments. *Measuring and computing devices in technological processes.* 2024. Issue 4. P. 215-220.

УПРАВЛІННЯ ТАЛАНТАМИ ЯК ІНСТРУМЕНТ ПОДОЛАННЯ ДЕФІЦИТУ КАДРІВ У ГАЛУЗІ КІБЕРБЕЗПЕКИ

Царенок С. О.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

В епоху цифрової трансформації організації стикаються з важливим викликом: зростаючим розривом між кіберстійкими і вразливими до кіберзагроз компаніями. Основним фактором, що збільшує цей розрив, є глобальний дефіцит кваліфікованих фахівців з кібербезпеки.

У 2024 році світ потребує 4,8 мільйона кіберфахівців для захисту цифрових активів, зі зростанням потреби на 19% порівняно з минулим роком. Високі вимоги до фахівців з кібербезпеки, їх адаптація до новітніх технологій і методів, зростання розриву між захищеними і вразливими компаніями вимагають збільшених інвестицій у навчання і розвиток кадрів [1].

Управління талантами (talent management) — це стратегічна система роботи з людьми, яка допомагає компанії розвивати, утримувати й масштабувати людський капітал відповідно до цілей бізнесу [2].

В умовах зростаючого дефіциту фахівців у галузі кібербезпеки традиційні підходи до кадрового забезпечення, що обмежуються підбором персоналу на відкриті вакансії, виявляються недостатньо ефективними. Конкуренція за висококваліфікованих спеціалістів на глобальному ринку праці зумовлює необхідність переходу від реактивної моделі управління персоналом до проактивної, стратегічно орієнтованої системи розвитку людського капіталу.

Розроблення стратегії управління талантами грунтується на таких принципах [3]:

1. Стратегічна узгодженість: стратегія управління талантами підпорядковується загальній стратегії управління персоналом, щоб у сукупності з іншими управлінськими діями забезпечити досягнення бізнес-цілей компанії.

2. Структурна цілісність: заходи управління талантами розглядаються як взаємопов'язані, внутрішньо збалансовані елементи єдиної системи, що застосовуються послідовно і цілеспрямовано, тримаючи у фокусі стратегічні пріоритети компанії.

3. Гнучкість і адаптивність: стратегія управління талантами не є постійною у довгостроковій перспективі і може змінюватися в залежності від мінливих умов ринкового середовища, бізнес-потреб і фінансово-економічних можливостей компанії.

4. Розподілене лідерство: відповідальність за управління талантами лежить на вищому керівництві, HR менеджерах та лінійних менеджерах. Залученість керівництва різних рівнів грунтується на спільному баченні ролі талантів і прагненні дотримуватися визначених політик і програм з управління ними.

5. Брендинг талантів: компанія свідомо розвиває власні унікальні переваги в управлінні талантами, тим самим забезпечуючи потенційні можливості притоку талантів ззовні.

Управління талантами виступає ефективним засобом подолання кадрової нестачі, оскільки воно спрямоване не лише на залучення зовнішніх фахівців, а й на системне формування внутрішнього кадрового потенціалу. Завдяки впровадженню механізмів визначення перспективних співробітників та створенню програм безперервного навчання організація формує власний резерв компетентних спеціалістів. У галузі кібербезпеки високий рівень професійного навантаження та стресу часто призводить до вигорання спеціалістів. Створення сприятливого середовища розвитку, можливостей кар'єрного зростання та визнання професійних досягнень підвищує рівень залученості працівників та їхню лояльність до організації.

Підсумовуючи можна сказати, що в умовах цифрової трансформації та стрімкого зростання кіберзагроз саме людський капітал стає ключовим чинником забезпечення кіберстійкості організацій. Глобальна нестача кваліфікованих фахівців у сфері кібербезпеки зумовлює необхідність переходу від традиційних методів кадрового забезпечення до стратегічного підходу, заснованого на принципах управління талантами. Системне впровадження механізмів виявлення, розвитку та утримання перспективних спеціалістів дозволяє не лише мінімізувати кадровий розрив, а й сформувати стійкий професійний потенціал, здатний ефективно протидіяти сучасним кіберзагрозам.

Література

1. Україна В. Дефіцит кадрів у кібербезпеці: Роль штучного інтелекту. Міжнародна аудиторська компанія BDO - BDO. URL: https://www.bdo.ua/uk-ua/insights-2/information-materials/2024/bridging-the-cybersecurity-talent-gap-augmenting-human-efforts-with-ai(дата звернення: 24.02.2026).

2. Що таке управління талантами і чому без нього бізнес не зростає | HURMA. HURMA. URL: https://hurma.work/blog/shho-take-upravlinnya-talantamy/ (дата звернення: 24.02.2026).

3. Sytnik N., Perminova S., Chuprina M. STRATEGIC ASPECTS OF TALENT MANAGEMENT IN A BUSINESS ORGANIZATION. Economic scope. 2024. No. 195. P. 62–67. URL: https://doi.org/10.30838/ep.195.62-67 (дата звернення: 24.02.2026).

СЕКЦІЯ 8. ЗАКОНОДАВЧА Й НОРМАТИВНА ОСНОВА ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ

ISO/IEC 25126 ЯК ІНСТРУМЕНТ АДАПТАЦІЇ МІЖНАРОДНИХ СТАНДАРТІВ БЕЗПЕКИ ДЛЯ ЗМІЦНЕННЯ КІБЕРСТІЙКОСТІ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

Ахмедов А. Ф.
Державний університет інформаційно-комунікаційних технологій
м. Київ, Україна

Стрімкий розвиток технологій розподіленого реєстру (Distributed Ledger Technology - DLT) та архітектури Web3 створює новий контекст, що кидає виклик існуючим правовим та регуляторним парадигмам. Протягом 2022-2025 років сумарні фінансові втрати у екосистемі Web3 від компрометацій ключів, експлойтів та атак на протоколи перевищили 12 млрд доларів США [1, с. 23].

На фоні інституціоналізації ринку DLT та появи профільних регуляцій (MiCA у ЄС, DLT-політики у США та Сінгапурі) виникла гостра необхідність розробки нового міжнародного стандарту інформаційної безпеки. Саме таким стандартом є ISO/IEC 25126, який станом на кінець 2025 року перебуває на етапі Working Draft (WD 25126.2) та є першим глобальним кроком до створення єдиної системи контролю для DLT та Web3.

Традиційні стандарти ISO/IEC 27001 та 27002 забезпечують високий рівень безпеки для корпоративних IT-систем, однак вони не враховують особливостей децентралізованого середовища: відсутність центрального адміністратора, незмінність даних у блокчейні, публічність журналів транзакцій, відповідальність за безпеку ключів, покладена на користувача, неможливість відкликання або видалення записів у реєстрі [2, с. 12-15]. Саме це

зумовлює необхідність стандартизованої системи контролів, спеціально розробленої для врахування специфіки та ризиків DLT.

Робоча версія стандарту ISO/IEC 25126 має назву: «Information security, cybersecurity and privacy protection - Information security controls for the use of distributed ledger technology services based on ISO/IEC 27002». Його ключова особливість - запровадження нових контролів, які є відсутніми у ISO 27002: DLT.01 Key Management (управління криптографічними ключами), DLT.02 Smart Contract Security (безпека смарт-контрактів), DLT.03 Consensus Security (безпека механізмів консенсусу), DLT.04 Oracle Security (безпека оракулів), DLT.05 Privacy in Public Ledgers (захист приватності), DLT.06 Bridge Security (безпека міжмережевих мостів), DLT.07 Governance Security (безпека управління) [3, с. 8-12].

Адаптація міжнародних стандартів до національних умов є критично важливою для України в контексті євроінтеграційних процесів та гармонізації законодавства з нормативною базою ЄС. Впровадження ISO/IEC 25126 дозволить: по-перше, створити методологічну основу для оцінки відповідності DLT-сервісів вимогам кібербезпеки; по-друге, інтегрувати специфічні DLT-контролі в національні системи управління інформаційною безпекою; по-третє, забезпечити довіру інституційних інвесторів та страхових організацій до вітчизняних Web3-проєктів.

Практична реалізація стандарту передбачає розробку галузевих методичних рекомендацій, підготовку фахівців з аудиту DLT-систем, створення тестових середовищ для верифікації смарт-контрактів та імплементацію механізмів реагування на інциденти в децентралізованих системах. Особлива увага має приділятися питанням юрисдикційної визначеності при використанні публічних блокчейнів та захисту прав користувачів в умовах транскордонного обігу криптоактивів.

Таким чином, ISO/IEC 25126 є першим глобальним стандартом, що адаптує міжнародні принципи інформаційної безпеки до децентралізованих технологій. Він не замінює ISO/IEC 27001 чи ISO/IEC 27002, а доповнює їх,

створюючи комплексну модель захисту для екосистеми Web3. Впровадження в Україні ISO/IEC 25126 сприятиме зміцненню кіберстійкості національного цифрового простору та гармонізації вітчизняних стандартів з вимогами регуляторної бази ЄС.

Література

1. Chainalysis. Crypto Crime Report 2025: Mid-Year Update. 2025. 156 с. URL: https://www.chainalysis.com/blog/2025-crypto-crime-mid-year-update/ (дата звернення: 17.02.2026).

2. ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection - Information security management systems - Requirements. Geneva: ISO, 2022. 24 с. URL: https://www.iso.org/standard/27001 (дата звернення: 17.02.2026).

3. Working Draft of ISO/IEC 25126.2: Information security, cybersecurity and privacy protection - Information security controls for the use of distributed ledger technology services based on ISO/IEC 27002. Geneva: ISO, 2025.48 с. URL: https://www.iso.org/standard/89024.html (дата звернення: 17.02.2026).

РЕФОРМУВАННЯ ЗАКОНОДАВСТВА ДЛЯ ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ УКРАЇНИ

Дарій В. Р.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

З початку вторгнення Росії, інтернет та кіберпростір стали дуже важливими зонами конфлікту, оскільки на критичну інфраструктуру України постійно здійснюються кібератаки. Одна з таких атак в грудні 2024 року тимчасово вивела з ладу низку дуже важливих державних систем. Надзвичайна

ситуація у країні призвела до необхідності комплексного перегляду чинного законодавства щодо кібербезпеки. Відповідність українського законодавства нормам і стандартам ЄС є важливою не тільки для покращення стану кібербезпеки в Україні і її посилення на кіберфронті, але й для інтеграції у світову кібербезпеку як держави, так і підприємств. Для України міжнародне співробітництво в галузі кібербезпеки та гармонізація нормативно-правових актів в цій сфері з Європейським союзом є стратегічним завданням.

Основу чинного регулювання закладено Законом України «Про основні засади забезпечення кібербезпеки України» [1]. Цей документ визначив загальні принципи та організаційну структуру національної системи кібербезпеки. Захист об'єктів критичної інформаційної інфраструктури додатково врегульовано Законом «Про критичну інфраструктуру» [2], однак і він не давав відповіді на запитання про те, як саме мають управлятися кіберризики і в які строки потрібно реагувати на інциденти. Було досить помітним суттєве відставання вітчизняної системи кіберзахисту від відповідних стандартів Євросоюзу та від реального рівня загроз, а питання реформування ставало дедалі актуальнішим в умовах зобов'язань України щодо зближення законодавства з нормами ЄС [3, с. 74–75].

Стандарти, до яких має наближатися Україна, передусім визначає Директива (ЄС) 2022/2555 про заходи для забезпечення високого спільного рівня кібербезпеки (NIS2) [4], що набула обов'язкової сили для держав — членів ЄС у жовтні 2024 року. Порівняно з попередньою версією вона значно підвищила вимоги: охоплює вже 18 секторів замість 7, передбачає особисту відповідальність керівників організацій за недотримання вимог кіберзахисту, посилює контроль за безпекою ланцюгів постачання та встановлює чіткі строки повідомлення про інциденти — 24 години для першого сигналу та 72 години для повноцінного звіту. Важливою новацією є поділ суб'єктів регулювання на «суттєві» та «важливі» залежно від рівня ризику та розміру організації, тоді як українська практика традиційно спирається на фіксований перелік секторів без урахування цих критеріїв [5].

Реакцією держави на описані виклики стало прийняття 27 березня 2025 року Закону України № 4336-IX «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури» [6], що набрав чинності 20 квітня 2025 року. Документ став відповіддю одночасно на атаку проти реєстрів у грудні 2024 року та на вимоги щодо наближення до норм NIS2. Закон запровадив систему авторизації безпеки інформаційних і комунікаційних систем замість застарілої процедури комплексних систем захисту інформації; зобов'язав державні органи та підприємства критичної інформаційної інфраструктури створювати окремі підрозділи з кіберзахисту та призначати відповідальних фахівців, погоджуючи їх кандидатури з Державною службою спеціального зв'язку та захисту інформації; запровадив обов'язкові навчання з кібергігієни для персоналу та розширив взаємодію між державним і приватним секторами. Уточнення термінів «кіберзахист» та «об'єкт критичної інформаційної інфраструктури» усунуло попередню неоднозначність і наблизило документ до термінології, застосованої в Директиві NIS2.

Попри позитивні зрушення, досі існують значні невідповідності NIS2 та сучасним викликам і загрозам. В Україні досі відсутній єдиний реєстр суб'єктів, класифікованих за рівнем критичності та ризику – інструмент, який дозволяє диференційований підхід до регулювання різних організацій. Механізм обов'язкового повідомлення про кіберінциденти зі встановленими строками та чіткою процедурою також ще не отримав нормативного закріплення у повному обсязі. Серед фахівців тривають дискусії щодо ризиків надмірної централізації повноважень Державної служби спеціального зв'язку та захисту інформації [7]. Окремою проблемою залишається фрагментарність правового регулювання загалом: норми розпорошені між великою кількістю законів, підзаконних актів та технічних стандартів, що ускладнює їх практичне застосування. Для усунення цих недоліків варто зосередитися на трьох напрямах. По-перше, розробити єдиний закон про кіберстійкість, який охоплюватиме повний обсяг вимог NIS2 та містить механізм класифікації і реєстрації суб'єктів. По-друге,

нормативно закріпити чіткі строки та процедури повідомлення про кіберінциденти. По-третє, запровадити механізм розкриття інформації про вразливості, який дозволить налагодити ефективну координацію між державними органами та приватними компаніями.

Узагальнюючи, можна зробити висновок що 2024–2025 роках законодавче забезпечення кіберстійкості України зробило помітний крок уперед. Прийняття Закону № 4336-IX закладає нову основу для захисту державних ресурсів та об'єктів критичної інформаційної інфраструктури. Разом з тим досягнення повної відповідності вимогам NIS2 потребує подальшої послідовної роботи. Ефективна система кіберстійкості сьогодні є одночасно умовою нормального функціонування держави в умовах воєнного стану та необхідною передумовою успішної євроінтеграції України.

Література

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : станом на 19 жовт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

2. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX : станом на 21 верес. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text

3. Журбинський Д. А., Костенко В. О. Актуальність посилення кібербезпеки України в умовах дії воєнного стану в контексті європейської інтеграції. Публічне управління та адміністрування в Україні. 2023. Вип. 34. С. 74–77.

4. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive). O.J. L 333, 27.12.2022, p. 80-152.

5. Горовенко В. І., Рибалко В. В. Кібербезпека критичної інфраструктури в законодавстві України та в Директиві (ЄС) 2022/2555. Електронне моделювання. 2023. Т. 45. № 5. С. 55–66. URL: https://www.researchgate.net/publication/375323482

6. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури : Закон України від 27.03.2025 № 4336-IX. URL: https://zakon.rada.gov.ua/laws/show/4336-20#Text

7. Ільєнко А. В., Телющенко В. О., Дубчак О. А. Сучасні кіберзагрози критичної інфраструктури України та світу. Кібербезпека: освіта, наука, техніка. 2025. Т. 3. № 27. С. 150–164.

РОЛЬ ОСВІТИ ТА ПРОФЕСІЙНИХ СТАНДАРТІВ У ФОРМУВАННІ КВАЛІФІКАЦІЙНИХ ВИМОГ ДО ФАХІВЦІВ З КІБЕРБЕЗПЕКИ

Коробенко Д. О.

Державний університет інформаційно-комунікаційних технологій

м. Київ, Україна

Освіта є фундаментальним чинником формування кваліфікаційних вимог до фахівців з кібербезпеки, оскільки забезпечує системну підготовку кадрів відповідно до професійних стандартів. В Україні спеціальність 125 «Кібербезпека» (галузь знань 12 «Інформаційні технології») запроваджена з 2015 року, а стандарти вищої освіти затверджено Міністерством освіти і науки.

Згідно з Національною рамкою кваліфікацій (НРК) та професійними стандартами (затвердженими Наказом Мінекономіки та Держспецзв’язку 2022–2024 рр.), випускники бакалаврського та магістерського рівнів повинні володіти компетенціями з аналізу загроз, реагування на інциденти, управління ризиками та впровадження систем захисту [1].

Професійні стандарти («Фахівець сфери захисту інформації», «Фахівець з реагування на інциденти кібербезпеки», «Аудитор інформаційних технологій з кібербезпеки») чітко визначають кваліфікаційні вимоги: від 6-го до 8-го рівня НРК. Вони інтегруються в освітні програми закладів вищої освіти (ЗВО), що підтверджує робоча зустріч НАQА 2023 року «Роль та місце професійних стандартів у формуванні освітніх програм з напряму кібербезпеки» [2].

Важливим аспектом є підвищення обізнаності та формування культури кібербезпеки серед усіх верств населення. Людський фактор залишається найслабшою ланкою: за даними досліджень, понад 90 % успішних кібератак пов'язані з помилками користувачів. Тому в Україні активно розвивається національна система кіберосвіти. Платформа «Дія.Освіта» у 2025 році опублікувала цикл практичних гайдів з кібергігієни для громадян, бізнесу та держслужбовців [3].

У закладах освіти запроваджуються обов'язкові модулі з кібербезпеки вже з початкової школи, а в ЗВО — кейс-орієнтоване та симуляційне навчання. Формування культури кібербезпеки передбачає безперервне навчання: регулярні тренінги, симуляції атак, розвиток критичного мислення щодо фішингу, соціальної інженерії та захисту персональних даних. Це безпосередньо впливає на кваліфікаційні вимоги: сучасний фахівець повинен не лише володіти технічними навичками, але й бути здатним формувати культуру безпеки в організації.

Законодавча й нормативна база є основою для формування кваліфікаційних вимог, оскільки чітко визначає обов'язки фахівців та стандарти їхньої підготовки. Базовим документом є Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII [4], який встановлює правові та організаційні засади захисту національних інтересів у кіберпросторі.

Ключовими нормативними актами є також Стратегія кібербезпеки України [5] та Постанова КМУ № 712 від 18.06.2025 щодо профілів безпеки [6]. У 2025 році набув чинності Закон № 4336-IX та Постанова КМУ № 712, які

передбачають перехід від комплексних систем захисту інформації (КСЗІ) до профілів безпеки та посилення вимог до кваліфікації фахівців об'єктів критичної інфраструктури.

Нормативна база вимагає від фахівців постійного підвищення кваліфікації (сертифікація, курси відповідно до профстандартів). Законодавство акцентує на координації освіти з потребами ринку: Держспецзв'язку, МОН та НАQA спільно формують освітні стандарти, щоб випускники відповідали реальним викликам гібридної війни та цифрової трансформації.

Таким чином, законодавча й нормативна основа не лише регулює сферу, а й безпосередньо визначає кваліфікаційні вимоги, роблячи освіту та професійні стандарти головними інструментами забезпечення кіберстійкості держави.

Освіта, обізнаність і культура кібербезпеки разом із чіткою законодавчо-нормативною основою формують сучасні кваліфікаційні вимоги до фахівців. Їхнє інтегроване застосування дозволяє Україні ефективно протистояти кіберзагрозам і розвивати висококваліфікований кадровий потенціал.

Література

1. Фахівець сфери захисту інформації : професійний стандарт. Дата затвердження: 25 листопада 2022 р. URL: https://register.nqa.gov.ua/profstandart/fahivec-sferi-zahistu-informacii (дата звернення: 24.02.2026).

2. Про робочу зустріч «Роль та місце професійних стандартів у формуванні освітніх програм закладів вищої освіти з напряму кібербезпеки». Національне агентство із забезпечення якості вищої освіти. URL: https://naqa.gov.ua/2023/05/про-робочу-зустріч-роль-та-місце-проф/ (дата звернення: 24.02.2026).

3. Основи кібергігієни : освітній серіал. Платформа «Дія.Освіта», 2025. URL: https://osvita.diia.gov.ua/courses/cyber-hygiene (дата звернення: 24.02.2026).

4. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 24.02.2026).

5. Про Стратегію кібербезпеки України : рішення Ради національної безпеки і оборони України від 14.05.2021 р., введене в дію Указом Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021 (дата звернення: 24.02.2026).

6. Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем : постанова Кабінету Міністрів України від 18.06.2025 № 712. URL: https://zakon.rada.gov.ua/laws/show/712-2025-п (дата звернення: 24.02.2026).