УДК 004.056:004.732
DOI: 10.31673/2409-7292.2025.041201

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

У статті здійснено комплексний огляд і систематичний аналіз сучасних методів, моделей, систем та інструментів, які використовуються для оцінювання рівня інформаційної безпеки в корпоративному середовищі. Розглянуто як традиційні, так і інноваційні підходи до виявлення та усунення вразливостей, з акцентом на адаптивність до швидкозмінного цифрового ландшафту. Особливу увагу приділено вивченню специфічних загроз, притаманних різним галузям бізнесу, зокрема внутрішнім інсайдерським загрозам, цільовим кібератакам, методам соціальної інженерії, атакам на ланцюги постачання тощо. У роботі проаналізовано переваги та обмеження наявних рішень, а також запропоновано критерії ефективності для оцінки рівня захищеності інформаційних систем у корпоративних структурах.

Окрему увагу приділено інтеграції систем моніторингу подій безпеки з автоматизованими засобами реагування, що дозволяє суттєво підвищити оперативність і точність виявлення інцидентів. Також розглянуто перспективи застосування штучного інтелекту та машинного навчання для прогнозування кіберзагроз і побудови динамічних моделей ризиків. На основі проведеного дослідження сформульовано практичні рекомендації щодо вибору оптимального підходу до оцінювання інформаційної безпеки з урахуванням специфіки IT-інфраструктури, масштабу компанії, галузі діяльності та наявних ресурсів. Представлені результати можуть бути використані як основа для розробки стратегій кіберзахисту в умовах підвищеної загрози інформаційним активам.

Ключові слова: інформаційна безпека, корпоративна мережа, оцінювання ризиків, кіберзагрози, інсайдерські атаки, хмарні технології, моделі захисту, моніторинг безпеки, машинне навчання, управління інформаційними ризиками.

Вступ

У сучасному корпоративному середовищі інформаційні ресурси відіграють ключову роль у забезпеченні стабільної діяльності організацій, їх конкурентоспроможності та розвитку. Водночас зростає кількість і складність інформаційних загроз, які можуть призвести до серйозних фінансових, репутаційних та операційних втрат. Це обумовлює необхідність впровадження ефективних методів оцінювання рівня інформаційної безпеки, що дозволяють своєчасно виявляти вразливості, аналізувати ризики та приймати обґрунтовані управлінські рішення. Незважаючи на наявність численних підходів і систем, що забезпечують оцінку безпеки, багато з них не враховують специфічні загрози, властиві тому чи іншому корпоративному середовищу. Наприклад, інсайдерські загрози, галузеві особливості або цільові атаки часто залишаються поза увагою стандартних моделей. Крім того, сучасні тенденції цифрової трансформації, зокрема активне впровадження хмарних технологій, віддаленого доступу та інтернету речей, створюють нові вектори атак і підвищують складність контролю за безпековими процесами. У зв'язку з цим виникає потреба у більш гнучких, динамічних і контекстно орієнтованих підходах до оцінювання інформаційної безпеки, які можуть адаптуватися до змін зовнішнього та внутрішнього середовища. Такі підходи повинні забезпечувати не лише технічний аналіз загроз, а й враховувати поведінкові, організаційні та стратегічні аспекти. У цьому контексті важливо дослідити сучасні методи і моделі, які дозволяють здійснювати комплексну оцінку рівня захищеності корпоративних систем та сприяти прийняттю ефективних рішень у сфері кібербезпеки.

Мета та постановка задачі

Отже метою цієї роботи є аналіз існуючих методів, моделей, систем та підходів до оцінки інформаційної безпеки з урахуванням специфіки корпоративного середовища та характерних для нього специфічних загроз. У роботі здійснено порівняльний огляд відомих інструментів і підходів, визначено їх переваги, недоліки та можливості адаптації під конкретні умови. Результати аналізу можуть слугувати основою для обґрунтованого вибору рішень у сфері кібербезпеки.

Виклад основного матеріалу дослідження

Кіберзагрози у корпоративному середовищі – це дії, що здійснюються окремими особами зі зловмисними намірами з метою викрадення інформації, пошкодження або порушення роботи комп'ютерних систем. До поширених типів кіберзагроз належать шкідливе програмне забезпечення, соціальна інженерія, атаки типу «людина посередині» (MitM), атаки типу «відмова в обслуговуванні» (DoS) та атаки типу «ін'єкція коду» – кожна з яких буде розглянута більш детально нижче.

Таблиця 1

Багатовимірна модель класифікації загроз [2]

Джерело загрози	Тип загрози	Підтип	Характер загрози	Потенційні наслідки
Зовнішня загроза	Людська	Зловмисна	Випадкова	Знищення інформації, пошкодження даних, крадіжка або втрата інформації, розголошення конфіденційних даних, відмова у доступі, несанкціоноване підвищення привілеїв
			Умисна	Цілеспрямоване знищення інформації, навмисне спотворення або пошкодження даних, крадіжка критичних даних, зловмисне розголошення, кібератаки на сервіси, доступ до обмежених функцій
	Незловмисна	Випадкова		Ненавмисне видалення даних, технічні помилки користувача, неусвідомлене порушення політик безпеки, що призвело до втрати або компрометації інформації
			Умисна	Дії, виконані без зловмисного наміру, але свідомо — наприклад, використання застарілих систем без оновлень або навмисне нехтування інструкціями без усвідомлення ризику
	Екологічна	Незловмисна	Випадкова	Природні катастрофи (повінь, землетрус, буря), що призводять до фізичного знищення обладнання та втрати даних
	Технологічна	Незловмисна	Випадкова	Аварії в інфраструктурі (вимкнення електрики, перегрів серверів, збої в мережі), що викликають втрату доступу або інформації
Внутрішня загроза	Людська	Зловмисна	Випадкова	Незнання внутрішнього співробітника, який має доступ до критичних даних, але через недбалість запускає зловмисне ПЗ або виконує дії, що шкодять системі
			Умисна	Навмисна крадіжка або маніпулювання даними внутрішнім працівником, саботаж, злив конфіденційної інформації, знищення або пошкодження файлів
	Незловмисна	Випадкова	Випадкова	Людські помилки, наприклад, надсилання листа не тому адресату, неправильне налаштування прав доступу, випадкове форматування носія з даними
			Умисна	Свідомі, але не шкідливі дії, наприклад, перевірка функціоналу без дотримання політик безпеки або самостійне оновлення програмного забезпечення
	Екологічна	Незловмисна	Випадкова	Витік води, пожежа, інші внутрішні фізичні фактори (наприклад, замикання), які руйнують техніку або мережі компанії
	Технологічна	Незловмисна	Випадкова	Внутрішні технічні збої: помилки системного адміністрування, неправильна конфігурація серверів, збої систем резервного копіювання

Ці загрози можуть надходити з різних джерел, таких як ворожі уряди, терористичні угруповання, незалежні хакери або навіть довірені інсайдери, такі як співробітники або підрядники, які зловживають своїми привілеями доступу для здійснення шкідливої діяльності [1, 2, 3].

Оцінка мережевої безпеки – це всебічне дослідження IT-інфраструктури компанії, що має на меті виявлення, аналіз, усунення вразливостей і забезпечення постійного захисту від можливих кіберзагроз. Актуальність таких загроз підтверджується даними звіту компанії Qualys за 2023 рік: виявлено 206 видів вразливостей високого рівня ризику, понад половину з яких активно експлуатують кіберзлочинці. Обсяг такої оцінки може варіюватися – від окремого підрозділу до всієї корпоративної мережі. [4, 5].

Risk score кібербезпеки визначається шляхом оцінки різних факторів, включаючи політику безпеки організації, інфраструктуру, методи роботи співробітників і взаємодію з третіми сторонами. Ключову роль відіграє політика кібербезпеки компанії, зокрема, те, як здійснюється управління конфіденційними даними, контроль доступу користувачів та реагування на інциденти. Крім того, важливе значення мають типи систем, мереж і технологій безпеки, таких як брандмауери і шифрування, а також їх обслуговування. Оскільки багато компаній покладаються на хмарні сховища і сторонніх постачальників, заходи безпеки навколо хмарних даних і перевірка сторонніх партнерів додають складності в оцінці ризиків. Нарешті, дії співробітників, включаючи управління паролями, обізнаність про безпеку та обробку даних, можуть суттєво вплинути на оцінку через потенційну можливість людської помилки. [5, 6].

CVSS виникла як дослідницький проект, ініційований Національною консультативною радою з питань інфраструктури (National Infrastructure Advisory Council, NIAC) у 2003 році з метою стандартизації оцінки вразливостей. Дослідники NIAC розробили CVSS як відкриту систему, яку можна адаптувати до різних IT-систем та середовищ. Версія 4.0 CVSS включає чотири групи метрик: Базові, Загрози, Середовище та Додаткові, кожна з яких відображає різні характеристики вразливостей програмного забезпечення.

Метрики експлуатації (Exploitability Metrics):

- вектор атаки (**A**ttack **V**ector);
- складність атаки (**A**ttack **C**omplexity);
- необхідні привілеї (**P**rivileges **R**equired);
- взаємодія з користувачем (**U**ser **I**nteraction);
- обсяг (**S**cope).

Метрики впливу (Impact Metrics):

- конфіденційність (**C**onfidentiality);
- цілісність (**I**ntegrity);
- доступність (**A**vailability).

CVSS використовує офіційно складну формулу, але в спрощеному вигляді це:

$$CVSS\ Base\ Score = f(Exploitability, Impact),$$

де:

$$Exploitability = 8.22 \times AV \times AC \times PR \times UI,$$
$$Impact = 1 - [(1 - C) \times (1 - I) \times (1 - A)].$$

А далі формула залежить від того, чи змінився обсяг впливу (**S**cope). Результат – числове значення від 0 до 10, яке вказує на критичність уразливості.

Організації можуть використовувати онлайн-калькулятори для визначення різних оцінок CVSS, в тому числі на основі попередніх версій, а також використовувати інструменти управління вразливостями, які інтегрують оцінки CVSS. Провідні програмні рішення для

оцінки вразливостей враховують показники CVSS поряд з іншими ключовими факторами, такими як контрольні показники відповідності, посібники з безпеки від постачальників та галузеві дослідження. Ці інструменти також можуть мати функції на основі штучного інтелекту, наприклад, автоматизоване виявлення даних у режимі реального часу, щоб покращити реагування на інциденти та управління конфіденційністю [7, 8].

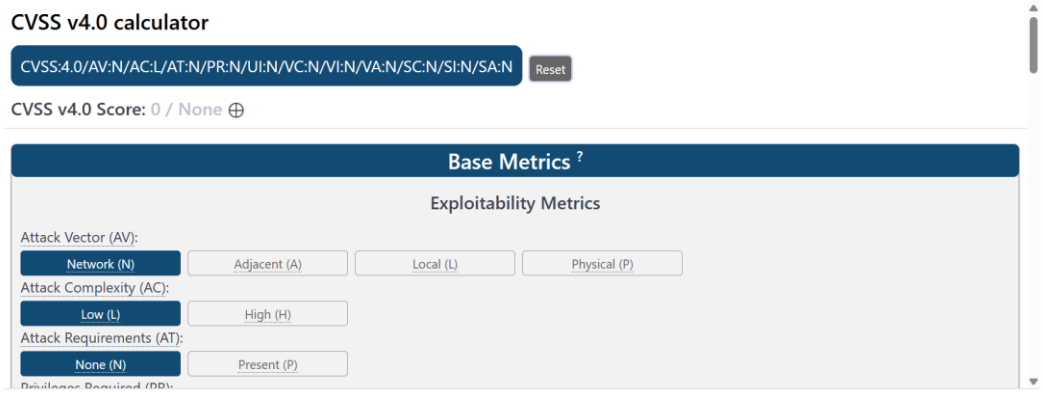

Рис. 1. Калькулятор CVSS v4.0 [9]

Комбіновані підходи до оцінки інформаційної безпеки поєднують різні методи та інструменти для всебічної оцінки ризиків та виявлення вразливостей в організаційних системах. Ці підходи включають як кількісні, так і якісні методи, такі як використання міжнародних стандартів (наприклад, ISO/IEC 27001), оцінки загроз і вразливостей, а також автоматизовані інструменти для моніторингу та аналізу загроз. Поєднуючи технічні інструменти, оцінки на основі політики безпеки та аналіз людського фактору, організації можуть отримати більш повну картину поточного стану безпеки та ефективно планувати заходи для зменшення ризиків та покращення інформаційної безпеки [9].

Рис. 2. ISO 27001 [10]

STRIDE, розроблений Лореном Конфельдером (Loren Kohnfelder) та Праеріт Гарг (Praerit Garg) у 1999 році, розшифровується як «підробка, фальсифікація, заперечення, розкриття

інформації, відмова в обслуговуванні та зловживання привілеями». Вона була створена для виявлення потенційних вразливостей і загроз для продуктів компанії. Методологія STRIDE від Microsoft покликана забезпечити відповідність додатків ключовим вимогам безпеки, включаючи конфіденційність, цілісність і доступність (CIA), а також авторизацію, аутентифікацію і відсутність відмови. Перевага STRIDE полягає в тому, що вона дозволяє організаціям оцінювати системи і мережі, класифікуючи загрози в пріоритетному списку на основі їх ймовірності і потенційної серйозності їх впливу [11, 12].

Таблиця 2

Діаграма STRIDE [13]

Об'єкт	Загроза	Визначення	Приклад
Аутентифікація	Підробка	Видавання себе за щось або когось іншого.	Видавання себе за billg, microsoft.com або ntdll.dll
Цілісність	Фальсифікація	Модифікація даних або коду	Модифікація DLL на диску або DVD, або пакету під час проходження через локальну мережу.
Ствердження	Заперечення	Ствердження, що ви не виконували певної дії.	«Я не надсилав цього листа», «Я не змінював цей файл», «Я точно не відвідував цей веб-сайт, дорогенька!»
Конфіденційність	Розкриття Інформації	Розкриття інформації особі, яка не має права її бачити	Дозвіл комусь читати вихідний код Windows; публікація списку клієнтів на веб-сайті.
Доступність	Відмова в обслуговуванні	Відмова або погіршення обслуговування користувачів	Збій Windows або веб-сайту, надсилання пакету та поглинання секунд процесорного часу або перенаправлення пакетів у чорну діру.
Авторизація	Підвищення привілеїв	Отримання можливостей без належного дозволу	Дозвіл віддаленому користувачеві Інтернету виконувати команди є класичним прикладом, але перехід від обмеженого користувача до адміністратора - це також EoP.

DREAD – це абревіатура, що описує п'ять критеріїв для оцінки загроз для програмного забезпечення. DREAD розшифровується як:

- пошкодження (**D**amage potential);
- відтворюваність (**R**eproducibility);
- експлутативність (**E**xploitability);
- кількість постраждалих користувачів (**A**ffected users);
- виявленість (**D**iscoverability).

$$DREAD\ Score = \frac{D+R+E+A+D}{5}.$$

Щоб пріоритетизувати загрози для вашого драйвера, оцініть кожну загрозу за шкалою від 1 до 10 за всіма 5 критеріями DREAD, після чого підсумуйте бали та поділіть на 5 (кількість критеріїв). Результатом буде числовий бал від 1 до 10 для кожної загрози. Високі бали вказують на серйозні загрози.[15]

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation – Оцінка операційно критичних загроз, активів і вразливостей) – це методологія оцінки ризиків, розроблена у 2003 році Університетом Карнегі-Меллона та підрозділом CERT Інституту програмної інженерії (SEI). На відміну від підходів, що зосереджуються переважно на технічних ризиках, OCTAVE акцентує увагу на організаційних ризиках, наприклад, на операційних наслідках витоку даних, і орієнтована переважно на малі та середні підприємства з кількістю співробітників до 100 осіб. Методологія є самокерованою: відповідальність за

© Шульга В.П., Іванченко Є.В., Берестяна Т.В., Роженко А.С. (2025) Аналіз існуючих методів, моделей, систем та інструментів, що використовуються для оцінки інформаційної безпеки в корпоративному середовищі з урахуванням специфічних загроз. Сучасний захист інформації, 4(64), 8–16.
https://doi.org/10.31673/2409-7292.2025.041201

визначення стратегії безпеки покладається на управлінський та операційний персонал, а не на технічні команди, що робить OCTAVE гнучкою, але складнішою для масштабування. Вона допомагає організаціям визначати методи пом'якшення ризиків, підвищує обізнаність про ризики, сприяє співпраці між командами, зменшує потребу у надмірній документації та забезпечує послідовні й відтворювані результати. OCTAVE підтримує розвиток культури інформаційної безпеки, покращує видимість ризиків для всіх команд і надає розробникам активоцентричне бачення безпеки. До недоліків можна віднести складність інтеграції методології в існуючі процеси, можливі прогалини в охопленні новітніх загроз і труднощі в управлінні великою кількістю документації в умовах динамічного середовища [16].

Кібербезпекова структура *NIST (CSF)* версії 2.0 надає рекомендації для промисловості, урядових установ та інших організацій щодо управління ризиками у сфері кібербезпеки.

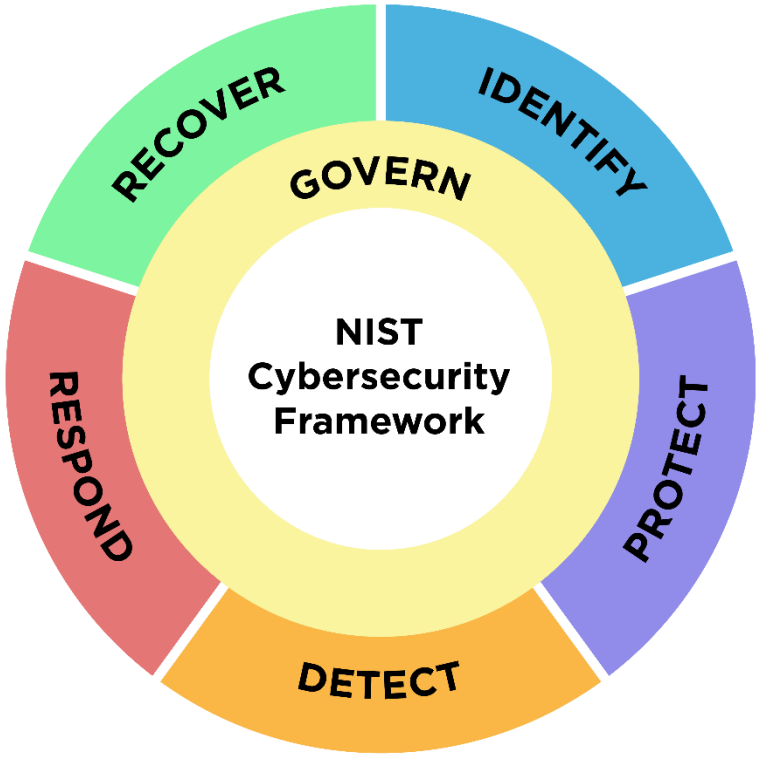

Рис. 3. Кібербезпекова структура NIST 2.0 [17]

Вона пропонує таксономію високорівневих результатів у галузі кібербезпеки, яку може використовувати будь-яка організація, незалежно від її розміру, галузі чи рівня зрілості, для кращого розуміння, оцінки, визначення пріоритетів і комунікації своїх зусиль у сфері кіберзахисту. CSF не встановлює, яким саме чином мають досягатися ці результати. Натомість, вона містить посилання на онлайн-ресурси з додатковими рекомендаціями щодо практик і засобів контролю, які можуть допомогти у досягненні зазначених результатів. Цей документ описує версію CSF 2.0, її складові та різноманітні способи її застосування [17].

Оцінка безпеки в сучасному кіберпросторі неможлива без використання спеціалізованих систем та інструментів, які забезпечують постійний моніторинг, аналіз та реагування на загрози. Нижче подано огляд основних категорій таких рішень.

SIEM-системи (Security Information and Event Management) – це платформи для централізованого збору, аналізу та зберігання журналів подій з усіх частин IT-інфраструктури. Вони дозволяють виявляти аномалії, корелювати події та швидко реагувати на інциденти. Прикладами таких рішень є Splunk та IBM QRadar, які поєднують можливості аналітики, машинного навчання та візуалізації даних для оперативного виявлення загроз [18].

Системи оцінки вразливостей призначені для сканування мереж, додатків та пристроїв з метою виявлення відомих вразливостей. Інструменти, як-от Nessus та Qualys, дозволяють проводити автоматизовані перевірки, створювати звіти з ризиками та рекомендаціями для усунення недоліків. Ці системи є ключовими для регулярного контролю стану кібербезпеки [19].

Інструменти аудиту та моніторингу забезпечують спостереження за системними ресурсами, навантаженням, доступом і діями користувачів. Наприклад, Zabbix дозволяє відстежувати стан серверів, мереж і додатків у реальному часі, а OpenVAS – це відкритий сканер безпеки, що підтримує широкий набір тестів для виявлення потенційних загроз [20, 21].

Таким чином у сучасному корпоративному середовищі, де інформаційна безпека є критично важливою складовою стабільної діяльності організацій, використання ефективних методів, моделей, систем та інструментів оцінки кіберзагроз є необхідністю. Серед методологій, що забезпечують стандартизований підхід до аналізу вразливостей та ризиків, варто виокремити CVSS, DREAD, STRIDE та OCTAVE, кожна з яких має свої переваги та сфери застосування. Наприклад, CVSS дозволяє кількісно оцінювати рівень критичності вразливостей, DREAD та STRIDE – класифікувати та пріоритезувати загрози, а OCTAVE зосереджена на стратегічному управлінні ризиками з боку бізнесу. Водночас такі фреймворки, як NIST Cybersecurity Framework 2.0, пропонують концептуальну основу для побудови комплексної системи кіберзахисту, яка охоплює всі ключові процеси – від виявлення активів до реагування та відновлення після інцидентів [22].

З технічного боку, системи типу SIEM (Splunk, QRadar), сканери вразливостей (Nessus, Qualys), моніторингові інструменти (Zabbix, OpenVAS) та інтегровані рішення (SOC, SOAR, XDR) забезпечують безперервний аналіз, контроль та автоматизацію заходів кібербезпеки. Їхня інтеграція дозволяє не лише зменшити час реакції на інциденти, а й покращити загальне управління безпековими процесами.

Загалом, комплексне використання цих підходів, як організаційних, так і технічних, з урахуванням специфіки корпоративних загроз, дозволяє суттєво підвищити рівень інформаційної безпеки, адаптуючи захист до постійно змінного ландшафту кіберризиків.

Таблиця 2

Порівняльна таблиця

Категорія	**Назва**	**Призначення / Функція**	**Переваги**	**Приклади використання**
Методи та моделі	CVSS	Оцінка критичності вразливостей	Кількісна оцінка, стандартизація	Приоритезація патчів, аналіз загроз
	DREAD	Оцінка загроз за п’ятьма критеріями	Гнучкість, пріоритетність	Оцінка ризику для програмних продуктів
	STRIDE	Класифікація загроз	Орієнтована на розробників	Проєктування захищених систем
	OCTAVE	Управління ризиками на рівні організації	Фокус на бізнес-процесах	Малий та середній бізнес

	NIST CSF 2.0	Рамка управління всіма аспектами безпеки	Гнучкість, сумісність, масштабованість	Побудова стратегії кібербезпеки
Системи та інструменти	SIEM	Збір, аналіз подій, реагування на інциденти	Централізація, автоматизація	Splunk, IBM QRadar
	Сканери вразливостей	Виявлення технічних вразливостей	Швидке виявлення, автоматизація	Nessus, Qualys
	Моніторинг	Контроль за IT-інфраструктурою	Реальний час, алерти	Zabbix, OpenVAS
	Інтегровані платформи	Комплексний кіберзахист	Автоматизація, масштабність, аналітика	SOC, SOAR, XDR

Висновки

Отже, було досліджено що ефективне оцінювання методів, моделей, систем та інструментів, що використовуються для оцінки рівня інформаційної безпеки в корпоративному середовищі є критично важливим для своєчасного виявлення вразливостей, мінімізації ризиків та забезпечення сталого функціонування інформаційних систем. Сучасні загрози, зокрема інсайдерські атаки, цільові кібератаки та уразливості, пов’язані з використанням хмарних технологій, вимагають комплексного та адаптивного підходу до моделювання ризиків і впровадження відповідних захисних механізмів. Розгляд існуючих методів оцінювання, дозволив виділити їх сильні сторони та обмеження. Було встановлено, що найбільш ефективними є ті підходи, які поєднують кількісну оцінку технічних параметрів із врахуванням контексту функціонування організації та її бізнес-процесів.

Перелік посилань

1. Гальченко, А. В. Оцінка рівня інформаційної безпеки корпоративних мереж / А. В. Гальченко. – К. : Наукова думка, 2020. 192 с.

2. FireMon. Network Security Assessment: A Guide. [Electronic resource] 2025. https://www.firemon.com /blog/ network-security-assessment-a-guide/.

3. Cybersecurity Threats. [Electronic resource]. https: // www.imperva.com /learn/ application-security/cyber-security- threats/.

4. SISA. What is Cyber Risk Score? How does it help an organization? [Electronic resource] 2024. https:// www.sisainfosec.com /blogs/ what-is-cyber-risk-score-how-does-it-help-an-organization/.

5. Кузнєцов, О. М. Кібербезпека підприємств: теорія та практика / О. М. Кузнєцов. Харків : Видавництво ХНЕУ, 2019. 210 с.

6. Classification of Security Threats in Information Systems. [Electronic resource]. https://www.sciencedirect.com/science/article/pii/S1877050914006528.

7. Савчук, А. І. Захист інформаційних систем від кіберзагроз / А. І. Савчук. Львів : Видавничий центр ЛНУ, 2021. 180 с.

8. IBM. What is the Common Vulnerability Scoring System (CVSS)? [Electronic resource]. https://www.ibm.com/docs/en/qradar-on-cloud?topic=vulnerabilities-common-vulnerability-scoring-system-cvss.

9. National Vulnerability Database - CVSS v4.0 calculator. [Electronic resource]. https://nvd.nist.gov/vuln-metrics/cvss/v4-calculator.

10. TIC-UA. Комплексний підхід до оцінки ризиків інформаційної безпеки. [Electronic resource]. https://tic-ua.com/uk/statti/kompleksnyj-pidhid-do-kiberbezpeky-zasnovanyj-na-oczinczi-ryzykiv/.

11. Панченко, В. Ю. Моделі та методи оцінки інформаційної безпеки / В. Ю. Панченко, О. В. Коваленко. Одеса : Астропринт, 2018. 250 с.
12. ISO-27001. [Electronic resource]. https://www.dqsglobal.com/uk-ua/sertifikujte/sertifikaciya-iso-27001
13. Мельниченко, О. П. Оцінка ризиків інформаційної безпеки: методологія та інструменти / О. П. Мельниченко. Львів : Видавництво ЛНУ, 2017. 180 с.
14. IriusRisk. Threat Modeling Methodology: STRIDE. [Electronic resource]. https://www.iriusrisk.com/resources-blog/threat-modeling-methodology-stride.
15. Microsoft Security. STRIDE chart. [Electronic resource]. https://www.microsoft.com/en-us/security/blog/2007/09/11/stride-chart/.
16. Microsoft Build. The future is yours. [Electronic resource] 2025, May 19-22. https: // developer. microsoft. com/en-us/.
17. IriusRisk. Threat Modeling Methodology: OCTAVE. [Electronic resource]. https://www.iriusrisk.com/resources-blog/octave-threat-modeling-methodologies.
18. The NIST Cybersecurity Framework (CSF) 2.0. [Electronic resource] 2024, February 26. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.
19. nist-cybersecurity-framework-20. [Electronic resource]. https: // my-itspecialist.com / nist-csf-2.0-six-cybersecurity-functions.
20. What is security information and event management (SIEM)? [Electronic resource]. https:// www.ibm.com /think/topics/siem.
21. Nessus vs. Qualys vs. OpenVAS. [Electronic resource] 2024, July 29. https://www.infosectrain.com/blog/nessus-vs-qualys-vs-openvas/.
22. 25 Best Vulnerability Scanning Software Reviewed in 2025. [Electronic resource]. https://thectoclub.com/tools/best-vulnerability-scanning-tools/.

Надійшла 10.09.2025

УДК 004.056.53
DOI: 10.31673/2409-7292.2025.041202

Ветлицька О. С.

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У КІБЕРБЕЗПЕЦІ: ІНТЕГРАЦІЯ РИЗИК-МЕНЕДЖМЕНТУ ТА ПРАВОВИХ МОДЕЛЕЙ

У статті досліджено критичну необхідність інтеграції законодавчих вимог (зокрема, GDPR) та технічних механізмів кібербезпеки для ефективного захисту персональних даних (ПД). Центральною тезою є те, що відповідність (compliance) не є тотожною безпеці, і вимагає впровадження проактивного підходу «приватність за дизайном» (Privacy by Design). Проаналізовано застосування оцінки впливу на приватність (PIA/DPIA) як діагностичного інструменту для виявлення зон ризику в життєвому циклі ПД. Запропоновано модель комплексного ризик-орієнтованого захисту ПД (МКРОЗ), що поєднує техніки мінімізації даних (токенизація, анонімізація) з принципами правового контролю. Обґрунтовано, що практичні аспекти захисту включають не лише посилення шифрування, але й архітектурну сегрегацію даних та впровадження методології управління доступом на основі ролей (RBAC), що підкріплена постійним правовим аудитом. Дослідження акцентує увагу на методологічному розриві між абстрактними юридичними вимогами (як-от «право на забуття» чи «мінімізація даних») та їхнім конкретним технічним втіленням. Для подолання цього розриву пропонується формалізована модель «правового ризику», що дозволяє кількісно оцінити потенційні регуляторні та фінансові наслідки невідповідності (штрафи, позови) і інтегрувати цю метрику в традиційні матриці технічних кіберризиків. Цей підхід забезпечує керівництву IT-безпеки можливість приймати економічно обґрунтовані рішення, пріоритизуючи інвестиції у ті засоби захисту, які одночасно мінімізують як технічні вразливості, так і регуляторні загрози. Практична значущість статті полягає в детальному обґрунтуванні архітектурних рішень, необхідних для реалізації МКРОЗ, включаючи принципи сегрегації даних (розділення ідентифікаторів та чутливої інформації) та використання токенізації для зниження периметра впливу порушення. Запропоновані механізми управління доступом, зокрема вдосконалена RBAC, інтегровані з юридичними ролями (наприклад, DPO чи комплаєнс-офіцер), дозволяють забезпечити, що технічні дозволи прямо відображають правові обмеження доступу до ПД. Це створює надійну основу для захисту даних не лише від зовнішніх загроз, але й від внутрішніх порушень, обумовлених неналежним управлінням правами.

Ключові слова: персональні дані, GDPR, privacy by design, data loss prevention, ризик-менеджмент, токенізація, правові моделі, конфіденційність.