МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Міжнародний гуманітарний університет
Кафедра комп'ютерної інженерії та інноваційних технологій

Радівілова Т. А., Йона Л.Г., Педяш В.В., Мазур Г.Д.

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРБЕЗПЕКОЮ

Конспект лекцій для здобувачів вищої освіти зі спеціальності
125 Кібербезпека та захист інформації

Одеса 2026

УДК 004.056.5:005.336(075.8)

Радівілова Т. А., Йона Л.Г., Педяш В.В., Мазур Г.Д.
Управління інформаційною та кібербезпекою: конспект лекцій / Т. А. Радівілова, Л.Г. Йона, В.В. Педяш , Г.Д. Мазур; Міжнар. гуманіт. ун-т. – Одеса : МГУ, 2025. – 62 с.

Конспект лекцій з дисципліни «Управління інформаційною та кібербезпекою» розроблено відповідно до навчального плану підготовки бакалаврів зі спеціальності 125 «Кібербезпека та захист інформації». Навчальний матеріал охоплює питання нормативно-правового регулювання, побудови систем управління інформаційною безпекою (СУІБ), оцінки ризиків, моніторингу інцидентів, аудиту захищеності та забезпечення безперервності бізнес-процесів. Видання призначено для здобувачів вищої освіти денної та заочної форм навчання.

ЗМІСТ

ВСТУП

Сучасний етап розвитку інформаційного суспільства характеризується стрімким зростанням кількості та складності кіберзагроз, що вимагає від фахівців у галузі кібербезпеки не лише технічних знань, а й глибокого розуміння управлінських процесів. Дисципліна «Управління інформаційною та кібербезпекою» є обов'язковим компонентом освітньо-професійної програми підготовки бакалаврів зі спеціальності 125 «Кібербезпека та захист інформації». Актуальність курсу зумовлена необхідністю інтеграції заходів кібербезпеки в організаційну структуру та бізнес-процеси відповідно до чинного законодавства України та найкращих світових практик.

Метою викладання дисципліни є забезпечення здобувачів фундаментальними знаннями з принципів побудови системи управління інформаційною безпекою, методик кількісної та якісної оцінки ризиків, а також вимог міжнародних стандартів серії ISO/IEC 27000. Навчальний матеріал охоплює широке коло питань, включаючи нормативно-правове регулювання, розробку політик безпеки, управління інцидентами, аудит систем захисту та забезпечення безперервності бізнес-процесів у контексті сучасних викликів. Особлива увага приділяється набуттю практичних навичок розробки політик безпеки, планування реагування на інциденти та проведення аудиту захищеності.

Структура навчальної дисципліни побудована навколо семи змістових модулів, які послідовно розкривають логіку управління безпекою від нормативного забезпечення до стратегічних тенденцій. Здобувачі опрацюють теми законодавчої бази України та міжнародних стандартів, принципи формування політик безпеки включаючи підходи Zero Trust, методології управління ризиками за стандартами ISO/IEC 27005 та NIST. Окремі розділи присвячені моніторингу та реагуванню на інциденти з використанням SIEM-систем, методологіям аудиту та тестування безпеки, побудові комплексних систем захисту за принципом «захист у глибину» та забезпеченню безперервності бізнесу. Завершальний модуль розглядає перспективи використання штучного інтелекту та машинного навчання для управління безпекою в умовах цифрової трансформації.

Конспект лекцій містить основний теоретичний матеріал, необхідний для опрацювання тем курсу, підготовки до практичних занять та самостійної роботи. Ефективне засвоєння матеріалу вимагає систематичної роботи з науковою та навчальною літературою, своєчасного виконання індивідуальних завдань та активної участі в обговоренні проблемних питань сучасної кібербезпеки.

ЛЕКЦІЯ 1. НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Сутність інформаційної безпеки та її місце в системі національної безпеки

Інформаційна безпека є однією з фундаментальних складових сучасної концепції національної безпеки держави. В умовах стрімкого розвитку цифрових технологій та глобалізації інформаційного простору захист інформації набуває стратегічного значення, оскільки від нього безпосередньо залежать обороноздатність країни, стабільність її економіки, надійність державного управління та безпека громадян. Зростання кількості кіберзагроз, масштаби яких за останнє десятиліття збільшилися в десятки разів, підтверджує нагальну потребу у формуванні комплексної системи управління інформаційною безпекою як на державному, так і на корпоративному рівні.

Поняття «інформаційна безпека» охоплює широкий спектр заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації. Конфіденційність означає, що доступ до інформації мають лише авторизовані суб'єкти; цілісність гарантує, що дані не були несанкціоновано змінені або знищені; доступність забезпечує можливість своєчасного та надійного використання інформації уповноваженими особами. Ці три властивості, відомі як тріада CIA (Confidentiality, Integrity, Availability), є базовими принципами, на яких будується будь-яка система захисту інформації.

У контексті національної безпеки інформаційна безпека тісно пов'язана з поняттям кібербезпеки. Якщо інформаційна безпека охоплює захист інформації в будь-якому її вигляді — паперовому, електронному, усному — то кібербезпека зосереджена переважно на захисті цифрових систем, мереж та даних від кіберзагроз. В сучасній практиці ці поняття нерідко вживаються як взаємозамінні, хоча між ними існують принципові відмінності, що відображено у відповідних нормативних документах і стандартах. Розуміння цих відмінностей є важливою передумовою для правильної побудови системи управління безпекою в організації.

Важливість інформаційної безпеки для держави підтверджується тим, що більшість сучасних держав включила її до переліку пріоритетів своїх стратегій національної безпеки. В Україні це знайшло відображення у Стратегії кібербезпеки, Законі України «Про основні засади забезпечення кібербезпеки України» та ряді інших нормативних актів. Стратегічні документи визначають основні загрози, об'єкти захисту, відповідальних суб'єктів та механізми координації зусиль у сфері кіберзахисту. Особливу роль у цій системі відіграє

захист критичної інфраструктури, до якої належать об'єкти енергетики, транспорту, фінансової системи, телекомунікацій та державного управління.

Концепція управління інформаційною безпекою передбачає не лише технічний захист систем, але й організаційні, правові та людські аспекти. Технічні засоби захисту — міжмережеві екрани, системи виявлення вторгнень, засоби криптографічного захисту — є лише частиною комплексного підходу до забезпечення безпеки. Не менш важливими є розробка та впровадження політик безпеки, навчання персоналу, формування культури безпечної поведінки в організації, а також створення ефективних процедур реагування на інциденти. Без узгодженої взаємодії всіх цих компонентів навіть найсучасніші технічні засоби не можуть гарантувати належного рівня захисту.

Взаємозв'язок основних складових системи інформаційної безпеки організації схематично представлено на рисунку 1.1.

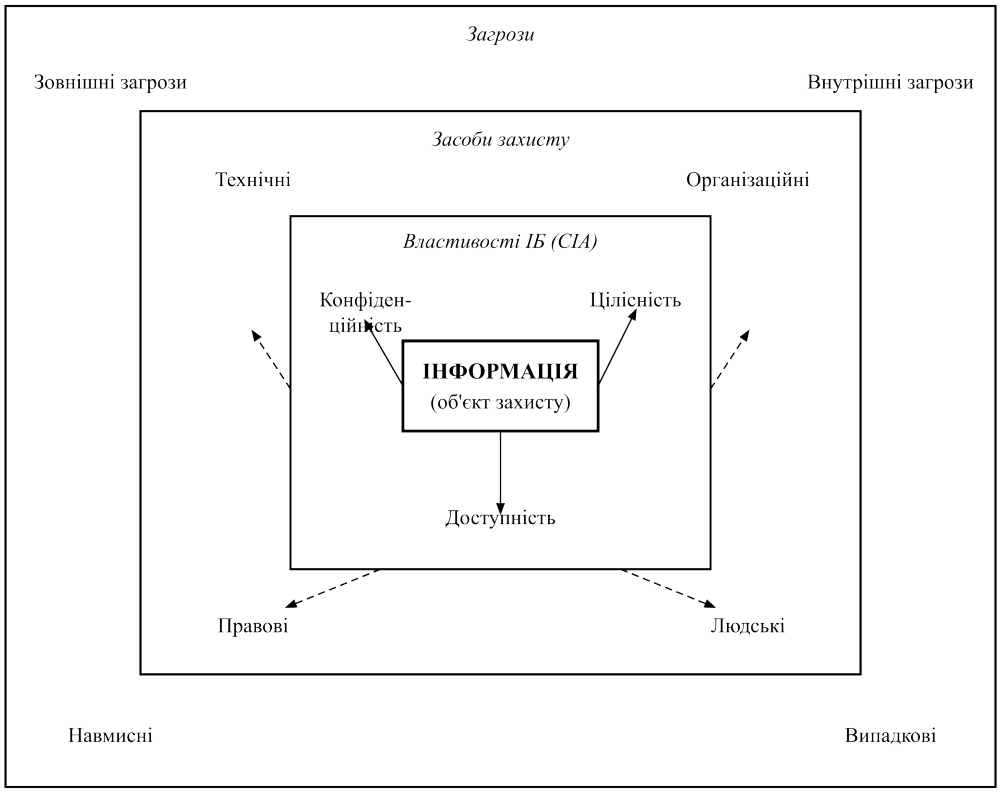


Рисунок 1.1 – Концептуальна модель інформаційної безпеки організації

Управління інформаційною безпекою як дисципліна сформувалося в другій половині XX століття, коли автоматизовані системи обробки інформації набули масового поширення. Перші системи захисту були зосереджені переважно на фізичній безпеці та контролі доступу до обчислювальних ресурсів. З розвитком мережевих технологій і особливо з появою глобальної мережі Інтернет у 1990-х роках кількість та різноманітність загроз значно зросла, що спонукало до розробки більш комплексних підходів до захисту інформації.

Сьогодні управління інформаційною безпекою являє собою зрілу дисципліну зі своєю методологією, стандартами та кращими практиками, що визнані на міжнародному рівні.

1.2. Нормативно-правова база інформаційної безпеки в Україні

Нормативно-правова база інформаційної безпеки в Україні сформована на трьох рівнях: конституційному, законодавчому та підзаконному. Конституція України (1996) гарантує право громадян на захист персональних даних, таємницю кореспонденції та захист від незаконного збору та використання інформації. Ці конституційні норми є основою для всього масиву законодавства у сфері захисту інформації та персональних даних. Виходячи з них, держава формує обов'язки суб'єктів правовідносин щодо захисту інформації та встановлює відповідальність за порушення відповідних норм.

На законодавчому рівні ключову роль відіграє Закон України «Про інформацію» (1992, із змінами), який визначає базові поняття інформаційних відносин, види інформації за режимом доступу та основи державної інформаційної політики. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» (1994) встановлює вимоги до захисту інформації в автоматизованих системах та визначає відповідальність за їх порушення. Важливим нормативним актом є також Закон України «Про захист персональних даних» (2010), прийнятий відповідно до вимог Директиви ЄС 95/46/ЕС, який регулює питання обробки персональних даних та встановлює права суб'єктів таких даних.

Сферу кібербезпеки безпосередньо регулює Закон України «Про основні засади забезпечення кібербезпеки України» (2017), який визначає правові та організаційні основи забезпечення кібербезпеки, об'єкти кіберзахисту, суб'єктів національної системи кібербезпеки та їх повноваження. Закон запровадив поняття критичної інфраструктури, визначив об'єкти критичної інформаційної інфраструктури та встановив вимоги до їх захисту. На підставі цього Закону Кабінет Міністрів України затвердив ряд підзаконних актів, які деталізують вимоги до суб'єктів кіберзахисту та порядок взаємодії між ними.

Важливу роль у системі нормативно-правового регулювання відіграють стандарти та технічні нормативні документи. В Україні діє ряд національних стандартів у сфері інформаційної безпеки, гармонізованих із міжнародними стандартами серії ISO/IEC 27000. Зокрема, ДСТУ ISO/IEC 27001:2015 встановлює вимоги до систем управління інформаційною безпекою (СУІБ), ДСТУ ISO/IEC 27002:2015 містить практичні рекомендації щодо заходів безпеки, а ДСТУ ISO/IEC 27005:2015 визначає підходи до управління ризиками

інформаційної безпеки. Крім того, Держспецзв'язку розробило та затвердило ряд нормативних документів системи технічного захисту інформації (ТЗІ), які є обов'язковими для застосування в органах державної влади та при роботі з інформацією, що становить державну таємницю.

Таблиця 1.1 – Основні законодавчі акти України у сфері інформаційної безпеки

Нормативний акт	Рік прийняття	Основний предмет регулювання
Закон України «Про інформацію»	1992	Базові поняття інформаційних відносин, режими доступу до інформації
Закон України «Про захист інформації в ІТС»	1994	Захист інформації в автоматизованих системах
Закон України «Про захист персональних даних»	2010	Обробка та захист персональних даних
Закон України «Про кібербезпеку»	2017	Основи кібербезпеки, критична інфраструктура, НСКБ
Указ Президента № 447/2021	2021	Стратегія кібербезпеки України на 2021–2025 роки

Кримінальна відповідальність за злочини у сфері інформаційних технологій встановлена розділом XVI Кримінального кодексу України. Стаття 361 КК України передбачає відповідальність за несанкціоноване втручання в роботу комп'ютерних систем, стаття 361-1 — за створення та розповсюдження шкідливих програм, стаття 362 — за несанкціоновані дії з комп'ютерною інформацією. Важливо зазначити, що з прийняттям Закону «Про кібербезпеку» та змінами до КК України відповідальність за кіберзлочини була суттєво посилена, а сфера застосування відповідних норм розширена з урахуванням сучасного рівня кіберзагроз.

Адміністративна відповідальність за правопорушення у сфері інформаційної безпеки передбачена Кодексом України про адміністративні правопорушення. Вона застосовується переважно за порушення вимог щодо захисту персональних даних, порушення правил поводження з інформацією, що становить банківську, комерційну або іншу охоронювану законом таємницю, а також за порушення вимог у сфері технічного захисту інформації. Адміністративні санкції застосовуються Державною службою спеціального

зв'язку та захисту інформації України та іншими уповноваженими органами в межах їхньої компетенції.

1.3. Міжнародні стандарти та їх роль у формуванні системи управління інформаційною безпекою

Серія стандартів ISO/IEC 27000 є найбільш визнаною міжнародною базою для побудови систем управління інформаційною безпекою. Стандарт ISO/IEC 27000 містить загальний огляд серії та словник термінів, ISO/IEC 27001 встановлює вимоги до СУІБ та є єдиним стандартом серії, відповідність якому може бути сертифікована незалежним органом. ISO/IEC 27002 містить детальні рекомендації щодо впровадження заходів безпеки, перелічених у Додатку А до ISO/IEC 27001. В редакції 2022 року структура стандарту зазнала суттєвих змін: кількість заходів безпеки скорочена з 114 до 93, а самі заходи реорганізовані з 14 у 4 тематичні групи — організаційні, кадрові, фізичні та технологічні.

Стандарт ISO/IEC 27001 базується на циклі Демінга PDCA (Plan-Do-Check-Act) і передбачає системний підхід до управління інформаційною безпекою. Відповідно до цього стандарту, організація повинна визначити контекст своєї діяльності та очікування зацікавлених сторін, провести оцінку ризиків, обрати відповідні заходи безпеки, впровадити та документувати їх, а також здійснювати постійний моніторинг та вдосконалення СУІБ. Процесний підхід, закладений у стандарті, забезпечує інтеграцію управління інформаційною безпекою в загальну систему менеджменту організації та дозволяє досягти вимірюваних результатів.

Схематичне зображення циклу PDCA в контексті СУІБ наведено на рисунку 1.2.

Поряд зі стандартами ISO/IEC 27000 важливу роль у практиці управління кібербезпекою відіграє Framework кібербезпеки NIST (NIST CSF), розроблений Національним інститутом стандартів і технологій США. У версії 2.0, опублікованій у 2024 році, Framework включає шість функцій: Govern (Управління), Identify (Ідентифікація), Protect (Захист), Detect (Виявлення), Respond (Реагування) та Recover (Відновлення). NIST CSF є гнучким інструментом, який може застосовуватися організаціями будь-якого розміру та типу незалежно від їхньої галузевої приналежності. Він широко використовується у сфері захисту критичної інфраструктури та доповнює вимоги ISO/IEC 27001.

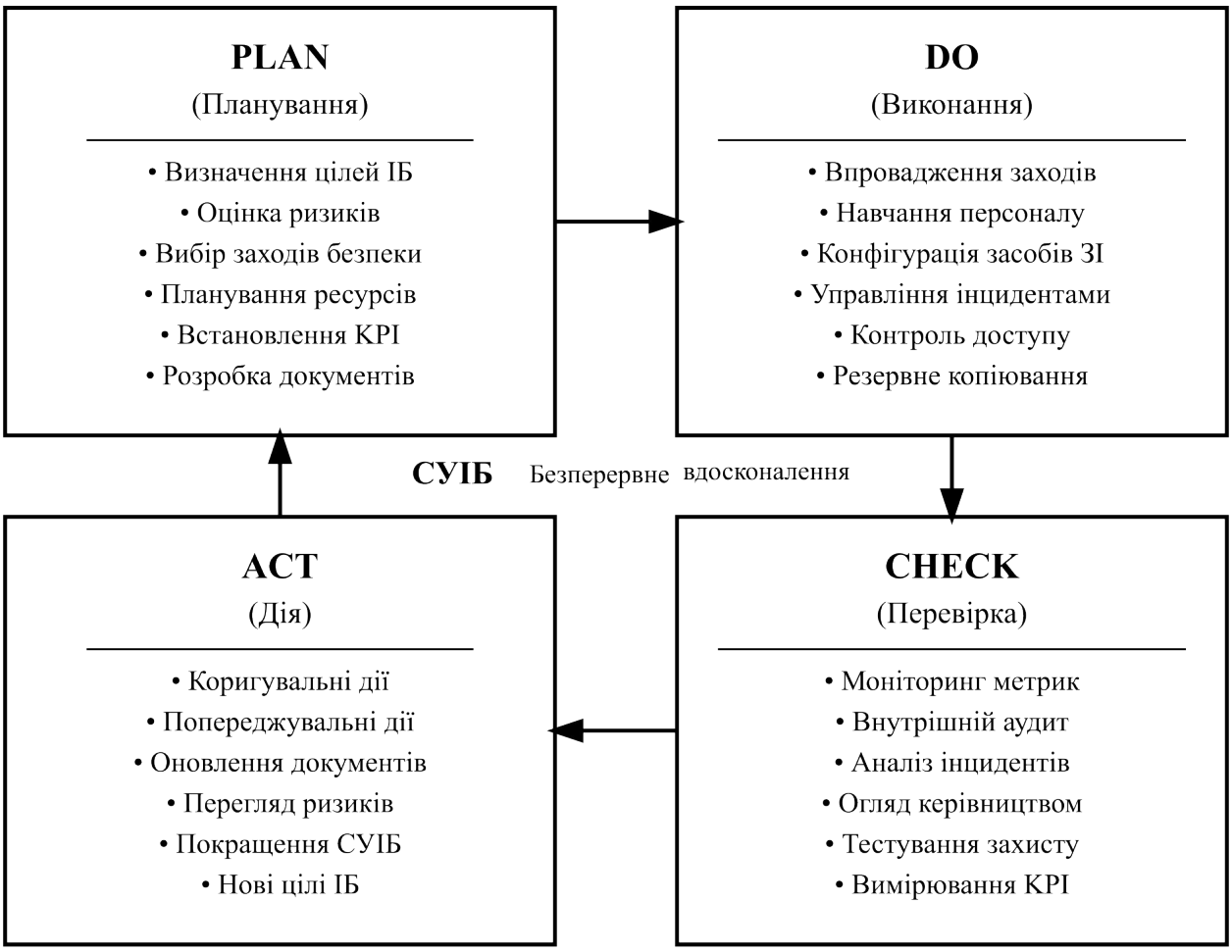


Рисунок 1.2 – Цикл PDCA у системі управління інформаційною безпекою

Стандарти PCI DSS (Payment Card Industry Data Security Standard) та HIPAA (Health Insurance Portability and Accountability Act) є прикладами галузевих нормативних документів, що встановлюють специфічні вимоги до захисту інформації у фінансовій та медичній сферах відповідно. Їхнє застосування є обов'язковим для організацій, що оперують платіжними картками або медичними даними. В Україні врахування цих стандартів є важливим для компаній, що прагнуть вийти на міжнародні ринки або співпрацювати з іноземними партнерами.

Зіставлення основних міжнародних стандартів і фреймворків кібербезпеки за сферою застосування представлено на рисунку 1.3. Рисунок 1.3 являє собою матрицю 4×4, де по вертикалі розташовані стандарти та фреймворки (ISO/IEC 27001, NIST CSF, PCI DSS, HIPAA), а по горизонталі — критерії оцінювання (Сфера застосування, Сертифікація, Управління ризиками, Відповідність регулятору). Кожна клітинка матриці містить умовне позначення рівня відповідності: «+» — повністю, «±» — частково, «—» — не передбачено. Матриця виконана у кольорах: зелений для «+», жовтий для «±», червоний для «—».

	Сфера застосування	Сертифі-кація	Управління ризиками	Відповідність регулятору
ISO/IEC 27001 (Система управління ІБ)	Будь-яка організація ✓	Так ✓	Обов'язкове ✓	Часткова ~
NIST CSF 2.0 (Фреймворк кібербезпеки)	Критична інфраструктура ~	Ні ✗	Обов'язкове ✓	Часткова ~
PCI DSS (Платіжні картки)	Платіжна галузь ●	QSA-аудит ✓	Часткове ~	Обов'язкова ✓
GDPR (Захист персо-нальних даних)	Обробники перс. даних ●	Ні ✗	Часткове ~	Обов'язкова ✓

Умовні позначення:
✓ – повністю відповідає; ~ – частково відповідає; ✗ – не передбачено;
● – галузево-специфічний стандарт

Рисунок 1.3 – Порівняльна характеристика міжнародних стандартів і фреймворків кібербезпеки

Особливе місце в системі міжнародних стандартів займає Загальний регламент про захист даних ЄС (GDPR), що набув чинності у 2018 році. Хоча GDPR є регуляторним актом ЄС, а не стандартом у традиційному розумінні, він суттєво вплинув на практику захисту персональних даних у всьому світі. Регламент встановлює жорсткі вимоги до обробки персональних даних, права суб'єктів даних та відповідальність контролерів і обробників даних. Для України, яка прагне до євроінтеграції, адаптація законодавства до вимог GDPR є важливим завданням. Прийнятий у 2021 році Закон України «Про персональні дані» (у новій редакції) враховує ряд ключових положень GDPR та спрямований на подальшу гармонізацію українського законодавства з правом ЄС.

Інтеграція вимог різних стандартів є актуальним завданням для більшості організацій. Оскільки між ISO/IEC 27001, NIST CSF, GDPR та іншими нормативними документами існує значний рівень перетину, розробники систем управління безпекою намагаються максимально уніфікувати документацію та процеси, щоб одночасно відповідати вимогам кількох стандартів. Для вирішення цього завдання застосовуються спеціальні матриці відповідності (compliance mapping), які дозволяють встановити взаємозв'язок між вимогами різних стандартів і уникнути дублювання зусиль при побудові комплексної системи управління інформаційною безпекою.

Таблиця 1.2 – Порівняльна характеристика вимог ISO/IEC 27001 та NIST CSF

Критерій	ISO/IEC 27001	NIST CSF 2.0
Призначення	Вимоги до СУІБ (сертифікація)	Гнучкий фреймворк для управління кіберризиками
Структура	10 розділів + Додаток А (93 заходи)	6 функцій, 22 категорії, 106 підкатегорій
Сертифікація	Так, незалежними органами	Ні, самооцінка
Охоплення ризиків	Ризики інформаційної безпеки	Ризики кібербезпеки загалом
Цільова аудиторія	Організації будь-якого розміру	Переважно критична інфраструктура США

ЛЕКЦІЯ 2. ПОЛІТИКИ БЕЗПЕКИ ТА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ В ОРГАНІЗАЦІЇ

2.1. Концепція та ієрархія документів системи управління інформаційною безпекою

Документаційне забезпечення є невід'ємною складовою будь-якої системи управління інформаційною безпекою. Без чітко сформульованих та належно оформлених документів неможливо забезпечити послідовне та відтворюване виконання процесів безпеки, провести аудит або довести відповідність вимогам стандартів. Ієрархія документів СУІБ традиційно будується у вигляді піраміди: на верхньому рівні — Політика інформаційної безпеки як стратегічний документ, нижче — стандарти та керівні принципи, далі — процедури та інструкції, і на нижньому рівні — записи та докази відповідності. Така структура забезпечує чіткий розподіл між стратегічними намірами та операційними практиками.

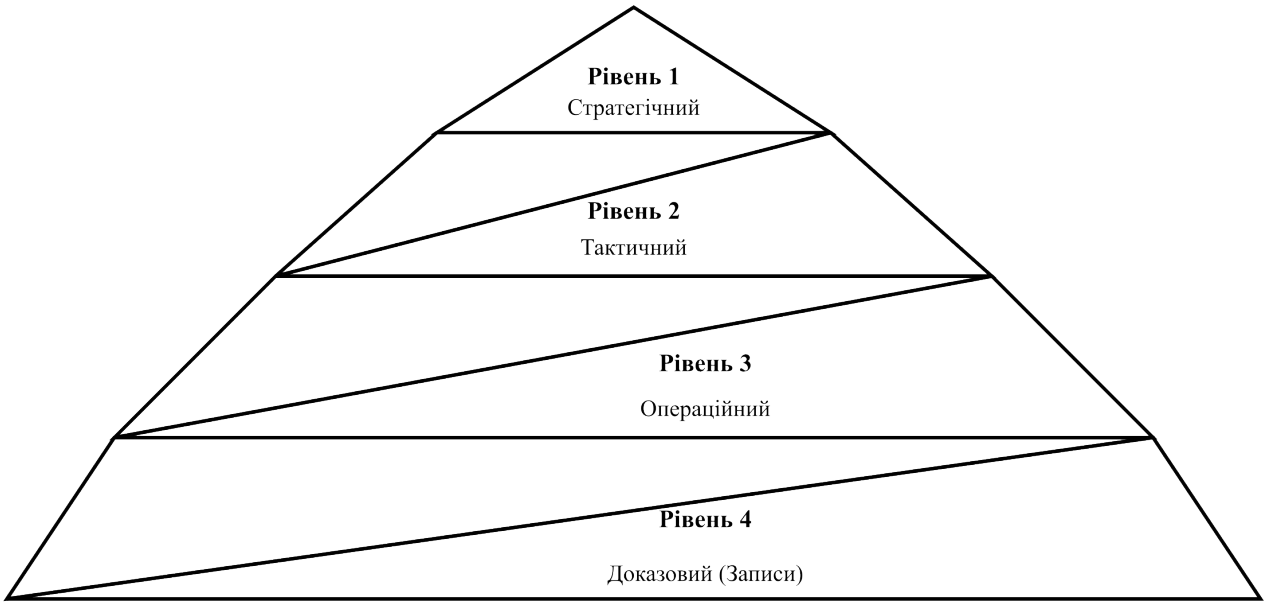
Політика інформаційної безпеки (ПІБ) є документом найвищого рівня в системі управління безпекою. Вона визначає загальні цілі, принципи та підходи організації до захисту інформації, встановлює розподіл відповідальності та повноважень у сфері безпеки, а також задає тон для всього комплексу заходів безпеки. ПІБ має бути затверджена вищим керівництвом організації, що демонструє підтримку ініціативи безпеки на стратегічному рівні. Згідно з вимогами ISO/IEC 27001, Політика інформаційної безпеки повинна відповідати стратегічному спрямуванню організації, включати зобов'язання щодо виконання застосовних вимог та постійного вдосконалення СУІБ.

Стандарти безпеки конкретизують вимоги Політики для певних сфер діяльності — управління доступом, класифікації інформації, захисту мереж, шифрування тощо. На відміну від Політики, стандарти містять вимірювані та конкретні вимоги, зокрема мінімальну довжину паролів, вимоги до криптографічних алгоритмів або частоту резервного копіювання даних. Процедури деталізують порядок виконання конкретних дій для досягнення відповідності стандартам. Вони описують покрокові інструкції для типових операцій безпеки: налаштування засобів захисту, реагування на інциденти, проведення перевірок тощо. Нижній рівень ієрархії — записи — зберігає докази того, що заплановані заходи безпеки дійсно виконуються.

Розробка та підтримка ієрархії документів безпеки — трудомісткий, але необхідний процес. Документи повинні регулярно переглядатися та актуалізуватися з урахуванням змін у технологічному середовищі, законодавстві та загрозах. Ключовим принципом є відповідність між задокументованими

вимогами та реальною практикою — документи не повинні бути формальними, а відображати дійсний стан справ в організації. Для забезпечення ефективності документальної системи необхідно визначити відповідальних за кожен документ, встановити процедури перегляду та затвердження, а також забезпечити доступність документів для всього персоналу, якого вони стосуються.

Ієрархія документів СУІБ організації зображена на рисунку 2.1. На рисунку 2.1 показана піраміда, розділена горизонтальними лініями на чотири рівні.



Приклади документів за рівнями:

Рівень 1: Політика ІБ організації | Рівень 2: Стандарт управління паролями

Рівень 3: Процедура резервного копіювання | Рівень 4: Журнал аудиту доступу

Рисунок 2.1 – Ієрархія документів системи управління інформаційною безпекою

Класифікація інформації є важливим інструментом управління безпекою. Відповідно до міжнародних практик інформація класифікується за рівнями конфіденційності, що визначають необхідний рівень її захисту. Типові категорії класифікації в корпоративному середовищі: відкрита (Public), для внутрішнього використання (Internal), конфіденційна (Confidential) та таємна (Secret або Restricted). Для кожної категорії встановлюються конкретні правила поводження: доступ, обробка, зберігання, передача та знищення. Без чіткої класифікації інформації неможливо ефективно застосовувати заходи безпеки, оскільки різні категорії даних потребують різних рівнів захисту.

2.2. Розробка та впровадження ключових політик безпеки

Повноцінна система управління кібербезпекою організації охоплює широкий спектр тематичних політик. Поряд із загальною Політикою інформаційної безпеки необхідними є Політика управління доступом, Політика захисту кінцевих точок, Політика управління паролями, Політика резервного копіювання, Політика реагування на інциденти, Політика прийнятного використання інформаційних систем та ряд інших. Кожна з цих політик охоплює конкретну сферу безпеки та встановлює вимоги, відповідальних і заходи контролю, що стосуються саме цієї сфери.

Політика управління доступом визначає принципи надання, перегляду та відкликання прав доступу до інформаційних ресурсів організації. В її основі лежать принципи найменших привілеїв (least privilege) — надання користувачам лише тих прав, які необхідні для виконання їхніх службових обов'язків — та розподілу обов'язків (separation of duties), що запобігає зосередженню критичних функцій в одних руках. Політика також регулює питання управління привілейованими обліковими записами (адміністраторами систем), що є однією з найбільш критичних сфер безпеки. Привілейовані облікові записи повинні перебувати під особливим контролем, а їхнє використання ретельно журналюватися.

Таблиця 2.1 – Типові розділи Політики управління доступом

Розділ	Зміст розділу
Цілі та сфера застосування	Визначення цілей документа та перелік систем і ресурсів, на які він поширюється
Принципи управління доступом	Найменші привілеї, розподіл обов'язків, обґрунтованість доступу
Процедура надання доступу	Запит, авторизація, технічне налаштування, документування
Процедура відкликання доступу	Порядок відкликання при звільненні, зміні посади або за ініціативою СБ
Перегляд прав доступу	Регулярне рецертифікування доступу (не рідше ніж раз на рік)
Привілейовані облікові записи	Умови надання, використання, ротація паролів, журналювання

Управління мобільними пристроями та дистанційним доступом набуває особливого значення в умовах поширення практики роботи з дому та використання особистих пристроїв у корпоративних цілях (BYOD — Bring Your Own Device). Відповідна політика повинна встановлювати вимоги до безпеки пристроїв, що використовуються для доступу до корпоративних ресурсів,

зокрема обов'язкове шифрування, встановлення засобів захисту (антивірус, MDM-рішень), заборону несанкціонованих програм, а також процедури у випадку втрати або крадіжки пристрою. Поширення хмарних технологій додатково ускладнює завдання управління доступом, оскільки корпоративні ресурси дедалі більше розміщуються поза традиційним периметром безпеки.

Розробка та впровадження політики реагування на інциденти інформаційної безпеки є критично важливим завданням для будь-якої організації. Ця політика визначає, що вважається інцидентом безпеки, яким є порядок його ідентифікації та класифікації, хто відповідає за реагування та які кроки мають бути вжиті на кожному етапі. Без заздалегідь розробленої та відпрацьованої процедури реагування на інциденти організація ризикує зазнати значних збитків через неефективну та безсистемну реакцію на кіберінцидент. Практика свідчить, що саме відсутність плану реагування є однією з головних причин катастрофічних наслідків кібератак.

Впровадження розроблених політик є не менш складним завданням, ніж їхня розробка. Навіть найдосконаліша політика залишається марною, якщо вона не виконується персоналом. Для успішного впровадження необхідно забезпечити: по-перше, підтримку керівництва, яке повинне не лише затвердити документ, а й демонструвати його дотримання на власному прикладі; по-друге, навчання та роз'яснення персоналу вимог політики та причин їхньої необхідності; по-третє, технічне впровадження засобів контролю, що унеможливлюють або ускладнюють порушення; по-четверте, моніторинг дотримання та реагування на порушення. Лише комплексний підхід до впровадження забезпечує реальне підвищення рівня безпеки, а не лише формальне виконання вимог.

2.3. Організаційна структура управління кібербезпекою

Ефективне управління кібербезпекою неможливе без чіткої організаційної структури та розподілу відповідальності. У великих організаціях зазвичай функціонують спеціалізовані підрозділи: Служба інформаційної безпеки (СІБ), Центр операцій безпеки (SOC — Security Operations Center), групи реагування на комп'ютерні інциденти (CERT/CSIRT). У менших організаціях ці функції можуть бути об'єднані або виконуватися одним фахівцем. Незалежно від розміру організації, ключовим є забезпечення незалежності функції інформаційної безпеки від IT-підрозділу, оскільки безпека покликана контролювати й оцінювати, а не лише обслуговувати інформаційні системи.

Ключовою посадою в системі управління кібербезпекою є CISO (Chief Information Security Officer) — директор з інформаційної безпеки. CISO

відповідає за формування стратегії кібербезпеки організації, забезпечення відповідності вимогам законодавства та стандартів, управління командою безпеки та комунікацію з топ-менеджментом щодо ризиків безпеки. Позиція CISO в організаційній ієрархії суттєво впливає на ефективність управління безпекою: ідеальним вважається безпосереднє підпорядкування генеральному директору або Раді директорів, що забезпечує необхідну незалежність та рівень повноважень.

Типова організаційна структура управління кібербезпекою у середній та великій організації зображена на рисунку 2.2.

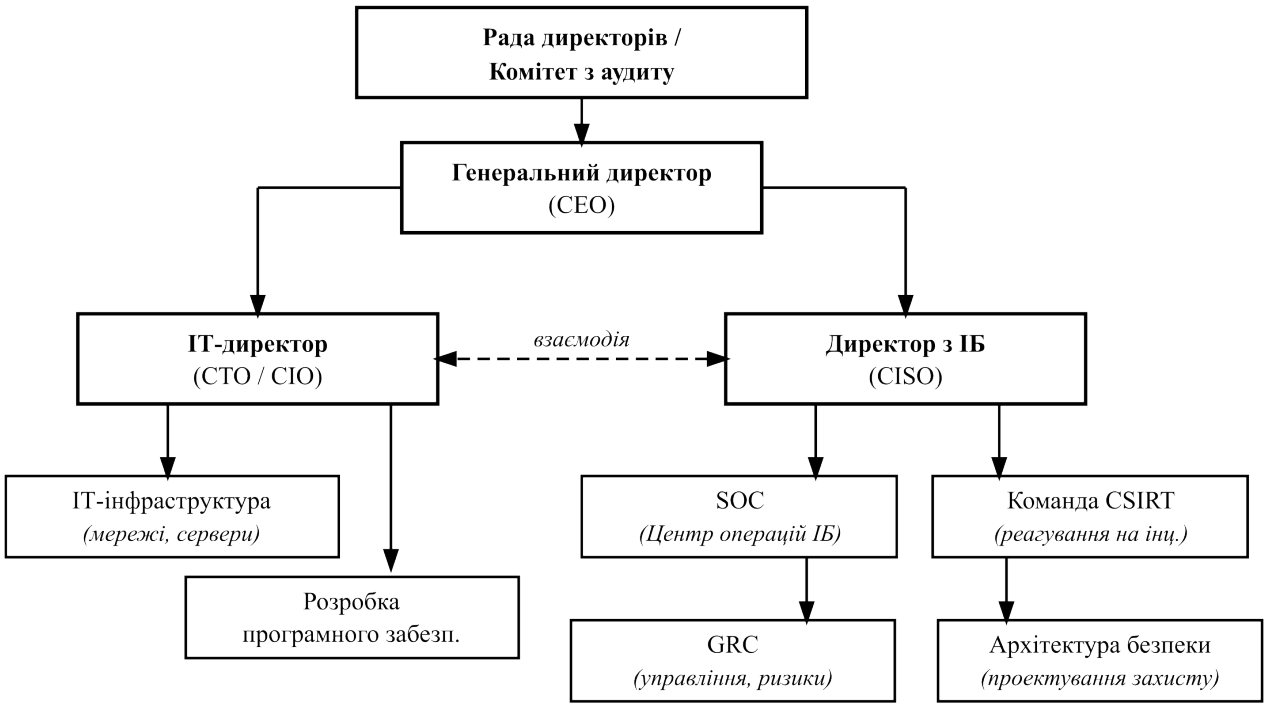


Рисунок 2.2 – Типова організаційна структура управління кібербезпекою

Концепція GRC (Governance, Risk Management, Compliance — Управління, управління ризиками, відповідність) набула широкого поширення як комплексний підхід до управління кібербезпекою та корпоративного управління загалом. Governance охоплює стратегічне керівництво, розподіл відповідальності та механізми прийняття рішень у сфері безпеки. Risk Management включає ідентифікацію, оцінку та обробку ризиків інформаційної безпеки. Compliance забезпечує відповідність вимогам законодавства, стандартів та контрактних зобов'язань. Інтегрований підхід GRC дозволяє уникнути розрізненості зусиль та забезпечити узгоджене управління безпекою на всіх рівнях організації.

Культура безпеки є тим нематеріальним чинником, який багато в чому визначає реальний рівень захищеності організації. Навіть найдосконаліші

технічні засоби та процедури безпеки виявляються неефективними, якщо співробітники не розуміють їхньої важливості або свідомо обходять встановлені обмеження. Формування культури безпеки — довгостроковий процес, що вимагає постійних зусиль з навчання, комунікації та мотивації персоналу. Програма підвищення обізнаності у сфері безпеки (Security Awareness) є стандартним інструментом формування культури безпеки і включає регулярні тренінги, розсилки, імітаційні фішингові атаки та інші методи підвищення рівня свідомості персоналу щодо кіберзагроз.

Управління ланцюгом постачання (Supply Chain Security) є відносно новим, але надзвичайно важливим аспектом управління кібербезпекою. Кібератаки через ланцюг постачання, зокрема атака на SolarWinds у 2020 році та атака на програмне забезпечення Kaseya у 2021 році, продемонстрували катастрофічні наслідки недостатньої перевірки постачальників. Організації повинні оцінювати ризики безпеки не лише своїх власних систем, а й систем їхніх постачальників, підрядників та сервісних провайдерів. Вимоги до безпеки постачальників мають бути включені в договори та регулярно перевірятися, а перелік довірених постачальників — постійно актуалізуватися.

Таблиця 2.2 – Ролі та відповідальність у системі управління інформаційною безпекою

Роль	Основні обов'язки	Рівень відповідальності
Рада директорів	Затвердження стратегії ІБ, нагляд за управлінням ризиками	Стратегічний
CISO	Керівництво функцією ІБ, управління командою, звітність перед CEO	Стратегічний / Тактичний
Менеджер SOC	Операційне управління моніторингом та реагуванням на інциденти	Тактичний / Операційний
Аналітик SOC	Аналіз подій безпеки, виявлення загроз, ескалація інцидентів	Операційний
Власник інформаційних активів	Класифікація активів, авторизація доступу, прийняття ризиків	Тактичний
Усі співробітники	Дотримання політик, звітування про підозрілі події	Операційний

ЛЕКЦІЯ 3. УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1. Концептуальні основи управління ризиками інформаційної безпеки

Управління ризиками є центральним процесом у системі управління інформаційною безпекою. Концепція ризику в сфері ІБ базується на розумінні того, що неможливо усунути всі загрози та вразливості, а отже, необхідно свідомо управляти залишковим рівнем ризику. Ризик інформаційної безпеки визначається як можливість того, що певна загроза скористається вразливістю активу та спричинить шкоду організації. Математично ризик традиційно виражається як добуток ймовірності реалізації загрози та величини потенційних збитків, хоча на практиці оцінка обох компонентів є складним завданням.

Фундаментальні поняття управління ризиками ІБ утворюють взаємопов'язану понятійну систему. Актив (asset) — це будь-що, що має цінність для організації: інформація, програмне та апаратне забезпечення, люди, репутація тощо. Загроза (threat) — потенційна причина небажаного інциденту, що може завдати шкоди активу або організації. Вразливість (vulnerability) — слабке місце активу або засобу управління безпекою, яке може бути використане загрозою. Вплив (impact) — наслідки для організації у випадку реалізації ризику. Розуміння взаємодії між цими поняттями є необхідною передумовою для проведення якісної оцінки ризиків.

Стандарт ISO/IEC 27005 визначає процес управління ризиками ІБ як ітеративний та циклічний. Він складається з таких етапів: встановлення контексту (визначення сфери застосування, критеріїв ризику та організаційного контексту), оцінка ризиків (ідентифікація, аналіз та оцінювання ризиків), обробка ризиків (вибір та впровадження заходів безпеки), прийняття ризиків (рішення керівництва про прийнятність залишкових ризиків), комунікація та консультації щодо ризиків, а також моніторинг та перегляд ризиків. Ключовим є ітеративний характер процесу: оцінка та обробка ризиків повторюються доти, доки залишкові ризики не досягнуть прийнятного рівня.

Процес управління ризиками інформаційної безпеки відповідно до ISO/IEC 27005 проілюстровано на рисунку 3.1.

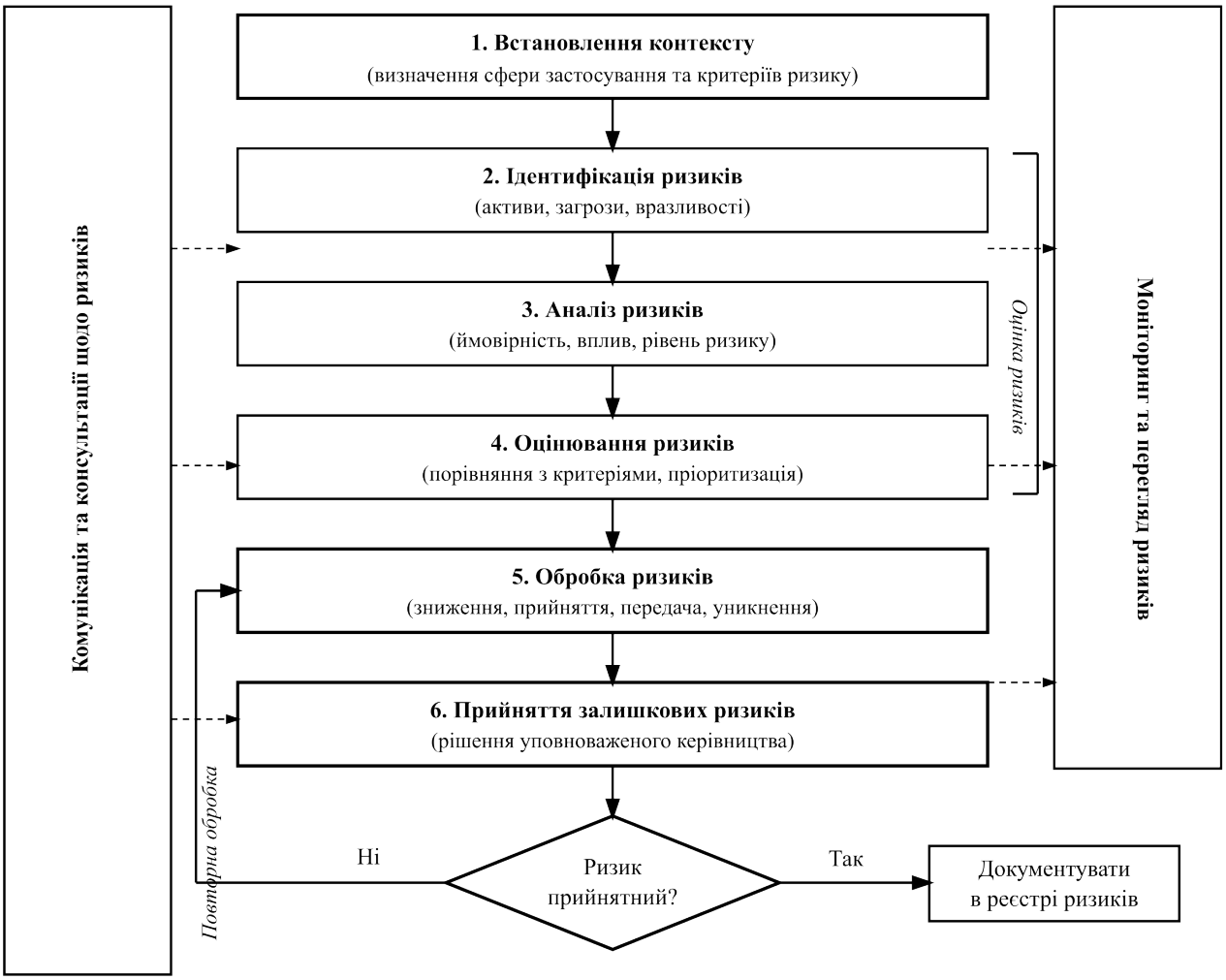


Рисунок 3.1 – Процес управління ризиками ІБ (ISO/IEC 27005)

Критерії прийнятного ризику є важливою передумовою для проведення оцінки ризиків. Організація повинна заздалегідь визначити, який рівень ризику вона готова прийняти, не вживаючи додаткових заходів захисту. Ці критерії залежать від галузі, розміру організації, вимог регуляторів, стратегії бізнесу та апетиту до ризику керівництва. У державних органах та критичній інфраструктурі вимоги до прийнятного рівня ризику, як правило, суттєво жорсткіші, ніж у комерційних організаціях. Відсутність чітко визначених критеріїв прийнятного ризику призводить до непослідовних рішень та труднощів при порівнянні та пріоритизації ризиків.

Реєстр ризиків є ключовим документом процесу управління ризиками. Він містить перелік ідентифікованих ризиків разом з їхніми характеристиками: описом ризику, відповідним активом, загрозою та вразливістю, ймовірністю та впливом (у числовому або якісному вираженні), рівнем ризику, обраним способом обробки, відповідальним власником ризику та строками впровадження заходів. Реєстр ризиків повинен регулярно оновлюватися та переглядатися — як за розкладом (наприклад, щорічно), так і у відповідь на суттєві зміни: появу

нових загроз, впровадження нових систем або зміни в організаційному середовищі.

3.2. Методи оцінки ризиків інформаційної безпеки

Якісні методи оцінки ризиків базуються на суб'єктивних оцінках фахівців і не потребують точних числових даних. Найпоширенішим якісним інструментом є матриця ризиків — двовимірна таблиця, в якій за осями відкладаються ймовірність загрози та потенційний вплив на активи організації. Кожна комбінація ймовірності та впливу відповідає певному рівню ризику (наприклад, від 1 до 5 або від «низький» до «критичний»). Матриця ризиків є інтуїтивно зрозумілим і швидким інструментом, що дозволяє наочно відобразити розподіл ризиків та пріоритизувати заходи безпеки.

Таблиця 3.1 – Матриця оцінки ризиків (5×5)

Вплив \ Ймовірність	Дуже низька (1)	Низька (2)	Середня (3)	Висока (4)	Дуже висока (5)
Критичний (5)	5 – Середній	10 – Високий	15 – Критичний	20 – Критичний	25 – Критичний
Значний (4)	4 – Низький	8 – Середній	12 – Високий	16 – Критичний	20 – Критичний
Помірний (3)	3 – Низький	6 – Середній	9 – Середній	12 – Високий	15 – Критичний
Незначний (2)	2 – Мінімальний	4 – Низький	6 – Середній	8 – Середній	10 – Високий
Мінімальний (1)	1 – Мінімальний	2 – Мінімальний	3 – Низький	4 – Низький	5 – Середній

Кількісні методи оцінки ризиків прагнуть виразити ризик у числових, переважно фінансових показниках. Базовими поняттями кількісної оцінки є AV (Asset Value — вартість активу), EF (Exposure Factor — коефіцієнт впливу, що показує, яка частина вартості активу втрачається при реалізації ризику), SLE (Single Loss Expectancy — очікувані втрати від одноразового інциденту, розраховується як AV × EF), ARO (Annualized Rate of Occurrence — річна частота реалізації ризику) та ALE (Annualized Loss Expectancy — річні очікувані втрати, розраховується як SLE × ARO). Порівняння ALE з вартістю засобів захисту дозволяє обґрунтувати економічну доцільність інвестицій у безпеку.

Кількісна оцінка ризиків має суттєві переваги та недоліки. Серед переваг — об'єктивність результатів, можливість прямого порівняння різних ризиків та фінансового обґрунтування заходів безпеки перед керівництвом. Однак точна кількісна оцінка вимагає значного обсягу достовірних вихідних даних — статистики інцидентів, даних про реальну вартість активів, актуарних показників ймовірності подій. На практиці такі дані часто відсутні або є недостатньо надійними, що знижує точність кількісних оцінок. Тому найпоширенішим на практиці є гібридний підхід, що поєднує якісну категоризацію ризиків з кількісними оцінками для найбільш критичних активів.

Методологія OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) є одним з найвідоміших комплексних методів оцінки ризиків, розроблених у Університеті Карнегі-Меллон. Метод орієнтований на самооцінку і дозволяє організації власними силами провести оцінку ризиків, не залучаючи зовнішніх консультантів. OCTAVE Allegro, одна із сучасних версій методу, зосереджена насамперед на оцінці ризиків для інформаційних активів і складається з восьми кроків: встановлення критеріїв вимірювання ризику, розробка профілю інформаційних активів, ідентифікація контейнерів активів, ідентифікація зон захопленості, визначення сценаріїв загроз, ідентифікація ризиків, аналіз ризиків та відбір підходу до обробки ризиків.

Методи моделювання загроз є важливим доповненням до традиційних методів оцінки ризиків, особливо в контексті розробки програмного забезпечення та проектування архітектур систем. Методологія STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege), розроблена в Microsoft, класифікує загрози за шістьма категоріями та допомагає систематично ідентифікувати потенційні загрози для кожного компонента системи. Метод PASTA (Process for Attack Simulation and Threat Analysis) є більш комплексним і включає сімірівневий процес аналізу від бізнес-цілей до симуляції атак. Застосування методів моделювання загроз на ранніх стадіях розробки дозволяє значно знизити вартість усунення вразливостей порівняно з виправленням проблем після розгортання системи.

Порівняння якісних та кількісних методів оцінки ризиків ІБ наведено на рисунку 3.2.

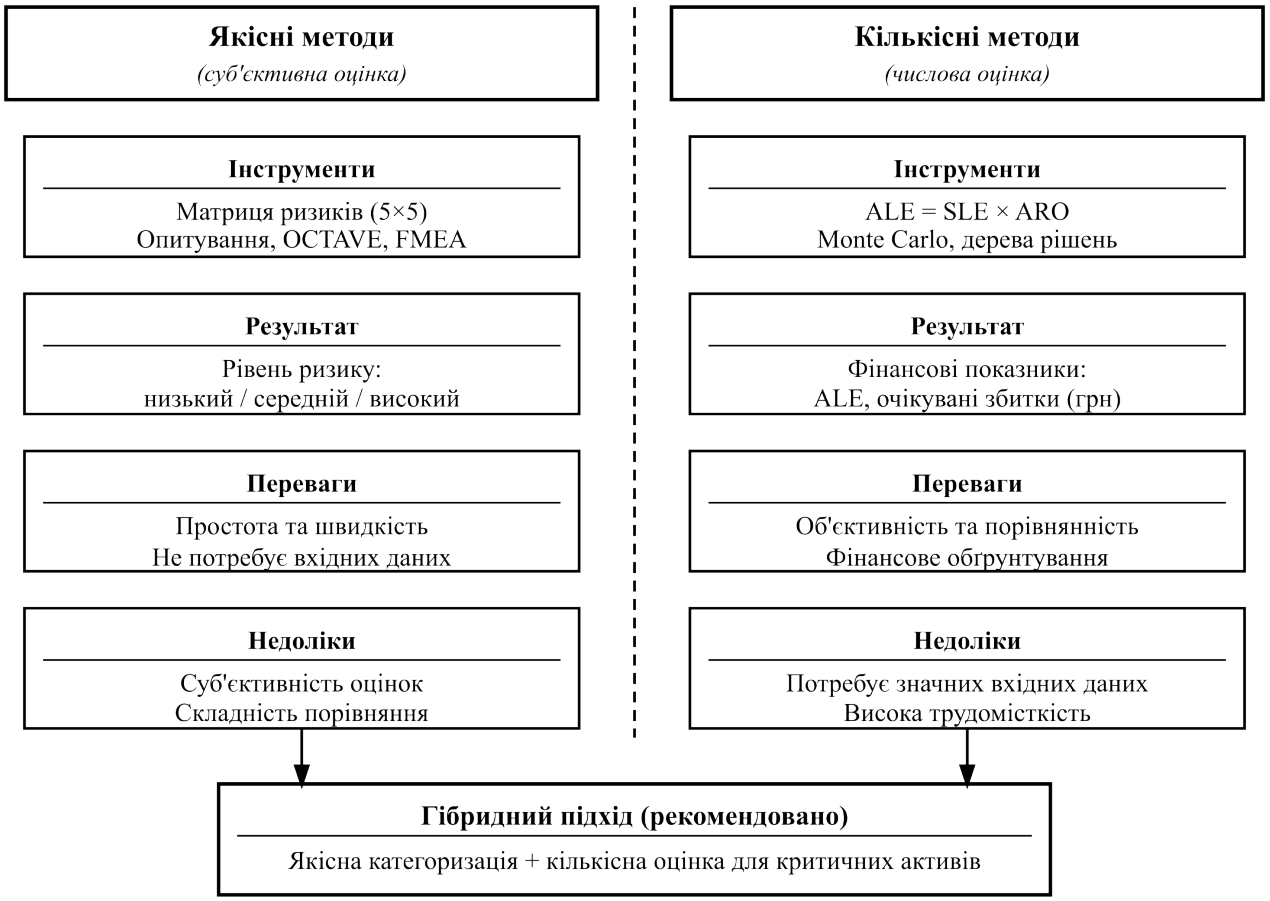


Рисунок 3.2 – Порівняння якісних та кількісних методів оцінки ризиків

3.3. Обробка ризиків та моніторинг ефективності заходів безпеки

За результатами оцінки ризиків організація обирає стратегію обробки для кожного ідентифікованого ризику. Стандарт ISO/IEC 27005 виділяє чотири основні стратегії обробки ризиків: модифікація ризику (зниження ризику через впровадження засобів безпеки), збереження ризику (прийняття ризику у разі, якщо він знаходиться в межах прийнятного рівня або вартість його зниження перевищує потенційні збитки), уникнення ризику (відмова від діяльності, що породжує ризик) та передача ризику (перенесення відповідальності за ризик на третю сторону, наприклад через страхування або аутсорсинг). На практиці для більшості ризиків застосовується комбінація цих стратегій.

Вибір заходів безпеки (контролів) для зниження ризиків є ключовим кроком у процесі обробки ризиків. Відповідно до ISO/IEC 27001, організація повинна визначити та впровадити необхідні засоби управління безпекою з числа тих, що наведені в Додатку А до стандарту, та/або інші засоби, що відповідають її специфіці. При виборі заходів безпеки необхідно оцінювати не лише їхню ефективність у зниженні ризику, а й вартість впровадження та підтримки, можливий вплив на бізнес-процеси, а також залишковий ризик після

впровадження заходу. Документ «Декларація про застосовність» (Statement of Applicability) фіксує рішення організації щодо кожного можливого заходу безпеки та обґрунтування цих рішень.

Моніторинг та вимірювання ефективності заходів безпеки є необхідними для забезпечення того, що впроваджені контролі дійсно функціонують та забезпечують запланований рівень захисту. ISO/IEC 27004 містить рекомендації щодо розробки метрик та показників ефективності СУІБ. Метрики безпеки можна розділити на три категорії: метрики впровадження (наприклад, відсоток систем, охоплених антивірусним захистом), метрики ефективності (наприклад, середній час виявлення інциденту) та метрики результативності (наприклад, кількість успішних атак або розмір фінансових збитків від інцидентів). Регулярне вимірювання та аналіз метрик дозволяє керівництву отримувати об'єктивну картину стану безпеки.

Таблиця 3.2 – Приклади метрик ефективності системи управління ІБ

Категорія метрики	Назва метрики	Формула / Опис	Цільове значення
Впровадження	Охоплення патчами	% систем з актуальними оновленнями	> 95%
Впровадження	Навчання з ІБ	% персоналу, що пройшов навчання за рік	100%
Ефективність	MTTD (Mean Time to Detect)	Середній час виявлення інциденту	< 24 год.
Ефективність	MTTR (Mean Time to Respond)	Середній час реагування на інцидент	< 4 год.
Результативність	Кількість інцидентів ІБ	Кількість підтверджених інцидентів на місяць	Тенденція до зниження
Результативність	Вартість інцидентів	Загальні збитки від інцидентів ІБ за рік (грн)	Тенденція до зниження

Управління залишковим ризиком є важливим аспектом, що нерідко залишається поза увагою. Після впровадження всіх обраних заходів безпеки в організації завжди залишається певний рівень залишкового ризику — той ризик, який не був повністю усунутий. Залишковий ризик повинен бути явно ідентифікований, задокументований та прийнятий уповноваженим керівництвом. Важливо, щоб рішення про прийняття залишкового ризику приймалося свідомо та на відповідному рівні відповідальності — адже безпека завжди є компромісом між рівнем захисту та вартістю його забезпечення.

Страхування кіберризиків (cyber insurance) є відносно новим, але інтенсивно зростаючим ринком послуг, що дозволяє організаціям фінансово захиститися від наслідків кіберінцидентів. Поліс кіберстрахування може

покривати витрати на розслідування та ліквідацію наслідків інциденту, витрати на юридичну підтримку, штрафи від регуляторів, збитки від перерви в діяльності та виплати потерпілим. Ринок кіберстрахування активно розвивається у зв'язку із зростанням масштабів кіберзагроз: лише за 2019–2022 роки середні страхові премії зросли в кілька разів. При цьому страховики дедалі більше вимагають від застрахованих організацій підтвердження певного базового рівня кіберзахисту як умови видачі поліса.

Логіку прийняття рішень щодо обробки ризиків інформаційної безпеки наведено на рисунку 3.3.

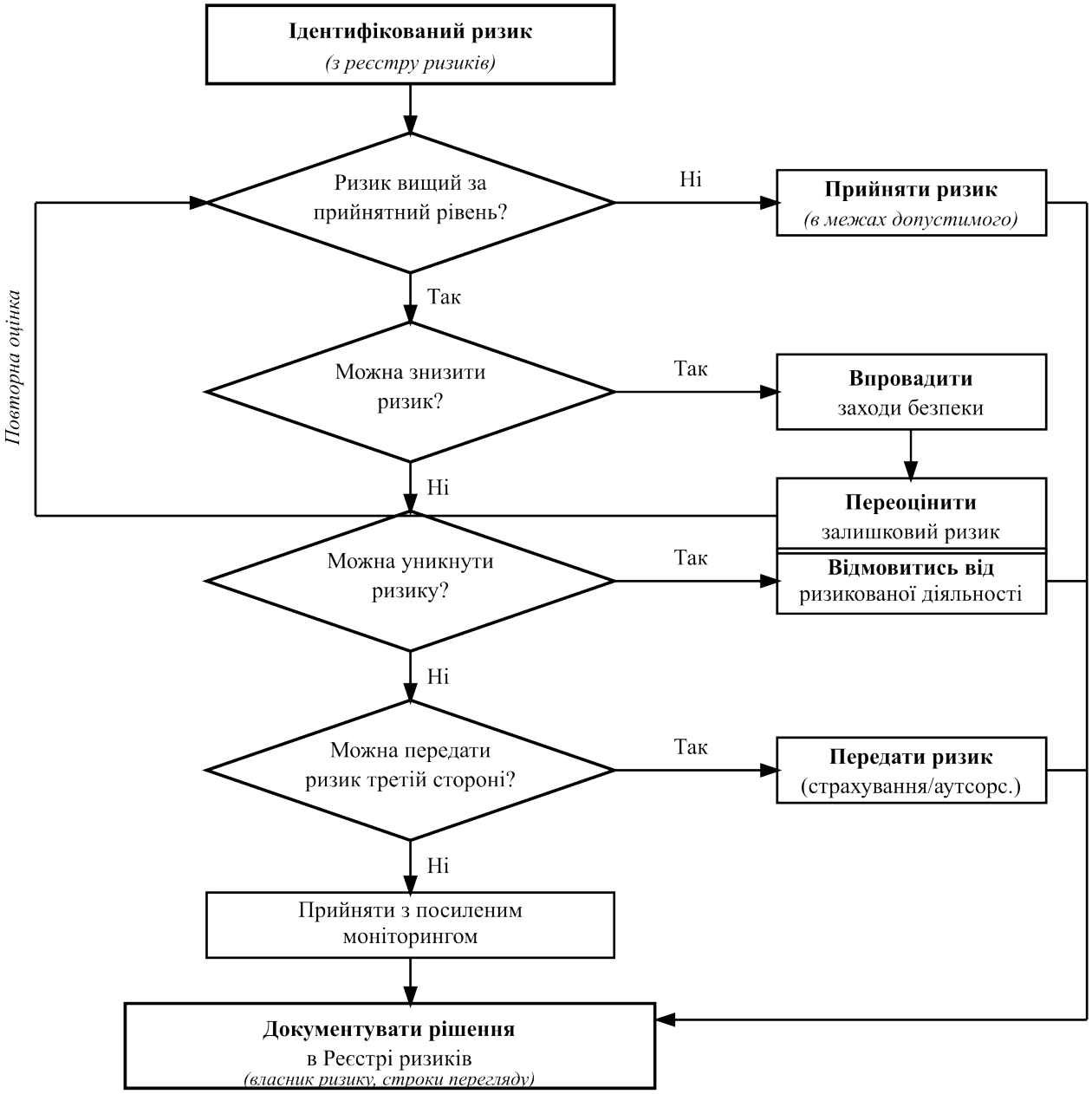


Рисунок 3.3 – Схема прийняття рішень щодо обробки ризиків ІБ

Зв'язок між управлінням ризиками та плануванням безперервності бізнесу (Business Continuity Planning, BCP) є нерозривним. Результати оцінки ризиків є вхідними даними для розробки Плану забезпечення безперервності бізнесу та Плану відновлення після катастрофи (Disaster Recovery Plan, DRP). Ці плани визначають, як організація буде функціонувати в умовах реалізації найбільш серйозних ризиків — наприклад, повного відключення основного дата-центру, масштабної кібератаки або пандемії. Ключовими показниками для BCP/DRP є RTO (Recovery Time Objective — максимально допустимий час відновлення) та RPO (Recovery Point Objective — максимально допустима втрата даних), що визначаються за результатами аналізу критичності бізнес-процесів.

Комунікація ризиків є невід'ємною складовою управління ризиками ІБ, оскільки рішення щодо ризиків приймаються на різних рівнях організації. Стратегічні ризики звітуються перед вищим керівництвом та Радою директорів у форматі звітів, що акцентують увагу на бізнес-наслідках та фінансових показниках. Тактичні та операційні ризики обговорюються на рівні менеджерів підрозділів та фахівців з безпеки. При комунікації ризиків важливо адаптувати мову та рівень деталізації до аудиторії: технічні деталі вразливостей, зрозумілі аналітику безпеки, є зайвими для генерального директора, якому важливіша інформація про потенційні фінансові збитки та репутаційні наслідки. Якісна комунікація ризиків забезпечує усвідомлені рішення на всіх рівнях та підтримку заходів безпеки з боку керівництва.

ЛЕКЦІЯ 4 МОНІТОРИНГ, ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА ІНЦИДЕНТИ

4.1. Безперервний моніторинг безпеки та системи виявлення подій

Сучасна концепція управління інформаційною безпекою нерозривно пов'язана з принципом безперервного моніторингу, який передбачає постійне автоматизоване спостереження за станом інформаційної інфраструктури організації. Безперервний моніторинг безпеки — це систематичний процес збору, аналізу та інтерпретації даних про події та стани інформаційних систем з метою своєчасного виявлення відхилень від встановленої норми та потенційних загроз. На відміну від епізодичного аудиту, постійний моніторинг забезпечує актуальну картину стану захищеності, дозволяючи оперативно реагувати на виникаючі загрози ще до того, як вони завдадуть суттєвої шкоди. Стандарт NIST SP 800-137 визначає такий підхід як «Information Security Continuous Monitoring», підкреслюючи його роль у підтримці ситуаційної обізнаності організації щодо стану кіберзахисту.

Архітектура системи безперервного моніторингу формується навколо кількох ключових компонентів: джерел даних, механізмів збору та передачі, аналітичного ядра та підсистеми реагування. Джерелами даних слугують мережеві пристрої (маршрутизатори, комутатори, міжмережеві екрани), сервери, робочі станції, прикладне програмне забезпечення, бази даних та хмарні сервіси. Кожен із цих компонентів генерує журнали подій — log-файли, що фіксують дії користувачів, системні операції, мережеві з'єднання та помилки. Механізми збору журналів реалізуються через агентів моніторингу, встановлених на кінцевих вузлах, або через безагентний збір даних по мережевих протоколах. Критично важливою є синхронізація системного часу на всіх вузлах, оскільки правильне встановлення хронологічної послідовності подій є обов'язковою умовою якісного аналізу інцидентів.

Серед найпоширеніших інструментів безперервного моніторингу особливе місце займають системи класу SIEM (Security Information and Event Management). SIEM-системи агрегують журнали подій з усіх компонентів інформаційної інфраструктури, нормалізують їх до єдиного формату, кореляційно аналізують та формують сповіщення для персоналу служби безпеки. Принцип кореляції подій полягає в тому, що система не просто фіксує окремі аномалії, а виявляє логічні зв'язки між подіями, які розрізнено виглядають нешкідливими, але разом утворюють патерн атаки. Наприклад, кілька невдалих спроб входу на різних вузлах мережі протягом короткого часу можуть свідчити про автоматизовану атаку перебором паролів, тоді як кожна окремо виглядала б

як рядова помилка користувача. Провідними комерційними платформами SIEM є Splunk, IBM QRadar, Microsoft Sentinel та ArcSight від OpenText.

Паралельно з SIEM-рішеннями широко застосовуються системи виявлення вторгнень (IDS) та запобігання вторгненням (IPS). IDS-системи функціонують у пасивному режимі: вони аналізують мережевий трафік або поведінку хостів та генерують сповіщення при виявленні підозрілої активності, не втручаючись у сам трафік. IPS-системи, навпаки, розміщуються в розрив мережевого з'єднання та здатні активно блокувати шкідливий трафік у реальному часі. Розрізняють також мережеві системи виявлення вторгнень (NIDS), що аналізують пакети на рівні мережі, та хостові (HIDS), що контролюють файлову систему, реєстр операційної системи та запущені процеси на окремому вузлі. Ефективність IDS/IPS значною мірою залежить від актуальності бази сигнатур атак, яку виробники регулярно оновлюють відповідно до розвитку ландшафту загроз.

На рисунку 4.1 представлена архітектура системи безперервного моніторингу безпеки, що охоплює всі рівні інформаційної інфраструктури організації — від кінцевих вузлів до центральної аналітичної платформи.

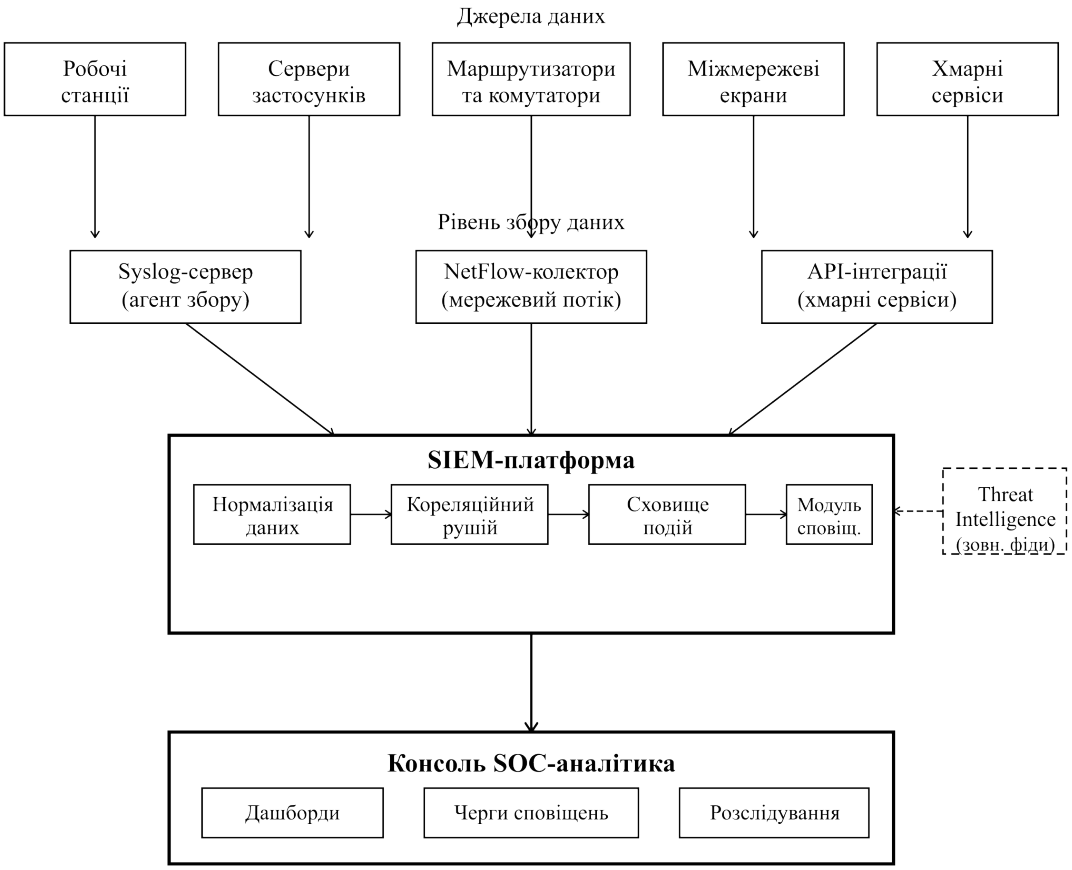


Рисунок 4.1 — Архітектура системи безперервного моніторингу безпеки

Важливим елементом сучасного моніторингу є концепція операційного центру безпеки (Security Operations Center, SOC). SOC — це структурний

підрозділ або аутсорсинговий сервіс, що цілодобово здійснює моніторинг, аналіз та реагування на інциденти інформаційної безпеки. Персонал SOC поділяється на кілька рівнів: аналітики першого рівня займаються початковою обробкою сповіщень та тріажем, аналітики другого рівня проводять глибше розслідування підозрілих подій, а фахівці третього рівня вирішують найскладніші випадки та займаються полюванням на загрози (threat hunting). Ефективність SOC залежить від правильно налаштованих правил кореляції, чітких процедур ескалації та відпрацьованих playbook-сценаріїв реагування, які детально описують кроки аналітика для кожного типу інциденту.

Окремої уваги заслуговує концепція аналізу поведінки користувачів та об'єктів (User and Entity Behavior Analytics, UEBA). UEBA-системи будують статистичні моделі нормальної поведінки кожного користувача та системи на основі накопичених даних, а потім виявляють статистично значимі відхилення від цих моделей. Такий підхід дозволяє виявляти інсайдерські загрози, компрометацію облікових записів та приховані атаки, які не мають відомих сигнатур. Наприклад, якщо рядовий бухгалтер раптово починає масово завантажувати конфіденційні технічні документи о третій ночі — UEBA-система зафіксує це як аномалію і підніме тривогу, навіть якщо дії технічно не порушують жодного правила доступу. Сучасні SIEM-рішення все частіше інтегрують UEBA-функціональність безпосередньо у свій аналітичний модуль.

У таблиці 4.1 наведено порівняльну характеристику основних інструментів моніторингу інформаційної безпеки за їхніми функціональними можливостями та застосуванням.

Таблиця 4.1 — Порівняльна характеристика інструментів моніторингу безпеки

Інструмент	Тип аналізу	Рівень захисту	Основне призначення
SIEM	Кореляційний	Мережа / Хост	Агрегація, кореляція та сповіщення про події
IDS	Сигнатурний / Аномалійний	Мережа / Хост	Виявлення вторгнень без блокування
IPS	Сигнатурний	Мережа	Блокування шкідливого трафіку в реальному часі
UEBA	Поведінковий / ML	Користувач / Об'єкт	Виявлення аномальної поведінки на основі моделей
NDR	Аномалійний / AI	Мережа	Виявлення прихованих загроз у мережевому трафіку
EDR	Поведінковий	Кінцевий вузол	Захист та видимість на рівні робочих станцій і серверів

4.2. Управління інцидентами інформаційної безпеки

Управління інцидентами інформаційної безпеки (Incident Management) є одним із центральних процесів у системі управління кібербезпекою організації. Інцидент інформаційної безпеки — це будь-яка подія або серія подій, що становить реальну або потенційну загрозу конфіденційності, цілісності чи доступності інформаційних активів. Важливо розрізняти поняття «подія» і «інцидент»: будь-який інцидент є подією, але далеко не кожна подія є інцидентом. Стандарт ISO/IEC 27035 «Information security incident management» визначає систематизований підхід до управління інцидентами, що включає підготовку, виявлення, оцінку, реагування, відновлення та аналіз постфактум. Цей підхід дозволяє не лише мінімізувати шкоду від конкретного інциденту, а й використовувати отримані уроки для вдосконалення системи захисту в цілому.

Класифікація інцидентів є необхідною умовою ефективного управління ними, оскільки різні типи інцидентів потребують різних процедур реагування та різного рівня ескалації. За своєю природою інциденти поділяються на: атаки на відмову в обслуговуванні (DoS/DDoS); несанкціонований доступ до систем або даних; розповсюдження шкідливого програмного забезпечення; витоки конфіденційних даних; атаки на вебзастосунки; компрометацію облікових даних; фішингові кампанії; порушення безперервності роботи критичних систем. За рівнем серйозності інциденти класифікують від критичного (P1), що потребує негайної реакції протягом хвилин, до мінімального (P4), що може бути вирішений у плановому порядку протягом тижнів. Визначення рівня серйозності базується на оцінці потенційного впливу на бізнес-процеси, кількості задіяних систем та чутливості скомпрометованих даних.

Ключовим документом, що регулює процес реагування, є план реагування на інциденти (Incident Response Plan, IRP). IRP — це формальний документ, що описує ролі та відповідальності членів команди реагування, процедури виявлення та класифікації, алгоритми реагування для різних типів інцидентів, порядок комунікацій та ескалації, а також вимоги до документування та звітності. Поряд із IRP організації розробляють більш детальні операційні посібники — playbook, що крок за кроком описують дії аналітика при конкретному типі інциденту. Наприклад, playbook для реагування на ransomware може включати: ізоляцію уражених вузлів від мережі, ідентифікацію початкового вектора зараження, перевірку цілісності резервних копій, оповіщення керівництва та юридичного відділу, взаємодію з правоохоронними органами та, за необхідності, зверненням до зовнішніх фахівців із реагування на інциденти.

Стандартний життєвий цикл реагування на інцидент наочно відображений на рисунку 4.2, де представлено шість послідовних фаз, кожна з яких має чітко визначені входи, виходи та артефакти.

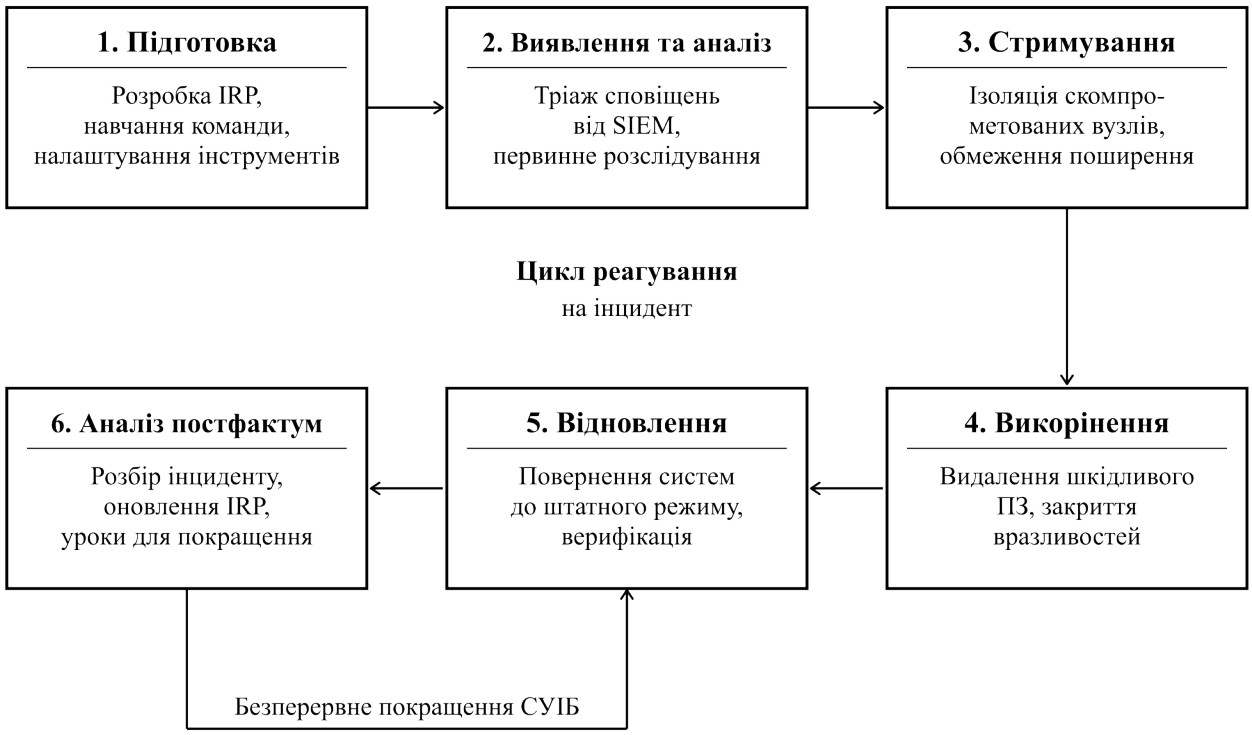


Рисунок 4.2 — Цикл реагування на інцидент інформаційної безпеки (за NIST SP 800-61)

Фаза стримування є однією з найкритичніших у процесі реагування, оскільки від швидкості та правильності дій на цьому етапі залежить масштаб збитків. Стримування поділяється на короткострокове — негайне обмеження поширення загрози, наприклад ізоляція зараженого вузла від мережі — та довгострокове, що передбачає більш глибокі структурні зміни: встановлення патчів, зміну облікових даних, посилення правил міжмережевого екрану. При цьому стримування не повинне знищувати цінні артефакти розслідування: дамп пам'яті ураженого вузла, мережеві журнали та інші криміналістичні дані необхідно зберегти ще до відключення системи. Це вимагає від аналітиків SOC чіткого розуміння того, які дані можуть бути втрачені при ізоляції або перезавантаженні системи, а які збережені в незалежних сховищах.

Взаємодія з зовнішніми структурами — командами реагування на комп'ютерні надзвичайні події (CERT/CSIRT) та правоохоронними органами — є невід'ємною складовою ефективного управління серйозними інцидентами. В Україні функції національного CERT виконує CERT-UA, підпорядкований Державній службі спеціального зв'язку та захисту інформації. Взаємодія з CERT-UA дає організаціям доступ до оперативних даних про актуальні кіберзагрози,

зокрема тактики, техніки та процедури (TTPs) відомих хакерських угруповань, що здійснюють атаки на українські організації. Крім того, CERT-UA координує реагування на масштабні кіберінциденти, що зачіпають одночасно кілька організацій або критичну інфраструктуру. Сповіщення CERT про виявлений інцидент не лише відповідає вимогам законодавства для певних категорій суб'єктів, а й дозволяє отримати кваліфіковану допомогу та збагатити загальний пул даних про загрози.

Таблиця 4.2 відображає ключові показники ефективності (KPI) процесу управління інцидентами, що дозволяють оцінити зрілість системи реагування в організації та встановити цільові орієнтири для її вдосконалення.

Таблиця 4.2 — Ключові показники ефективності управління інцидентами

Показник (KPI)	Визначення	Цільове значення (зріла організація)
MTTD (Mean Time to Detect)	Середній час від початку інциденту до його виявлення	< 1 година для критичних інцидентів
MTTP (Mean Time to Respond)	Середній час від виявлення до початку реагування	< 4 години
MTTR (Mean Time to Recover)	Середній час повного відновлення після інциденту	< 24 години для критичних систем
False Positive Rate	Частка хибних спрацювань у загальній кількості сповіщень	< 20%
Рівень ескалації	Частка інцидентів, що потребували залучення вищого рівня підтримки	< 15%
Повнота документування	Частка інцидентів із повністю заповненими картками	100%

4.3. Цифрова криміналістика та аналіз після інциденту

Цифрова криміналістика (Digital Forensics) — це наукова дисципліна та практика збору, зберігання, аналізу та представлення цифрових доказів з дотриманням вимог юридичної допустимості. У контексті реагування на інциденти криміналістичний аналіз дозволяє відповісти на ключові питання: що саме відбулося, коли, яким чином зловмисник отримав доступ, які дані були скомпрометовані та які наслідки матиме інцидент. Первинною вимогою будь-якого криміналістичного дослідження є збереження ланцюжка доказів (chain of custody) — документованої хронології всіх дій з доказами від моменту їх збору до представлення у суді. Порушення ланцюжка доказів може призвести до

визнання доказів недопустимими, що унеможливить кримінальне переслідування зловмисників.

Першочерговим кроком криміналістичного збору є документування стану системи до будь-яких змін. Це включає знімання образу оперативної пам'яті (memory dump), оскільки вона зберігає надзвичайно цінні артефакти: запущені процеси, відкриті мережеві з'єднання, ключі шифрування, вміст буфера обміну та навіть фрагменти шкідливого коду, що не залишив слідів на жорсткому диску (fileless malware). Після збору пам'яті здійснюється криміналістична копія носіїв даних методом побітового копіювання із збереженням хеш-сум для верифікації цілісності. Безпосереднє дослідження проводиться виключно з копіями, тоді як оригінальні носії зберігаються незмінними. Інструментарій криміналістичного аналітика включає Autopsy, Sleuth Kit, Volatility (для аналізу пам'яті), Wireshark (для аналізу мережевого трафіку) та безліч спеціалізованих утиліт.

Аналіз тактик, технік та процедур (TTPs) зловмисника є критичним для розуміння природи атаки та запобігання її повторенню. Структурованим фреймворком для опису TTPs є MITRE ATT&CK — база знань про поведінку зловмисників, що систематизує відомі методи атак за стадіями: від початкового доступу до ексфільтрації даних. Зіставлення виявлених артефактів з матрицею MITRE ATT&CK дозволяє ідентифікувати хакерське угруповання, визначити повноту компрометації та спрогнозувати подальші кроки атакуючого. Наприклад, виявлення утиліти Mimikatz у результатах криміналістичного аналізу вказує на техніку «Credential Dumping» (T1003 за класифікацією MITRE), що означає компрометацію облікових даних та необхідність примусової зміни паролів для всіх облікових записів у системі.

На рисунку 4.3 відображена послідовність кроків криміналістичного розслідування цифрового інциденту з урахуванням вимог збереження доказів та юридичної допустимості.

Звіт після інциденту (Post-Incident Report або Lessons Learned Report) є обов'язковим результатом завершеного процесу реагування. Такий звіт містить детальний хронологічний опис інциденту, оцінку ефективності реагування, виявлені прогалини в системі захисту та конкретні рекомендації щодо їх усунення. Ефективна організація перетворює кожен інцидент на цінний урок, що веде до покращення захисних механізмів. Аналіз після інциденту повинен охоплювати щонайменше такі питання: чи були виконані всі кроки відповідно до IRP; скільки часу зайняв кожен етап; які рішення виявилися невдалими та чому; чи були актуальними контактні дані всіх залучених осіб; які додаткові інструменти чи ресурси могли б прискорити реагування. Результати аналізу використовуються для актуалізації IRP, playbook, правил кореляції SIEM та програм навчання персоналу.

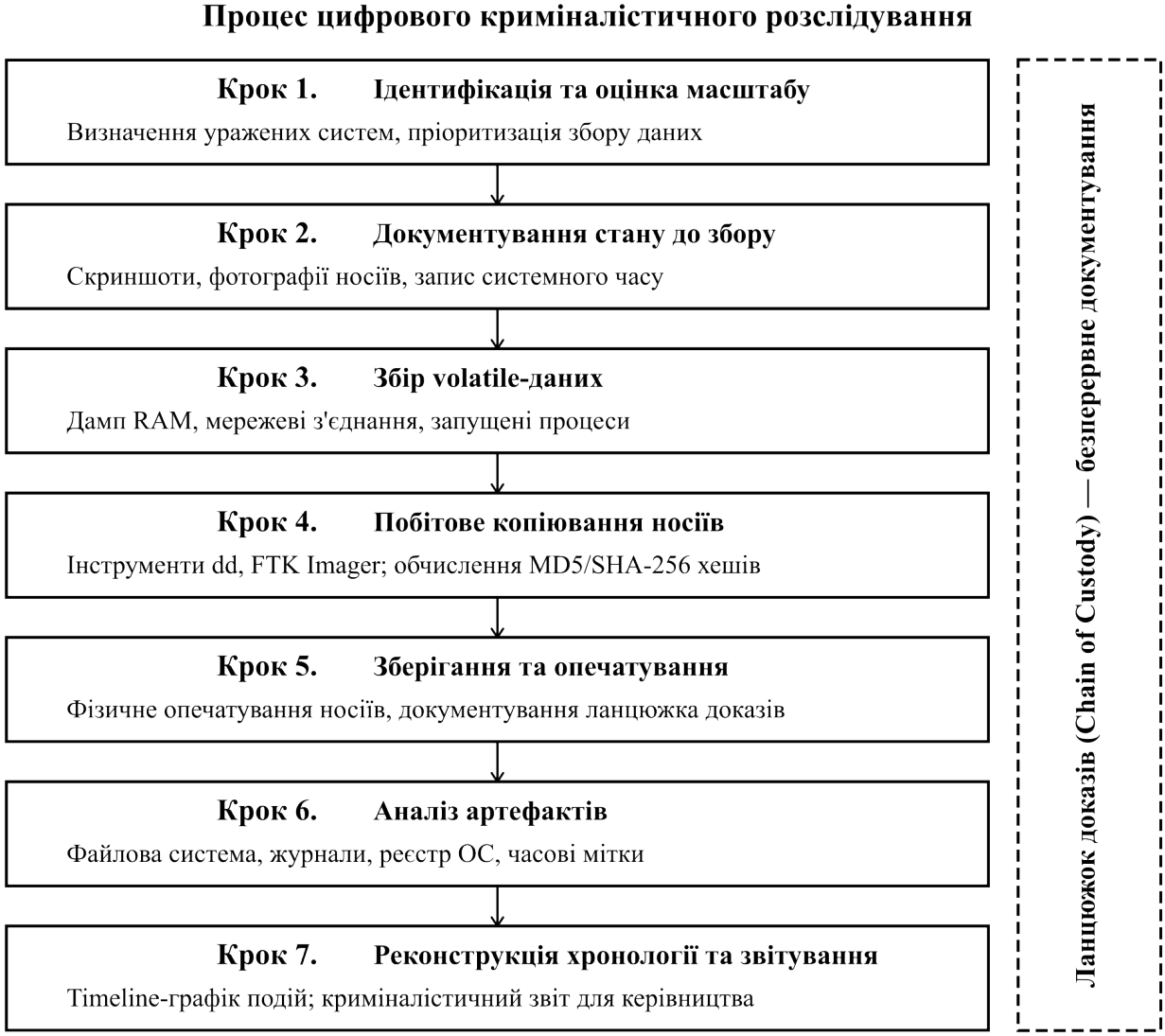


Рисунок 4.3 — Процес цифрового криміналістичного розслідування

Технологія автоматизації реагування на інциденти реалізується через платформи класу SOAR (Security Orchestration, Automation and Response). SOAR-системи інтегрують між собою різні інструменти безпеки (SIEM, EDR, міжмережеві екрани, системи управління вразливостями) та автоматизують повторювані операції відповідно до заздалегідь визначених playbook. Наприклад, при отриманні сповіщення про підозрілий вхід SOAR може автоматично заблокувати обліковий запис, ізолювати вузол через EDR, знайти пов'язані події у SIEM, збагатити індикатори компрометації даними Threat Intelligence та створити тікет у системі управління інцидентами — усе без участі аналітика. Це не лише пришвидшує реагування, а й дозволяє звільнити аналітиків від рутинних операцій для зосередження на складних розслідуваннях, що потребують творчого мислення та досвіду.

ЛЕКЦІЯ 5 АУДИТ ТА ТЕСТУВАННЯ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ

5.1. Методологія аудиту інформаційної безпеки

Аудит інформаційної безпеки є систематичним, незалежним і документованим процесом отримання свідчень щодо стану системи захисту організації та об'єктивного оцінювання ступеня відповідності встановленим критеріям — внутрішнім політикам, галузевим стандартам чи законодавчим вимогам. На відміну від тестування на проникнення, яке орієнтоване на пошук конкретних вразливостей, аудит безпеки охоплює ширший спектр питань: організаційні заходи, технічні засоби захисту, процедури управління, компетентність персоналу та відповідність нормативним вимогам. Міжнародний стандарт ISO/IEC 27007 визначає вимоги до аудиту систем управління інформаційною безпекою, тоді як ISO/IEC 27008 описує методи технічного аудиту контролів безпеки. Правильно проведений аудит дає керівництву організації об'єктивне і всебічне уявлення про реальний рівень захищеності та допомагає визначити пріоритети інвестицій у кібербезпеку.

Розрізняють кілька видів аудиту інформаційної безпеки залежно від ряду критеріїв. За суб'єктом проведення аудит поділяється на внутрішній — що проводиться власними фахівцями організації — та зовнішній, що здійснюється незалежними сертифікованими аудиторами. Перший є більш оперативним і дешевшим, другий — більш об'єктивним і авторитетним з погляду зовнішніх зацікавлених сторін. За предметом розрізняють аудит відповідності (compliance audit), що перевіряє дотримання конкретного стандарту або регуляторної вимоги, та операційний аудит, що оцінює ефективність і результативність систем захисту в реальних умовах. За методом проведення — документальний аудит (desk audit), що базується на перевірці документації без відвідування об'єкту, та аудит на місці (on-site audit), що передбачає безпосереднє обстеження приміщень, систем і опитування персоналу.

Методологічна основа аудиту включає декілька усталених підходів. Фреймворк COBIT (Control Objectives for Information and Related Technologies) розроблений асоціацією ISACA і широко застосовується для аудиту корпоративного управління в IT, забезпечуючи відповідність між IT-процесами та бізнес-цілями організації. NIST Cybersecurity Framework (CSF) пропонує гнучку структуру для оцінки і покращення програми кібербезпеки, організовану навколо п'яти функцій: Identify, Protect, Detect, Respond, Recover. Стандарт ISO/IEC 27001 є основою для сертифікаційного аудиту системи управління інформаційною безпекою (СУІБ) і визначає вимоги до формування,

впровадження, підтримки та постійного вдосконалення СУІБ. Вибір методологічної основи аудиту залежить від галузі, розміру організації, вимог регуляторів та конкретних цілей перевірки.

Процес проведення аудиту складається з кількох послідовних фаз. Перша фаза — планування та підготовка — передбачає визначення меж аудиту, цілей, критеріїв оцінки та формування аудиторської команди. На цьому етапі аудитори вивчають документацію організації: політики безпеки, процедури, організаційну структуру, результати попередніх аудитів та звіти про інциденти. Друга фаза — збір доказів — включає інтерв'ювання персоналу, спостереження за процесами, технічне тестування та аналіз журналів. Третя фаза — аналіз та оцінка — полягає у зіставленні зібраних доказів з критеріями аудиту для виявлення невідповідностей та формулювання висновків. Четверта фаза — звітування — передбачає підготовку звіту, що містить перелік виявлених невідповідностей, їх класифікацію за рівнем критичності та рекомендації щодо усунення. П'ята фаза — супровід та контроль виконання — забезпечує верифікацію виконання коригувальних заходів у встановлені терміни.

На рисунку 5.1 схематично представлено методологію проведення аудиту інформаційної безпеки з відображенням взаємозв'язків між фазами, входами та виходами кожного з етапів.

Рисунок 5.1 — Методологія проведення аудиту інформаційної безпеки

Аудиторський звіт є центральним результатом проведеного аудиту і повинен бути чітким, обґрунтованим та орієнтованим на практичні дії. Невідповідності класифікуються за рівнем критичності: критичні (major nonconformities) — суттєві відхилення, що ставлять під загрозу досягнення цілей СУІБ; некритичні (minor nonconformities) — менш суттєві відхилення; спостереження (observations) — ситуації, що не є поточними невідповідностями, але потенційно можуть ними стати. Рекомендації аудиторів мають бути конкретними, вимірюваними та реалістичними з точки зору ресурсів організації. Звіт адресується різним аудиторіям: технічна частина деталізована для фахівців з безпеки, а виконавче резюме — стисло і зрозуміло для керівництва, що не має технічної підготовки.

У таблиці 5.1 наведено порівняльну характеристику провідних фреймворків, що використовуються для проведення аудиту інформаційної безпеки, з описом їх сфери застосування та особливостей.

Таблиця 5.1 — Порівняльна характеристика фреймворків аудиту інформаційної безпеки

Фреймворк	Розробник	Сфера застосування	Тип аудиту	Результат
ISO/IEC 27001	ISO/IEC	СУІБ будь-якої організації	Відповідності	Сертифікат відповідності
NIST CSF	NIST (США)	Критична інфраструктура, держсектор	Операційний	Профіль зрілості (Tier 1-4)
COBIT 2019	ISACA	І Т - у п р а в л і н н я підприємством	Відповідності / Операційний	Рівень зрілості процесів
PCI DSS	PCI SSC	Обробка платіжних карток	Відповідності	Звіт про відповідність (ROC/SAQ)
SOC 2 Type II	AICPA	Хмарні та SaaS-провайдери	Відповідності + Операційний	Незалежний аудиторський звіт

5.2. Тестування на проникнення та оцінка вразливостей

Тестування на проникнення (penetration testing, або pentesting) — це авторизований процес симуляції реальних кібератак на інформаційну систему з метою виявлення вразливостей, що можуть бути використані зловмисниками для несанкціонованого доступу або завдання шкоди. На відміну від автоматизованого сканування вразливостей, тестування на проникнення є творчим процесом, що поєднує технічні інструменти з аналітичним мисленням досвідченого фахівця. Пентестер намагається досягти конкретних цілей — отримати доступ до критичних даних, підвищити привілеї, виконати

горизонтальне переміщення по мережі — використовуючи ті ж методи та інструменти, що і реальний зловмисник, але в межах заздалегідь узгодженого scope та з чіткими правилами взаємодії (rules of engagement). Юридичним підґрунтям тестування є документ «дозвіл на тестування» (letter of authorization), без якого будь-які дії пентестера є незаконними, незалежно від намірів.

Методологія тестування на проникнення систематизована кількома галузевими стандартами. OWASP Testing Guide є де-факто стандартом для тестування безпеки вебзастосунків і охоплює понад 90 типів тестів, організованих за категоріями вразливостей: перевірка конфігурації, автентифікація, управління сесіями, контроль доступу, валідація вхідних даних тощо. Стандарт PTES (Penetration Testing Execution Standard) описує повний методичний процес тестування від збору інформації до фінального звіту. OSSTMM (Open Source Security Testing Methodology Manual) пропонує строгу та відтворювану методологію для різних каналів тестування: мережевого, фізичного, людського та телекомунікаційного. На практиці пентестери часто поєднують елементи кількох методологій, адаптуючи підхід до специфіки конкретної системи та цілей замовника.

За обсягом інформації, що надається тестеру, розрізняють три типи тестування. Тестування методом чорної скрині (black box) — тестер не має жодної попередньої інформації про систему та має діяти як зовнішній зловмисник, починаючи з розвідки. Тестування методом білої скрині (white box) — тестеру надається вся доступна інформація: вихідний код, архітектурні схеми, облікові дані, що дозволяє провести найглибший технічний аналіз. Тестування методом сірої скрині (grey box) займає проміжну позицію — тестеру надається часткова інформація, яка є у розпорядженні привілейованого користувача або партнера. Останній підхід є найбільш поширеним у корпоративному середовищі, оскільки дає реалістичне уявлення про ризики від внутрішніх загроз та компрометованих облікових записів.

Рисунок 5.2 ілюструє стандартний процес тестування на проникнення, що відображає послідовні фази від визначення scope до підготовки звіту з рекомендаціями.

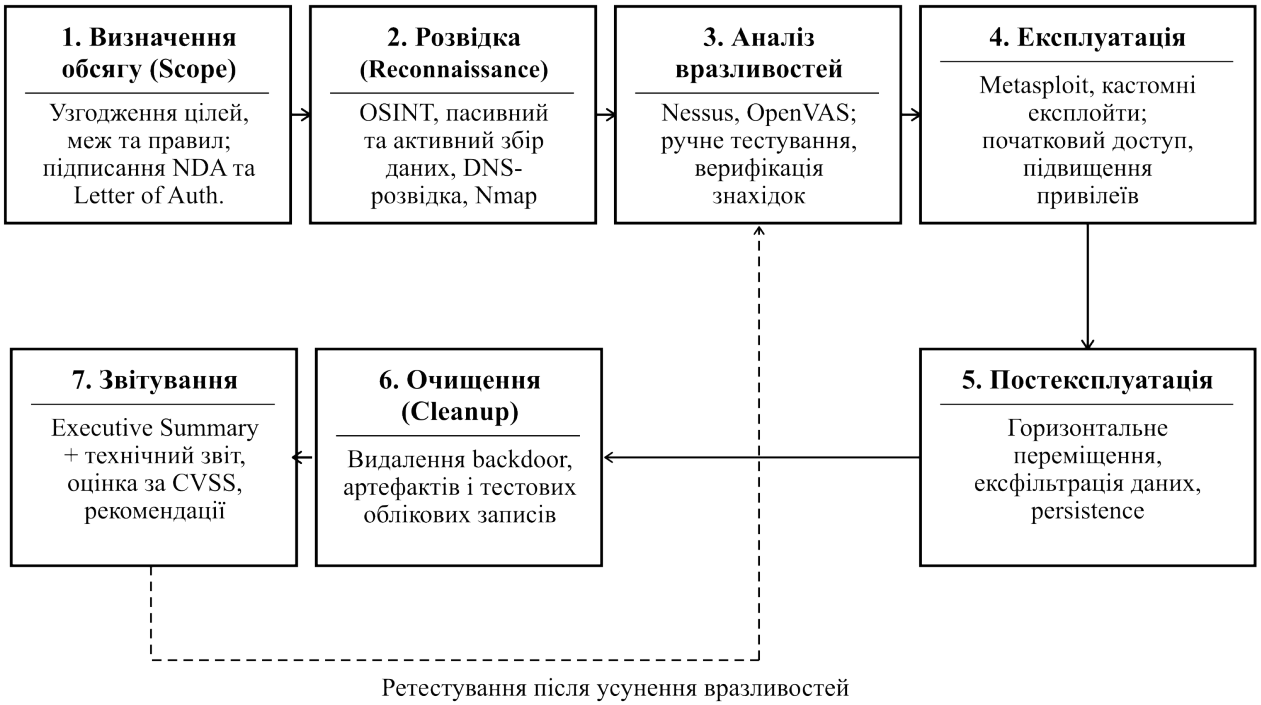


Рисунок 5.2 — Процес тестування на проникнення (Penetration Testing Lifecycle)

Оцінка вразливостей (Vulnerability Assessment, VA) є менш глибоким, але ширшим за охопленням процесом порівняно з тестуванням на проникнення. VA зосереджується на ідентифікації, класифікації та пріоритизації вразливостей у всіх компонентах інфраструктури, не намагаючись їх активно експлуатувати. Основним інструментарієм є автоматизовані сканери вразливостей: Nessus, Qualys, OpenVAS, Rapid7 InsightVM. Ці інструменти порівнюють стан сканованих систем із базою відомих вразливостей (CVE — Common Vulnerabilities and Exposures) та генерують детальні звіти. Система оцінки критичності вразливостей CVSS (Common Vulnerability Scoring System) дозволяє об'єктивно пріоритизувати виявлені проблеми за числовою шкалою від 0 до 10, де 9.0–10.0 відповідає критичному рівню, а 0.1–3.9 — низькому. Важливо розуміти, що автоматизовані сканери можуть генерувати хибно позитивні результати, тому виявлені вразливості потребують верифікації досвідченим фахівцем.

Таблиця 5.2 демонструє порівняльну характеристику оцінки вразливостей та тестування на проникнення, що дозволяє обрати відповідний підхід залежно від цілей, бюджету та наявного часу.

Таблиця 5.2 — Порівняльна характеристика VA та тестування на проникнення

Характеристика	Оцінка вразливостей (VA)	Тестування на проникнення (Pentest)
Мета	Ідентифікація та класифікація вразливостей	Симуляція реальної атаки, перевірка здатності до захисту
Підхід	Переважно автоматизований	Ручний + автоматизований
Глибина	Широке охоплення, менша глибина	Менше охоплення, більша глибина
Частота	Щоквартально або щомісяця	Щорічно або після суттєвих змін
Результат	Перелік вразливостей з оцінкою CVSS	Детальний звіт з proof-of-concept та ланцюжками атак
Вартість	Відносно низька	Висока (залежить від scope)

5.3. Стандарти та рекомендації у сфері аудиту та тестування безпеки

Міжнародна нормативна база у сфері аудиту та тестування безпеки інформаційних систем формується навколо кількох ключових документів, що визначають вимоги, рекомендації та кращі практики. Сімейство стандартів ISO/IEC 27000 є найбільш авторитетним і широко визнаним у світі. Стандарт ISO/IEC 27001 встановлює вимоги до СУІБ, тоді як ISO/IEC 27002 є практичним керівництвом з впровадження контролів безпеки, що охоплює 93 категорії засобів управління. ISO/IEC 27005 присвячений управлінню ризиками інформаційної безпеки, ISO/IEC 27007 — проведенню аудиту СУІБ, а ISO/IEC 27008 — технічному аудиту та огляду засобів управління. Для організацій, що прагнуть отримати міжнародне визнання рівня своєї захищеності, сертифікація за ISO/IEC 27001 є важливим конкурентним чинником, що підтверджує серйозний підхід до управління інформаційною безпекою.

Рекомендації CERT (Computer Emergency Response Team) відіграють важливу роль у формуванні кращих практик аудиту та тестування безпеки. CERT/CC при університеті Карнегі-Меллон, ENISA (Агентство ЄС з кібербезпеки) та CERT-UA публікують технічні настанови, сценарії типових атак та методичні посібники з проведення аудиту. Особливу роль відіграє CERT Resilience Management Model (CERT-RMM) — комплексна система управління стійкістю організації в умовах кіберзагроз, що охоплює питання ідентифікації активів, управління ризиками, реагування на інциденти та відновлення. Для проведення технічного аудиту безпеки вебзастосунків OWASP (Open Web Application Security Project) пропонує розгорнутий Testing Guide та перелік топ-10 вразливостей (OWASP Top 10), що є de facto стандартом у цій галузі.

Сфера технічного тестування безпеки охоплює не лише вебзастосунки та мережеву інфраструктуру, а й специфічні категорії систем, що потребують

спеціалізованих підходів. Тестування мобільних застосунків регламентується рекомендаціями OWASP Mobile Testing Guide, що враховує специфіку платформ iOS та Android. Аудит безпеки хмарних інфраструктур здійснюється відповідно до рекомендацій CSA (Cloud Security Alliance) та вбудованих інструментів хмарних провайдерів: AWS Security Hub, Microsoft Defender for Cloud, Google Security Command Center. Тестування безпеки промислових систем управління (ICS/SCADA) є особливо чутливою галуззю, де некоректно проведені тести можуть мати реальні фізичні наслідки, тому вимагають спеціалізованої підготовки та надзвичайно обережного підходу. Стандарт IEC 62443 визначає вимоги до кібербезпеки промислових автоматизованих систем управління і є базовим документом для аудиту в цій галузі.

Сертифікація фахівців у сфері аудиту та тестування безпеки є важливим індикатором компетентності та дотримання галузевих стандартів. Асоціація ISACA пропонує сертифікацію CISA (Certified Information Systems Auditor) — одну з найавторитетніших у галузі аудиту IT-систем. Для фахівців з тестування на проникнення визнаними є сертифікати OSCP (Offensive Security Certified Professional) від Offensive Security, яка вимагає успішного виконання практичного іспиту з пентестингу реальних систем, а також CEH (Certified Ethical Hacker) від EC-Council. Фахівці з управління безпекою прагнуть отримати сертифікат CISSP (Certified Information Systems Security Professional) від (ISC)², що є одним з найпрестижніших у галузі. Сертифікований аудитор чи пентестер несе підвищену відповідальність за якість своєї роботи та дотримання етичних норм, що є важливим чинником довіри з боку замовників послуг.

На рисунку 5.3 наведено ієрархічну структуру нормативно-методичної бази аудиту та тестування безпеки інформаційних систем, що систематизує ключові стандарти та рекомендації за рівнями та сферами застосування.

Управління знахідками аудиту та тестування потребує систематичного підходу до пріоритизації, призначення відповідальних та контролю виконання. Кожна виявлена вразливість або невідповідність повинна бути внесена до системи відстеження (bug tracker або спеціалізована система управління вразливостями), де їй присвоюється рівень критичності, призначається власник, встановлюється термін усунення та відстежується поточний статус. Системи управління вразливостями, такі як Tenable.io, Qualys VMDR або Rapid7 InsightVM, інтегруються з інструментами ITSM (Jira, ServiceNow) для автоматичного створення тікетів та відстеження їх виконання. Повторне тестування (retesting) після усунення вразливостей є обов'язковим кроком, що підтверджує ефективність вжитих заходів та закриває цикл управління вразливостями. Результати всіх аудитів і тестів зберігаються у документованому

вигляді та слугують доказовою базою для демонстрації відповідності регуляторним вимогам.

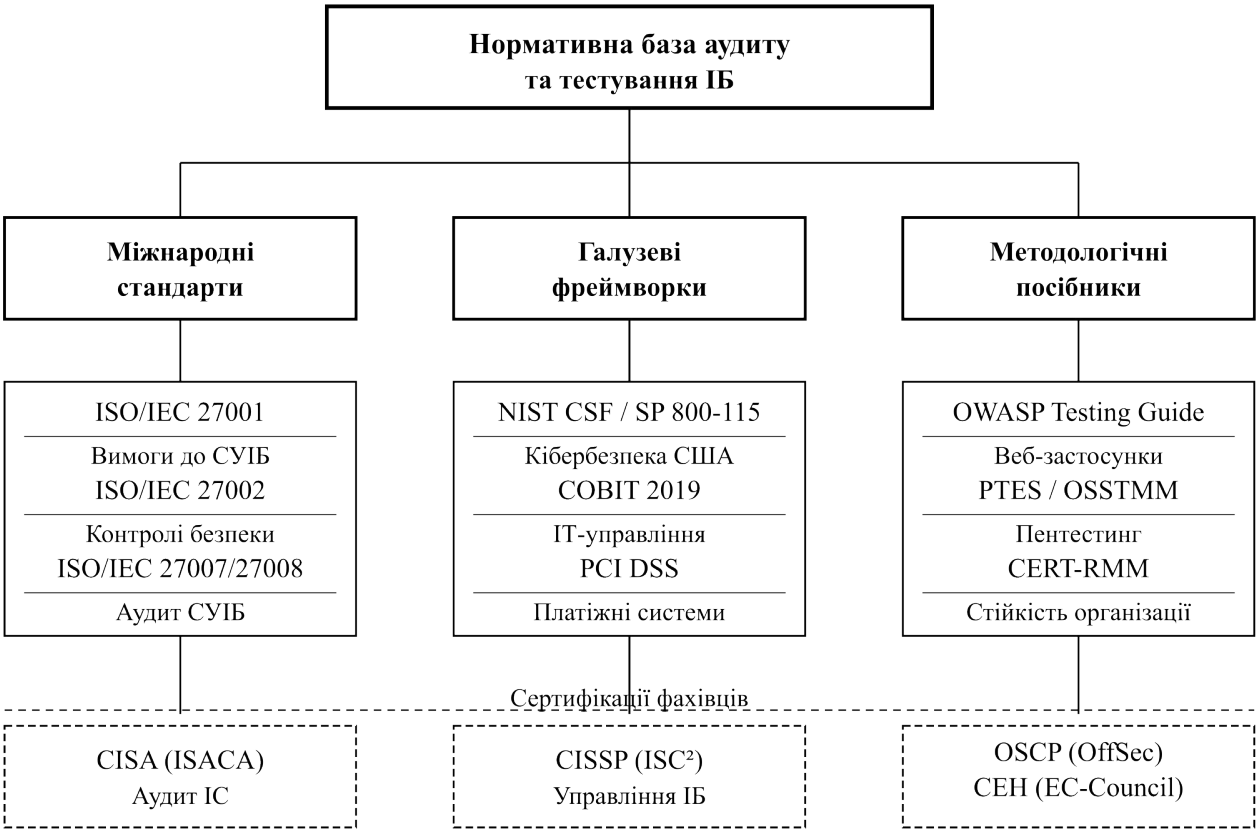


Рисунок 5.3 — Нормативно-методична база аудиту та тестування безпеки

Практичне значення регулярного тестування та аудиту безпеки для організації виходить далеко за межі формального виконання вимог регуляторів. По-перше, воно дозволяє об'єктивно виміряти реальний рівень захищеності, а не покладатися виключно на власну оцінку. По-друге, виявлені вразливості слугують обґрунтуванням для інвестицій у безпеку перед керівництвом та радою директорів. По-третє, регулярне тестування формує культуру безпеки в організації, де розробники та адміністратори усвідомлюють реальні наслідки своїх технічних рішень. Нарешті, організації, що проходять незалежний аудит і публікують його результати партнерам та клієнтам, демонструють відповідальне ставлення до захисту їхніх даних, що є суттєвою конкурентною перевагою в умовах зростаючої стурбованості суспільства питаннями конфіденційності та кіберзахисту.

ЛЕКЦІЯ 6. КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ТА БЕЗПЕРЕРВНІСТЬ БІЗНЕСУ

6.1. Концепція комплексного захисту інформації та архітектура КСЗІ

Комплексна система захисту інформації (КСЗІ) є центральним поняттям сучасної теорії та практики інформаційної безпеки, що відображає перехід від фрагментарних заходів захисту до системного, інтегрованого підходу до управління безпекою. Під КСЗІ розуміють сукупність організаційних заходів, технічних засобів, програмного забезпечення, нормативно-правових документів та процедур, що у взаємодії забезпечують захист інформаційних ресурсів організації від повного спектру актуальних загроз. Ключовою рисою комплексного підходу є не просто наявність окремих механізмів захисту, а їхня координована взаємодія в межах єдиної архітектурної концепції, де кожен елемент підсилює інші та де відсутність будь-якого компонента суттєво знижує загальну захищеність системи. Держава в особі відповідних органів (в Україні — Державна служба спеціального зв'язку та захисту інформації, ДССЗЗІ) встановлює обов'язкові вимоги до побудови та атестації КСЗІ для інформаційно-телекомунікаційних систем, що обробляють інформацію з обмеженим доступом або критичну інфраструктуру.

Архітектурно КСЗІ прийнято описувати через кілька взаємопов'язаних рівнів захисту, кожен з яких відповідає за певний аспект безпеки і реалізує власний набір механізмів. Перший рівень — фізичний — охоплює засоби контролю фізичного доступу до приміщень і обладнання, системи відеоспостереження, сигналізації та охорони периметру. Другий рівень — технічний або апаратний — включає засоби захисту від витоку інформації через технічні канали (побічне електромагнітне випромінювання, акустичні канали тощо), спеціалізоване захищене обладнання та апаратні модулі довіреного завантаження. Третій рівень — програмний — реалізується за допомогою операційних систем із вбудованими механізмами розмежування доступу, антивірусного програмного забезпечення, систем виявлення вторгнень, міжмережевих екранів і криптографічних засобів захисту інформації. Четвертий рівень — організаційний — є, мабуть, найвагомішим з управлінської точки зору, оскільки включає в себе всю нормативну базу підприємства: політику безпеки, регламенти, процедури і відповідальність персоналу.

Розуміння структури КСЗІ неможливе без аналізу концепції глибокого захисту (Defense in Depth), яка є методологічною основою побудови комплексних систем і передбачає ешелонований захист інформаційних активів, де кожен наступний рівень бар'єрів компенсує потенційні слабкості попередніх.

Ця концепція запозичена з військової стратегії і ґрунтується на розумінні того, що жодний окремий механізм захисту не є абсолютно надійним, а тому для досягнення прийнятного рівня безпеки необхідно поєднувати кілька незалежних рівнів захисту. Якщо зловмиснику вдається подолати один бар'єр — наприклад, обійти периметровий міжмережевий екран через скомпрометований VPN-акаунт — він все одно стикається з контролями на рівні хоста (EDR-агент), мережевих сегментів (мікросегментація) і застосунків (контроль привілейованого доступу).

На рисунку 6.1 схематично зображено архітектуру КСЗІ з ешелонованим захистом. Схема являє собою концентричні кола, де у центрі розміщені критичні інформаційні активи — бази даних, сервери застосунків та документи з обмеженим доступом. Навколо центру послідовно розміщені захисні рівні: рівень фізичного захисту (охоронна зона, контроль доступу до приміщень); рівень мережевого периметру (міжмережеві екрани, DMZ, IDS/IPS); рівень хоста (антивірус, EDR, контроль цілісності); рівень застосунків (аутентифікація, авторизація, шифрування); рівень даних (DLP, класифікація, шифрування сховищ). Кожне кільце позначено відповідним кольором та символами характерних для нього засобів захисту. Стрілки показують напрямок потенційних атак ззовні всередину та ешелони захисних заходів.

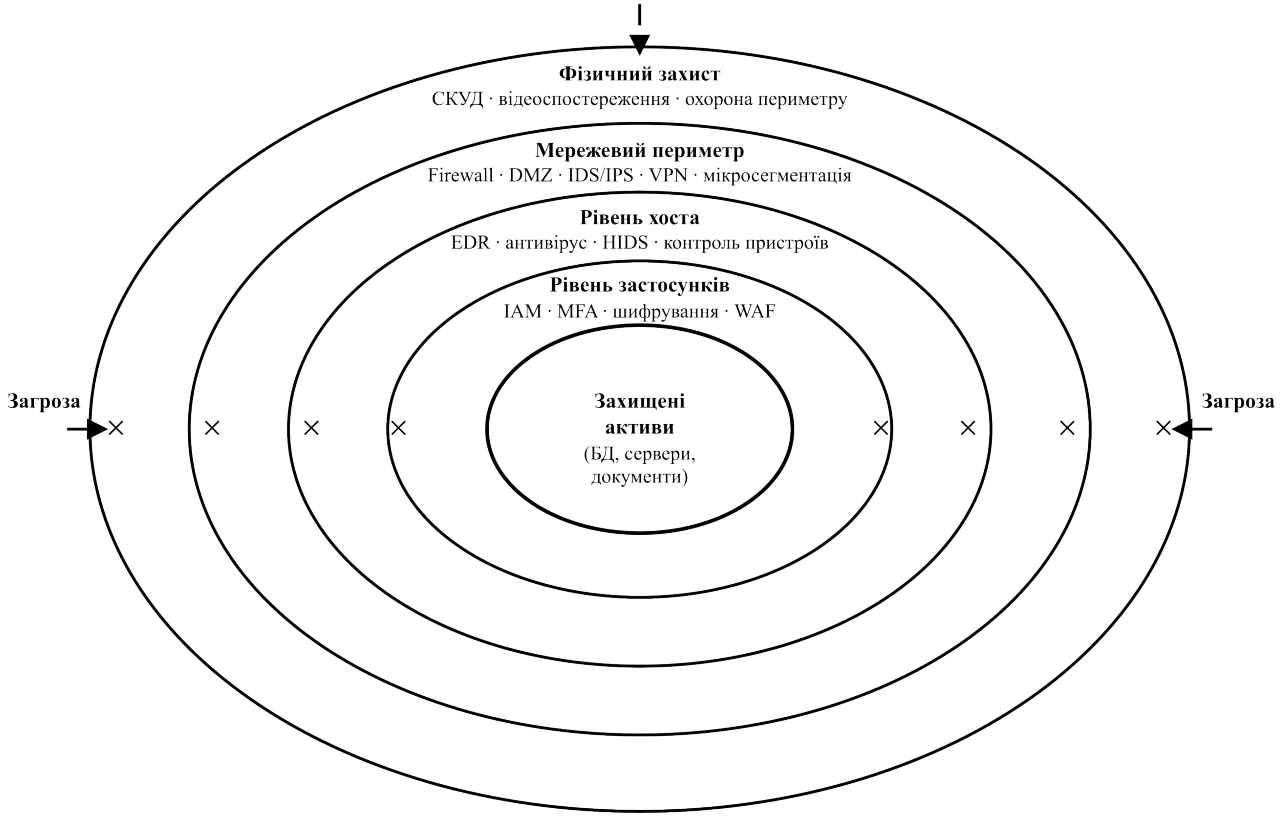


Рисунок 6.1 – Архітектура КСЗІ з ешелонованим захистом (Defense in Depth)

Нормативно-правова база, що регулює побудову КСЗІ в Україні, є досить розгалуженою і охоплює як законодавчий, так і підзаконний рівні. Закон України «Про захист інформації в інформаційно-комунікаційних системах» встановлює загальні вимоги до захисту інформації та відповідальність власників систем, а також визначає поняття комплексної системи захисту. Нормативні документи технічного захисту інформації (НД ТЗІ), що розробляються й оновлюються ДССЗЗІ, конкретизують технічні вимоги до різних класів захисту інформаційних систем. Важливим документом є НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі», який визначає етапи проєктування, впровадження та атестації КСЗІ. Паралельно організації, що прагнуть відповідності міжнародним стандартам, орієнтуються на сімейство ISO/IEC 27000, зокрема ISO/IEC 27001:2022, що встановлює вимоги до системи управління інформаційною безпекою як базової управлінської конструкції, яка охоплює і КСЗІ.

Важливою складовою КСЗІ є підсистема управління ідентифікацією та доступом (Identity and Access Management, IAM), яка реалізує принцип найменших привілеїв і забезпечує, щоб кожен суб'єкт — людина чи програма — міг отримати доступ лише до тих ресурсів, які необхідні для виконання його функцій, і лише в допустимий час і спосіб. IAM-підсистема в сучасних КСЗІ, як правило, включає централізований каталог ідентичностей (Active Directory, LDAP або хмарний IdP), систему єдиного входу (SSO), багатофакторну автентифікацію (MFA) та механізми привілейованого управління доступом (PAM). Усі ці компоненти повинні бути інтегровані між собою та із засобами журналювання і моніторингу, щоб забезпечити повну аудиторну стежку для кожної операції з інформаційними ресурсами. Нехтування IAM як складовою КСЗІ є однією з найпоширеніших причин успішних атак із використанням викрадених облікових даних.

Розробка та впровадження КСЗІ є проєктом, що охоплює кілька послідовних етапів, кожен з яких є обов'язковою передумовою для наступного. Першим етапом є обстеження та категоризація інформаційних активів — виявлення того, яка інформація обробляється в системі, яку цінність вона становить і які загрози для неї є актуальними. На цьому ж етапі проводиться класифікація інформації за рівнями конфіденційності та встановлюється клас захищеності системи відповідно до нормативних вимог. Другий етап — розробка технічного завдання (ТЗ) на КСЗІ, де формулюються конкретні вимоги до всіх підсистем захисту. Третій етап — проєктування та реалізація — включає вибір і налаштування конкретних засобів захисту, їхню інтеграцію та документування. Завершальним є четвертий етап — атестація КСЗІ, за результатами якої

видається атестат відповідності, що підтверджує здатність системи забезпечувати захист інформації відповідно до встановлених вимог.

Таблиця 6.1 – Підсистеми КСЗІ та їхні основні компоненти

Підсистема КСЗІ	Основні компоненти	Стандарти / нормативи
Управління доступом (IAM)	LDAP/AD, SSO, MFA, PAM, RBAC/ABAC	ISO/IEC 27001 A.9, NIST SP 800-63
Мережевий захист	Firewall, IDS/IPS, DDoS-захист, VPN, мікросегментація	ISO/IEC 27033, НД ТЗІ 2.5-004
Захист кінцевих точок	EDR, антивірус, HIDS, контроль пристроїв	ISO/IEC 27001 A.12, CIS Benchmark
Криптографічний захист	PKI, TLS/IPSec, шифрування дисків та БД, СКЗІ	ISO/IEC 18033, ДСТУ 4145, НД ТЗІ 2.5-008
Моніторинг та аудит	SIEM, log management, NTA, SOC	ISO/IEC 27001 A.12.4, NIST SP 800-92
Захист даних (DLP)	DLP-системи, класифікація даних, Data Masking	ISO/IEC 27001 A.8, GDPR, Закон про ЗПД
Фізичний захист	СКУД, відеоспостереження, охорона периметру	ISO/IEC 27001 A.11, НД ТЗІ 1.6-001

Розробка та впровадження КСЗІ є проєктом, що охоплює кілька послідовних етапів, кожен з яких є обов'язковою передумовою для наступного. Першим етапом є обстеження та категоризація інформаційних активів — виявлення того, яка інформація обробляється в системі, яку цінність вона становить і які загрози для неї є актуальними. На цьому ж етапі проводиться класифікація інформації за рівнями конфіденційності та встановлюється клас захищеності системи відповідно до нормативних вимог. Другий етап — розробка технічного завдання (ТЗ) на КСЗІ, де формулюються конкретні вимоги до всіх підсистем захисту. Третій етап — проєктування та реалізація — включає вибір і налаштування конкретних засобів захисту, їхню інтеграцію та документування. Завершальним є четвертий етап — атестація КСЗІ, за результатами якої видається атестат відповідності, що підтверджує здатність системи забезпечувати захист інформації відповідно до встановлених вимог.

6.2. Управління безперервністю бізнесу та відновлення після надзвичайних ситуацій

Управління безперервністю бізнесу (Business Continuity Management, BCM) є стратегічною дисципліною, що зосереджується на здатності організації продовжувати виконання критичних функцій під час порушень і відновлювати нормальну діяльність після інцидентів у визначені строки. BCM виходить за

рамки суто технічних заходів резервування та охоплює управлінські, організаційні та комунікаційні аспекти, що роблять організацію стійкою (resilient) до широкого кола загроз — від кібератак і відмов обладнання до стихійних лих і пандемій. Міжнародний стандарт ISO 22301:2019 «Системи управління безперервністю бізнесу» є основним нормативним орієнтиром для побудови BCM-систем і структурно є дуже схожим на ISO/IEC 27001, використовуючи ту саму Annex SL структуру, що дозволяє інтегрувати BCM-систему з системою управління інформаційною безпекою в єдину інтегровану систему управління.

Центральним поняттям BCM є аналіз впливу на бізнес (Business Impact Analysis, BIA), який є методологічним інструментом для ідентифікації критичних бізнес-процесів, оцінки наслідків їхнього переривання та встановлення пріоритетів відновлення. BIA дозволяє відповісти на ключові питання: які процеси є критичними для виживання організації? Скільки часу організація може функціонувати без кожного з них? Які ресурси — персонал, інформаційні системи, обладнання, постачальники — необхідні для відновлення цих процесів? За результатами BIA встановлюються два ключових показники для кожного критичного процесу: максимально допустимий час простою (Maximum Tolerable Period of Disruption, MTPD) — час, після якого переривання процесу спричинює катастрофічні наслідки для організації, та цільовий час відновлення (Recovery Time Objective, RTO) — час, за який процес має бути відновлений.

Паралельно з RTO у контексті відновлення інформаційних систем після інцидентів використовується поняття цільової точки відновлення (Recovery Point Objective, RPO), що визначає максимально допустимий обсяг втрачених даних, виміряний у часовому вимірі. Якщо RPO для певної бази даних становить дві години, це означає, що остання резервна копія даних повинна бути не старшою за дві години на момент настання інциденту, інакше втрата даних матиме неприйнятні наслідки. Відповідно, чим менше значення RPO, тим частіше необхідно виконувати резервне копіювання (або використовувати технології реплікації в реальному часі), що прямо впливає на вартість рішення. Раціональні значення RTO і RPO є результатом балансування між вартістю відновлення і вартістю простою, що є бізнес-рішенням, а не суто технічним.

На рисунку 6.2 зображено часову вісь розгортання інциденту та ключові показники BCM. Графік показує часову вісь з відміткою події — моменту настання інциденту. До цього моменту позначена точка останнього резервного копіювання, а відрізок від неї до моменту інциденту відповідає фактичній втраті даних. Між моментом інциденту і бажаним моментом відновлення позначено RTO. Над графіком стрілками позначено RPO (відстань від останнього бекапу

до моменту інциденту) та MTPD (максимально допустима тривалість простою). Штриховою лінією позначено рівень мінімально допустимого рівня сервісу, до якого система має бути повернута в межах RTO. Рисунок ілюструє взаємозв'язок між усіма показниками та їх практичний зміст.

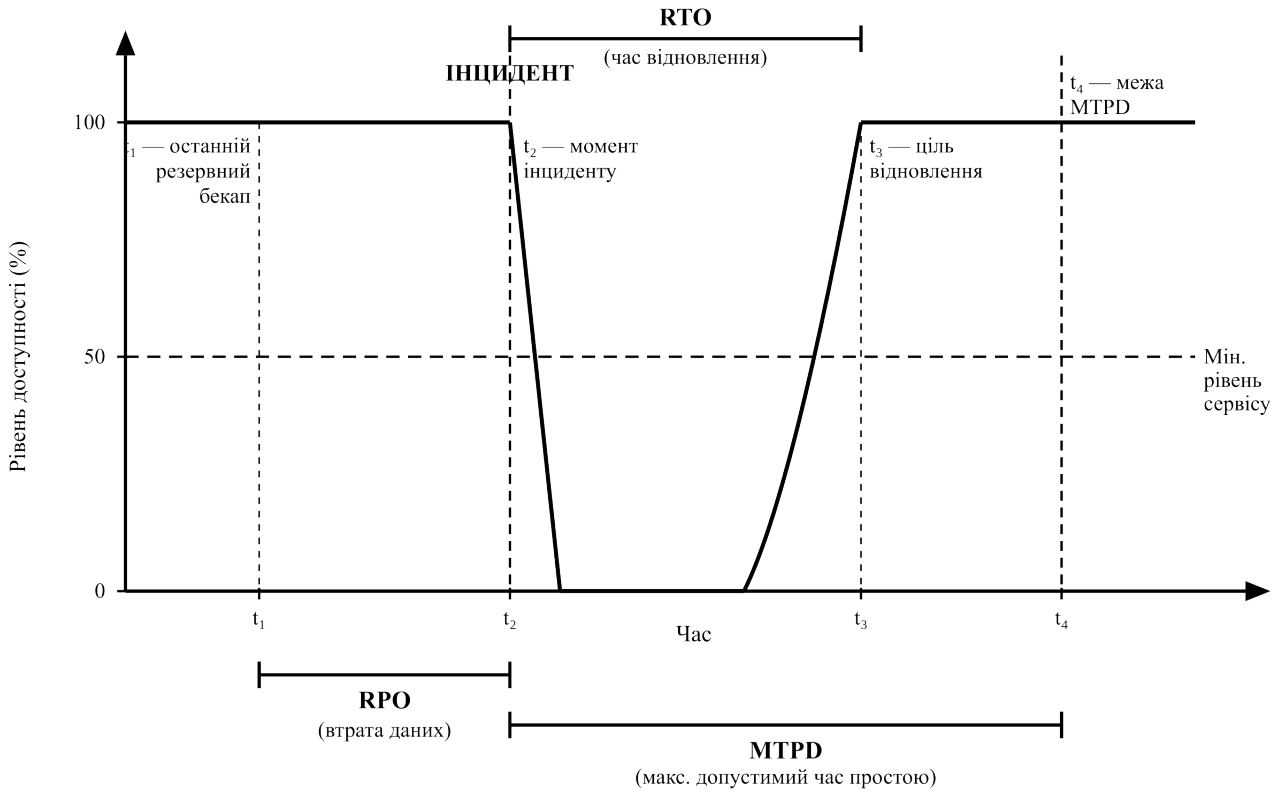


Рисунок 6.2 – Часова вісь інциденту та ключові показники BCM: RPO, RTO, MTPD

Планування безперервності бізнесу матеріалізується у вигляді кількох взаємодоповнюючих документів. План безперервності бізнесу (Business Continuity Plan, BCP) є операційним документом, що описує, як організація продовжуватиме виконання критичних функцій під час і безпосередньо після порушення. Він визначає альтернативні місця роботи, перерозподіл функцій між персоналом, порядок комунікації з зацікавленими сторонами. Окремо розробляється план відновлення після катастроф (Disaster Recovery Plan, DRP), що зосереджується на відновленні інформаційно-технологічної інфраструктури після серйозних інцидентів, включаючи процедури відновлення з резервних копій, активацію резервного дата-центру або хмарного середовища, порядок дій технічного персоналу. Важливим є також план управління кризою (Crisis Management Plan), що охоплює управлінські рішення на рівні вищого керівництва в умовах кризи.

Технічна сторона DR-рішень є надзвичайно різноманітною і включає декілька основних стратегій відновлення, що відрізняються співвідношенням

вартості та готовності. Стратегія «холодного резерву» (Cold Standby) передбачає наявність резервної площадки або інфраструктури, що не функціонує у звичайний час і потребує тривалого часу для активації (від кількох годин до кількох днів). Стратегія «теплого резерву» (Warm Standby) передбачає частково сконфігуровану та готову до запуску резервну систему, що може бути активована протягом кількох годин. Стратегія «гарячого резерву» (Hot Standby) забезпечує паралельну роботу основної та резервної систем із синхронізацією даних у реальному часі, що дозволяє переключення за лічені хвилини або секунди. В умовах широкого розповсюдження хмарних технологій до цього переліку додаються хмарні DR-рішення, зокрема Disaster Recovery as a Service (DRaaS), що поєднують гнучкість і масштабованість хмари з автоматизацією процедур відновлення.

Таблиця 6.2 – Порівняння стратегій резервування та їхніх характеристик

Стратегія	RTO (орієнт.)	RPO (орієнт.)	Відносна вартість	Приклади технологій
Backup & Restore	Годин – діб	Годин – діб	Низька	Tape backup, cloud storage
Cold Standby	Годин – 1-2 дні	Годин	Помірна	Резервний дата-центр
Warm Standby	Хвилин – годин	Хвилин	Середня	Реплікація БД, auto-scaling
Hot Standby	Секунд – хвилин	Секунд	Висока	Active-Active кластер, синхр. реплікація
DRaaS (хмарний)	Хвилин	Хвилин	Гнучка (OPEX)	AWS DR, Azure Site Recovery

6.3. Тестування КСЗІ та планів безперервності бізнесу

Навіть ідеально спроєктована КСЗІ та ретельно розроблені плани BCM/DR залишаються лише теоретичними конструкціями доти, поки вони не пройдуть практичної перевірки. Тестування є невіддільною частиною управління безперервністю бізнесу і передбачає систематичне проведення різноманітних вправ, що перевіряють як спроможність системи захисту протистояти загрозам, так і здатність організації відновитися після їх реалізації. ISO 22301 прямо вимагає, щоб процедури BCM проходили регулярне тестування та оновлення за результатами виявлених недоліків. Нехтування тестуванням є однією з найбільш небезпечних практик, оскільки інцидент, що трапляється у реальному житті, незмінно виявляє численні вади в планах, що ніколи не перевірялися на практиці.

Тестування BCM-планів відбувається у форматі різних типів вправ, що відрізняються за складністю та масштабом залучення ресурсів. Найпростішим і

найменш витратним є кабінетний (tabletop) тренінг, де учасники команди реагування збираються разом і покроково «програють» сценарій інциденту в режимі обговорення, без реального втручання у виробничі системи. Функціональні тренінги (functional exercises) вже передбачають активацію певних реальних процедур — наприклад, сповіщення команди, розгортання резервного командного центру або перевірку засобів зв'язку. Найбільш всеосяжним є повномасштабне навчання (full-scale exercise), що максимально наближено до реальної кризи і може передбачати реальне перемикання на резервні системи. Кожен тип вправ має свою роль у циклі вдосконалення BCM: кабінетні тренінги ефективні для виявлення прогалин у планах і навчання нових учасників, а повномасштабні навчання підтверджують, що плани дійсно спрацюють.

Окремим напрямком тестування є перевірка технічних засобів КСЗІ, що включає низку спеціалізованих підходів. Тестування на проникнення (penetration testing) імітує дії реального зловмисника і дозволяє виявити вразливості в системах і процесах захисту до того, як ними скористається реальний атакуючий. Сканування вразливостей забезпечує систематичну перевірку всіх компонентів IT-інфраструктури на наявність відомих вразливостей та невідповідностей конфігурацій. Перевірка цілісності резервних копій є часто недооцінюваним, але критично важливим видом тестування — адже лише регулярно тестована і перевірена резервна копія є надійним засобом відновлення, тоді як нетестована копія може виявитися пошкодженою або неповною у найкритичніший момент. Червоні команди (Red Teams) проводять тривалі, складні операції з імітації реальних APT-атак, що дозволяє оцінити не лише окремі засоби захисту, а й комплексну реакцію організації.

На рисунку 6.3 показано цикл тестування та вдосконалення BCM/DR відповідно до принципу постійного вдосконалення. Діаграма являє собою циклічний процес із чотирьох фаз, зображений у вигляді кола зі стрілками за годинниковою стрілкою. Перша фаза — «Планування» — включає розробку та актуалізацію BCP/DRP, визначення сценаріїв і цілей тестування. Друга фаза — «Тестування» — охоплює кабінетні тренінги, функціональні вправи та повномасштабні навчання. Третя фаза — «Аналіз результатів» — передбачає документування недоліків, складання звіту про тестування, виявлення прогалин. Четверта фаза — «Вдосконалення» — включає оновлення планів і процедур, усунення виявлених вразливостей, навчання персоналу. Між фазами розміщені стрілки-переходи із зазначенням часового горизонту (щоквартально, щорічно тощо). У центрі кола — символ організаційної стійкості (resilience).

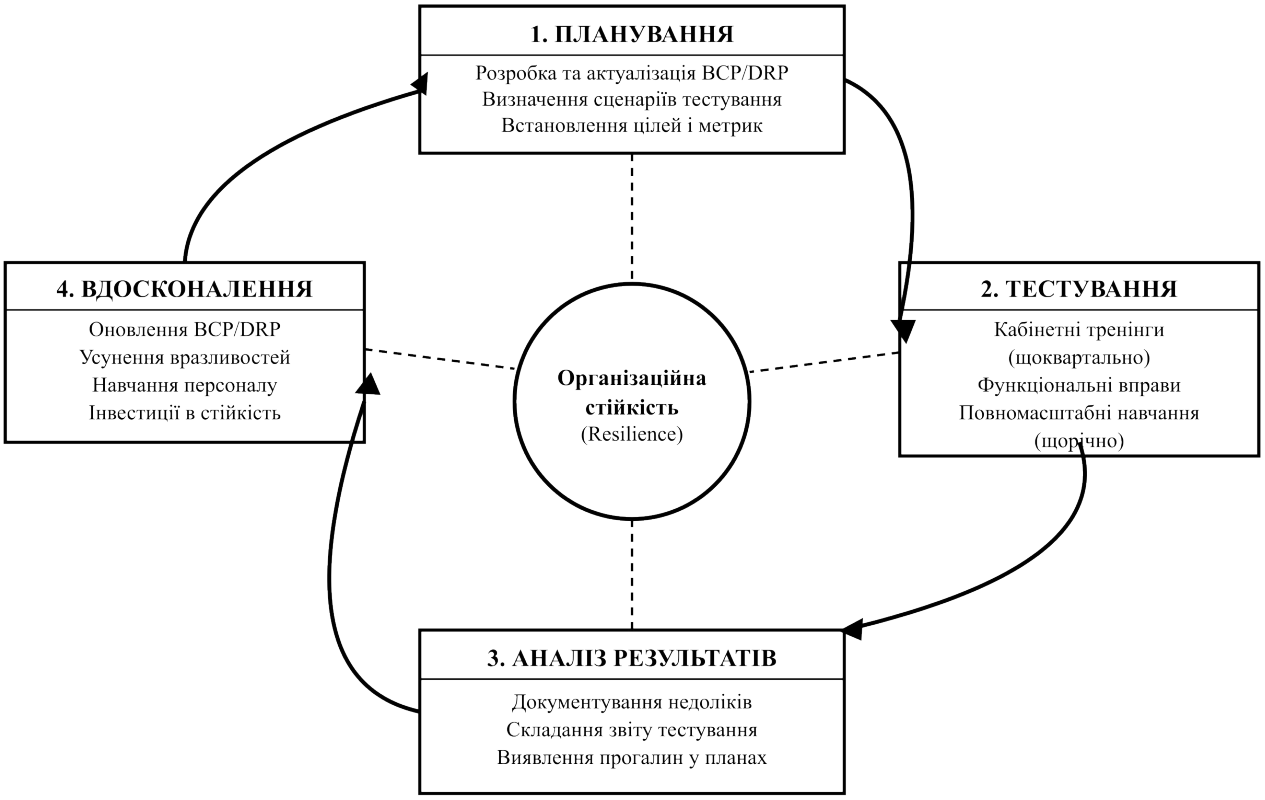


Рисунок 6.3 – Цикл тестування та вдосконалення BCM/DR

Результати тестування оформлюються у вигляді звіту, що є офіційним документом для вищого керівництва та органів нагляду. Звіт містить опис проведених вправ, виявлені невідповідності та їхній ступінь критичності, конкретні рекомендації щодо усунення недоліків і строки їх реалізації. Важливо, що звіт є не формальністю, а реальним інструментом управління: він забезпечує видимість стану BCM-системи для вищого керівництва, яке несе відповідальність за організаційну стійкість, і дозволяє приймати обґрунтовані рішення щодо пріоритетів інвестицій у безперервність бізнесу. Відповідно до вимог ISO 22301, результати тестування є вхідними даними для огляду з боку керівництва (Management Review), де приймаються рішення щодо ресурсів і стратегічних напрямів розвитку BCM-системи.

Інтеграція КСЗІ та BCM є стратегічним завданням для організацій, які усвідомлюють, що технічний захист і організаційна стійкість є двома сторонами однієї медалі. Кіберінцидент — наприклад, атака програмою-вимагачем — є одночасно і подією в площині інформаційної безпеки, і кризою в площині безперервності бізнесу, тому він повинен активувати і процедури реагування КСЗІ (ізоляція уражених систем, збір криміналістичних даних), і процедури BCM (активація BCP, оповіщення зацікавлених сторін, перехід на резервні процеси). Найбільш зрілі організації будують єдині інтегровані програми управління стійкістю, де СУІБ і BCM-система функціонують у спільному

нормативному середовищі, використовують спільні процеси ризик-менеджменту і проходять спільні аудити та навчання. Такий підхід не лише забезпечує вищий рівень захищеності, а й є економічно ефективним, оскільки усуває дублювання зусиль і ресурсів.

ЛЕКЦІЯ 7. ПЕРСПЕКТИВИ ТА СТРАТЕГІЧНІ ТЕНДЕНЦІЇ УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ

7.1. Сучасний ландшафт загроз: нові виклики та вектори атак

Ландшафт кіберзагроз у 2020-х роках характеризується безпрецедентною динамікою і складністю, що є наслідком кількох взаємопов'язаних тенденцій: стрімкої цифровізації суспільства, яка суттєво розширює поверхню атаки; підвищення рівня кваліфікації та організованості зловмисників, у тому числі державних акторів; появи нових технологій, що одночасно надають можливості для захисту і для атак. Традиційна модель захисту, що ґрунтується на периметрі мережі та реагуванні на відомі підписи атак, стає дедалі менш ефективною в умовах розмивання корпоративного периметру через хмарні технології, масову віддалену роботу і широке використання IoT-пристроїв. Організації, що продовжують покладатися виключно на традиційні підходи, стають легкою мішенню для сучасних зловмисників, які еволюціонували разом із захисними технологіями та навчилися обходити їх.

Атаки на ланцюг постачання (Supply Chain Attacks) стали одним із найбільш резонансних векторів загроз останніх років, а такі інциденти, як компрометація SolarWinds Orion у 2020 році та атака на Kaseya VSA у 2021 році, продемонстрували, що зловмисники здатні скомпрометувати тисячі організацій через довірений програмний продукт. Суть атаки на ланцюг постачання полягає в тому, що зловмисник не атакує цільову організацію напряму, а замість цього компрометує одного з її постачальників програмного забезпечення, обладнання або послуг. Це особливо небезпечно з кількох причин: жертви за замовчуванням довіряють постачальнику і не перевіряють ретельно оновлення або пристрої від нього; масштаб ураження може бути колосальним — один скомпрометований продукт поширює шкідливий код до всіх його клієнтів одночасно; виявлення факту компрометації є вкрай складним завданням, що може займати місяці. У відповідь на ці загрози виникли концепції SBOM (Software Bill of Materials) та підписання коду, що дозволяють організаціям краще контролювати склад і цілісність програмного забезпечення, що вони використовують.

Програми-вимагачі (Ransomware) еволюціонували від простих зашифровувачів файлів до складних операцій Ransomware-as-a-Service (RaaS), де автори шкідливого ПЗ продають або здають в оренду свої інструменти іншим злочинцям — так званим «афіліатам» — за частку від викупу. Сучасні ransomware-операції, такі як LockBit, ALPHV/BlackCat та Clop, використовують тактику подвійного або навіть потрійного вимагання: спочатку шифруються файли, потім погрожують публікацією викрадених даних, а деякі групи ще й

погрожують DDoS-атаками або безпосередньо зв'язуються з клієнтами і партнерами жертви. Ransomware-інциденти дедалі частіше спрямовані не на масових споживачів, а на великі організації — підприємства критичної інфраструктури, лікарні, муніципальні органи влади — де простій є найбільш болісним і де жертви найбільш схильні платити великий викуп.

Штучний інтелект (AI) та машинне навчання (ML) вже трансформують кібербезпеку як зі сторони захисту, так і зі сторони атаки, і ця тенденція прискорюватиметься. На боці захисту AI дозволяє аналізувати колосальні обсяги телеметрії з різних джерел і виявляти аномалії, які не помітив би жоден аналітик, а також автоматизувати рутинні завдання реагування на інциденти, звільняючи фахівців для вирішення складніших проблем. На боці атаки зловмисники вже використовують генеративний AI для створення більш переконливих фішингових листів, що не мають типових граматичних помилок і відрізняються від масових розсилок персоналізованим змістом. Більш серйозною перспективою є використання AI для автоматизованого виявлення вразливостей і генерації експлойтів, що може суттєво знизити поріг входу для кіберзлочинців. Концепція «AI-powered attacks» — атак, які самостійно адаптуються до захисних заходів у реальному часі — вже перестала бути науковою фантастикою.

Таблиця 7.1 – Сучасні вектори кіберзагроз та відповідні стратегії захисту

Вектор загрози	Характеристика	Стратегії захисту
Supply Chain Attack	Компрометація через довіреного постачальника ПЗ або обладнання	SBOM, підписання коду, Zero Trust, перевірка постачальників
Ransomware-as-a-Service	Екосистема кіберзлочинності з подвійним вимаганням	Резервне копіювання (3-2-1), EDR, сегментація мережі, навчання
AI-powered Phishing	Персоналізовані фішингові атаки на основі OSINT та GenAI	Поведінковий аналіз пошти, MFA, навчання персоналу
Living off the Land (LotL)	Використання легітимних системних інструментів (PowerShell, WMI)	EDR з аналізом поведінки, обмеження PowerShell, UEBA
API-атаки	Зловживання незахищеними API-інтерфейсами хмарних сервісів	API Gateway, автентифікація, rate limiting, WAF
OT/ICS Attacks	Атаки на промислові системи управління та критичну інфраструктуру	Сегментація OT/IT, моніторинг SCADA, IEC 62443

Загрози для операційних технологій (Operational Technology, OT) і промислових систем управління (Industrial Control Systems, ICS) набули особливої актуальності після таких інцидентів, як атака на українські енергомережі у 2015–2016 роках та атака на водопостачання у Флориді у 2021

році. OT-середовища традиційно розроблялися із пріоритетом доступності та функціональності, а не безпеки, і тепер є вразливими до кіберзагроз з кількох причин: застарілі операційні системи та протоколи, що не підтримують оновлень безпеки; зростаюча конвергенція IT та OT мереж, яка розширює поверхню атаки; критичні наслідки відмов, що унеможливлюють традиційне тестування на проникнення у виробничих середовищах. Міжнародний стандарт IEC 62443 є основним нормативним орієнтиром для захисту промислових систем управління і визначає вимоги до безпеки на всіх рівнях — від рівня компонентів до рівня систем управління підприємством.

7.2. Стратегічні моделі кібербезпеки майбутнього: Zero Trust, SASE та AI-driven Security

Архітектура Zero Trust («Нульова довіра») є однією з найбільш впливових парадигматичних змін у сфері кібербезпеки останнього десятиліття, що кардинально переосмислює базові принципи проєктування систем захисту. Традиційна модель безпеки ґрунтується на концепції «замок і рів» — довіряй усьому, що знаходиться всередині корпоративного периметру, і не довіряй нічому ззовні. Zero Trust відкидає цю модель і базується на протилежному принципі: «Ніколи не довіряй, завжди перевіряй» (Never Trust, Always Verify). Це означає, що кожен запит на доступ до ресурсів — незалежно від того, надходить він від внутрішнього користувача з корпоративного пристрою чи від зовнішнього підрядника — підлягає явній автентифікації, авторизації та постійній перевірці на відповідність контексту і поведінці. Модель Zero Trust набула практичного підґрунтя після публікації NIST SP 800-207 у 2020 році, яка визначила архітектурні принципи та компоненти Zero Trust Architecture (ZTA).

Реалізація Zero Trust у практиці організації є комплексним проєктом, що охоплює кілька архітектурних доменів і вимагає поетапного впровадження. Перший домен — ідентичності (Identity): впровадження MFA для всіх корпоративних сервісів, прийняття моделі ідентичності як нового периметру безпеки, безперервна оцінка ризику кожної сесії на основі поведінкових патернів. Другий домен — пристрої (Devices): забезпечення того, що лише відповідні та керовані пристрої можуть отримати доступ до корпоративних ресурсів (Mobile Device Management, Endpoint Compliance). Третій домен — мережа (Network): мікросегментація, шифрування трафіку між усіма сегментами, відмова від VPN на користь ZTNA (Zero Trust Network Access). Четвертий домен — застосунки (Applications): захист API, інтеграція рішень CASB для хмарних застосунків, обмеження доступу до сервісів виключно для авторизованих

ідентичностей. Нарешті, п'ятий домен — дані (Data): класифікація і маркування даних, шифрування, DLP-контроль навіть для внутрішнього трафіку.

На рисунку 7.1 зображено порівняння традиційної периметрової архітектури безпеки та архітектури Zero Trust. Ліва половина рисунку показує традиційну модель: великий прямокутник позначає корпоративний периметр (мережу), всередині якого розміщені сервери і користувачі, що вільно взаємодіють між собою, а брандмауер лише на зовнішньому рубежі відокремлює «довірену» внутрішню мережу від «недовіреного» Інтернету. Стрілка показує компрометованого інсайдера, що вільно переміщується мережею. Права половина показує архітектуру Zero Trust: немає єдиного периметру, кожна взаємодія між суб'єктом (користувачем, пристроєм) і ресурсом (сервером, застосунком) проходить через Policy Decision Point та Policy Enforcement Point, де перевіряються ідентичність, стан пристрою та контекст. Хмара, офіс та мобільні користувачі рівноправно підключаються через єдину площину контролю доступу. Підписи і символи ілюструють компоненти ZTA: IdP, MFA, ZTNA, CASB, мікросегментацію.

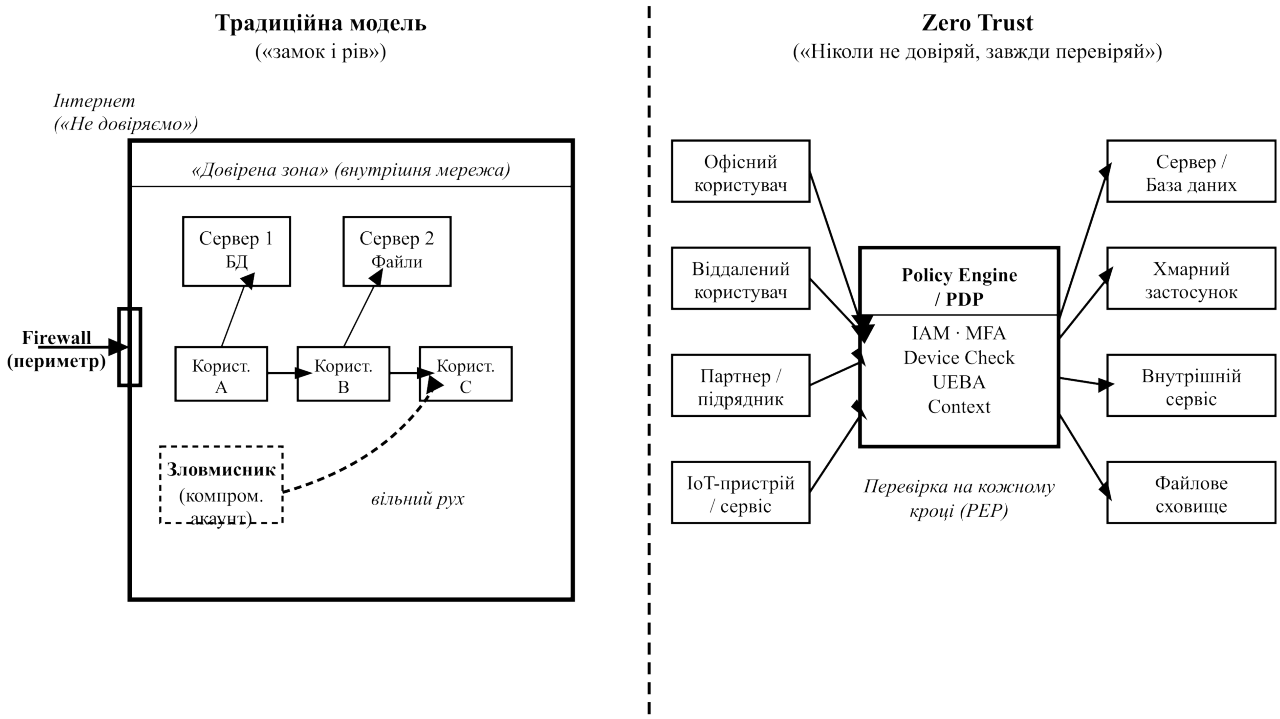


Рисунок 7.1 – Традиційна периметрова модель та архітектура Zero Trust

Концепція Secure Access Service Edge (SASE) — вимовляється «sassy» — запропонована Gartner у 2019 році, є архітектурним підходом, що конвергує мережеві сервіси і сервіси безпеки в єдину хмарну платформу, яку організація споживає як послугу. SASE об'єднує технології SD-WAN (Software-Defined Wide Area Network), ZTNA, CASB (Cloud Access Security Broker), SWG (Secure Web

Gateway) і FWaaS (Firewall as a Service) в єдину архітектуру, де всі ці функції надаються з найближчої до користувача точки присутності (PoP) хмарного провайдера. Це фундаментально вирішує проблему, яка виникає в традиційній моделі: якщо всі користувачі та сервіси знаходяться у хмарі і повсюдно розподілені, то немає жодного сенсу направляти їхній трафік у центральний корпоративний дата-центр для перевірки безпеки — це лише збільшує затримку і знижує продуктивність.

Автоматизація і оркестрація в кібербезпеці реалізуються через платформи SOAR (Security Orchestration, Automation and Response), що стають невіддільним компонентом сучасних SOC (Security Operations Center). SOAR-платформи дозволяють автоматизувати повторювані, добре відомі сценарії реагування на інциденти за допомогою playbook-ів — заздалегідь прописаних сценаріїв дій, що автоматично запускаються при виявленні певного типу інциденту. Наприклад, при виявленні фішингового листа SOAR-платформа може автоматично: витягти URL-посилання і хеш вкладень із листа, перевірити їх в системах репутації (VirusTotal, URLhaus), заблокувати шкідливі домени на проксі-сервері, помістити лист у карантин у всіх поштових скриньках організації, оповістити SOC-аналітика про інцидент із уже зібраним контекстом і виконаними діями. Це скорочує середній час реагування (MTTR) з годин до хвилин і звільняє аналітиків від рутинних завдань.

Таблиця 7.2 – Еволюція архітектурних моделей кібербезпеки

Характеристика	Периметрова модель	Zero Trust	SASE
Базовий принцип	Довіряй всередині периметру	Ніколи не довіряй, завжди перевіряй	Хмарна конвергенція мережі та безпеки
Периметр мережі	Чіткий фізичний периметр	Відсутній або розмитий	Відсутній, замінений PoP
Підхід до доступу	Мережевий доступ (VPN)	Identity-based ZTNA	ZTNA як частина SASE
Хмарна підтримка	Обмежена, через backhauling	Підтримує, потребує IdP	Cloud-native, основна сила
Складність	Нижча (для традиційних середовищ)	Середня – висока	Вища при впровадженні

7.3. Стратегічне управління кібербезпекою: людський фактор, регуляторні тенденції та майбутнє професії

Стратегічне управління кібербезпекою виходить далеко за рамки технічних рішень і все більше стає питанням корпоративного управління (governance) на найвищому рівні організацій. Ради директорів і наглядові ради

провідних компаній дедалі частіше включають питання кібербезпеки до своїх порядків денних, а в деяких юрисдикціях регулятори починають прямо вимагати від рад директорів демонстрації компетентності у сфері кіберризиків. Американська Комісія з цінних паперів (SEC) у 2023 році прийняла правила, що зобов'язують публічні компанії розкривати в регуляторних звітах інформацію про матеріальні кіберінциденти у 4-денний строк, а також щорічно звітувати про процеси управління кіберризиками та роль ради директорів у нагляді за ними. Аналогічна тенденція спостерігається і в ЄС у контексті Директиви NIS2, яка набула чинності в 2023 році і поширює строгі вимоги кібербезпеки на значно ширший круг організацій у критичних секторах.

Людський фактор залишається найслабшою ланкою в будь-якій системі захисту і є причиною переважної більшості успішних кібератак. За різними оцінками, від 70 до 90 відсотків успішних атак мають в основі соціальну інженерію, фішинг або помилки персоналу, що наочно демонструє: навіть найбільш технічно досконала КСЗІ буде зведена нанівець, якщо у працівників відсутня належна культура кібербезпеки. Ефективне навчання персоналу з питань кібербезпеки — Security Awareness Training — є не разовим заходом, а безперервним процесом, що включає регулярні теоретичні навчання, симуляції фішингових атак, рольові ігри для відпрацювання дій в екстрених ситуаціях і вимірювання ключових показників ефективності (кількість співробітників, що «клікнули» на симульований фішинг, час до повідомлення про підозрілий лист тощо). Концепція «людського брандмауера» (Human Firewall) описує ситуацію, коли кожен співробітник є обізнаним і мотивованим учасником системи кібербезпеки, а не пасивним об'єктом захисту.

На рисунку 7.2 наведено структуру програми підвищення обізнаності з питань кібербезпеки (Security Awareness Program). Схема зображена у вигляді піраміди. Основу піраміди (широкий нижній рівень) становить «Базова обізнаність»: охоплення всіх співробітників організації, базові модулі навчання (фішинг, паролі, фізична безпека, класифікація даних), онлайн-тестування. Середній рівень піраміди — «Рольове навчання»: спеціалізовані навчальні треки для груп підвищеного ризику (IT-адміністратори, фінансовий відділ, юридичний відділ, топ-менеджмент), більш детальні сценарії загроз, симуляції фішингу. Вершина піраміди — «Поглиблена підготовка»: тренінги для команди SOC та IR, Red/Blue Team вправи, реагування на кризу. Стрілки показують зростання складності вгору, а стрілка вліво вказує на широке охоплення. Нижче піраміди — шкала метрик: клік-рейт фішингу, час до звіту, результати тестувань.

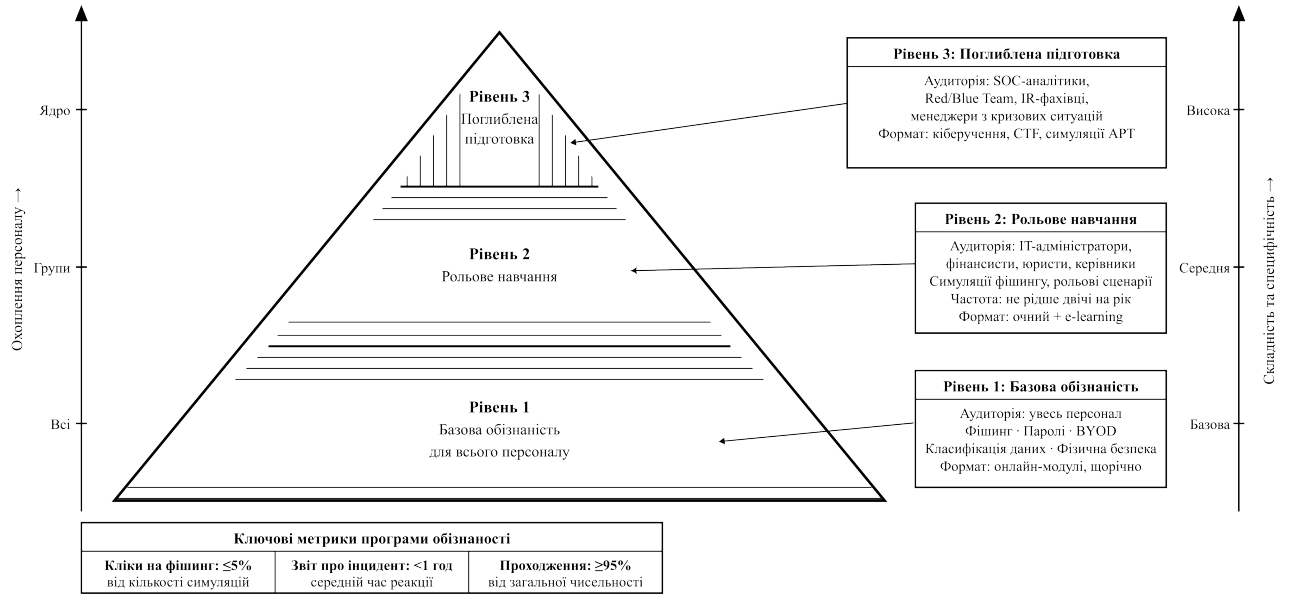


Рисунок 7.2 – Піраміда програми підвищення обізнаності персоналу з кібербезпеки

Квантові обчислення є технологією, що несе фундаментальний виклик для сучасної криптографії: алгоритм Шора, реалізований на достатньо потужному квантовому комп'ютері, здатний зламати широко використовувані асиметричні криптосистеми — RSA, ECC та Diffie-Hellman — за поліноміальний, а не експоненціальний час. Хоча квантові комп'ютери, здатні виконати таку атаку, ще не існують (і, за оптимістичними оцінками, з'являться не раніше ніж через 10–15 років), вже сьогодні виникає загроза так званих атак «Harvest Now, Decrypt Later» (HNDL): зловмисники, у першу чергу державні актори, можуть збирати зашифровані дані вже зараз, щоб розшифрувати їх пізніше, коли квантові комп'ютери стануть достатньо потужними. Це робить перехід на постквантову криптографію (Post-Quantum Cryptography, PQC) питанням стратегічної важливості вже сьогодні, а не у далекому майбутньому. NIST у 2024 році опублікував перші стандарти PQC-алгоритмів (FIPS 203, 204, 205), що є практичним кроком до пост-квантового захисту.

Регуляторне середовище у сфері кібербезпеки продовжує інтенсивно розвиватися по всьому світу, що безпосередньо впливає на стратегічне управління організаціями. Директива NIS2 (Network and Information Security Directive 2) значно розширила перелік суб'єктів, на які поширюються вимоги ЄС щодо кібербезпеки, і посилила відповідальність вищого керівництва за стан кібербезпеки. Регламент DORA (Digital Operational Resilience Act) встановлює суворі вимоги операційної стійкості для фінансового сектора ЄС. В Україні в умовах повномасштабної збройної агресії питання кіберзахисту критичної інфраструктури набули особливої гостроти: Закон України «Про основні засади

забезпечення кібербезпеки України» та відповідні підзаконні акти визначають систему суб'єктів кібербезпеки, їхні повноваження і зобов'язання операторів критичної інфраструктури. Глобальна тенденція до обов'язкового повідомлення про кіберінциденти означає, що організації більше не можуть замовчувати серйозні інциденти і мусять будувати процеси розкриття інформації регуляторам і постраждалим.

Майбутнє професії фахівця з кібербезпеки є яскравим і повним можливостей, незважаючи на те, що сама галузь стрімко трансформується під впливом AI та автоматизації. Дефіцит кваліфікованих кадрів у галузі кібербезпеки залишається критичним і, за оцінками ISC², перевищує 4 мільйони незаповнених вакансій у всьому світі. Водночас характер необхідних компетенцій змінюється: рутинні аналітичні задачі дедалі більше автоматизуються, а попит зростає на фахівців із гібридними компетенціями, здатних поєднувати глибоке технічне розуміння з бізнес-аналітикою, юридичними знаннями і комунікаційними навичками. Управлінські ролі — CISO, директор з ризик-менеджменту, менеджер BCM — набувають дедалі більшої ваги на рівні вищого керівництва організацій, оскільки кіберризики перетворилися на стратегічні бізнес-ризики. Для студентів спеціальності «Кібербезпека та захист інформації» це означає необхідність не лише оволодіти технічними навичками, а й розвивати здатність до стратегічного мислення, управлінські компетенції і розуміння бізнес-контексту кіберзагроз.

Підсумовуючи, можна констатувати, що кібербезпека перебуває на порозі нової ери, де технічна складність атак і захисних заходів зростає одночасно з розширенням стратегічного значення галузі для організацій, держав і суспільства в цілому. Фахівці, що прагнуть досягти успіху в цій галузі, мають поєднувати фундаментальне розуміння принципів і стандартів інформаційної безпеки з постійним навчанням і адаптацією до нових технологій і загроз, управлінські компетенції з технічними, а також усвідомлювати свою роль у забезпеченні цифрової стійкості сучасного суспільства. Дисципліна «Управління інформаційною та кібербезпекою» закладає саме ті концептуальні та практичні основи, що є необхідним фундаментом для цього шляху.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ананьїн В. О., Горлинський В. В., Гангал А. В. Інформаційна безпека. Менеджмент інформаційної безпеки держави : курс лекцій. Київ : ІСЗЗІ КПІ ім. Ігоря Сікорського, 2025. 284 с.

2. Андерсон Р. Дж. Інженерія безпеки : посібник для створення захищених систем / пер. з англ. Київ : Логос, 2010. 576 с.

3. Бараннік Р. В. Кібербезпека і управління інформаційними ресурсами : навч. посіб. Київ : Юрінком Інтер, 2025. 236 с.

4. Богуш В. М., Богуш В. В., Бровко В. Д., Гордієнко С. Б., Кудін А. М. Управління інформаційною безпекою та кібербезпекою організації : навч. посіб. Київ : Букрек, 2024. 312 с.

5. ДСТУ ISO/IEC 27001:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. Системи управління інформаційною безпекою. Вимоги. Київ : ДП «УкрНДНЦ», 2023. 42 с.

6. ДСТУ ISO/IEC 27002:2023. Інформаційні технології. Методи захисту. Звід практичних правил управління інформаційною безпекою. Київ : ДП «УкрНДНЦ», 2023. 108 с.

7. ДСТУ-Н 4440:2021. Інформаційна безпека. Керівні принципи оцінки ризиків інформаційної безпеки. Київ : ДП «УкрНДНЦ», 2021. 36 с.

8. ДСТУ-Н 7799.3:2020. Інформаційна безпека. Керівництво з управління безпекою інформаційних технологій. Київ : ДП «УкрНДНЦ», 2020. 54 с.

9. Жилін А. В., Шаповал О. М., Успенський О. А. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2020. 298 с.

10. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII. // Відомості Верховної Ради України. 2017. № 45. Ст. 412.

11. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР. // Відомості Верховної Ради України. 1994. № 31. Ст. 282.

12. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI. // Відомості Верховної Ради України. 2010. № 34. Ст. 478.

13. Закон України «Про електронні комунікації» від 16.12.2020 № 1089-IX // Відомості Верховної Ради України. 2021. № 10. Ст. 68.

14. Закон України «Про електронні довірчі послуги» від 05.10.2017 № 2155-VIII // Відомості Верховної Ради України. 2017. № 45. Ст. 411.

15. Йона Л. Г., Онацький О. В., Бєлова Ю. В. Криптографічний захист інформації : навч. посіб. Одеса : ДУІТЗ, 2023. 250 с.

16. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Geneva : International Organization for Standardization, 2022. 34 p.

17. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — Information security controls. Geneva : International Organization for Standardization, 2022. 104 p.

18. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection — Guidance on managing information security risks. Geneva : International Organization for Standardization, 2022. 58 p.

19. ISO/IEC 27701:2022. Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines. Geneva : International Organization for Standardization, 2022. 46 p.

20. Остапов С. Е., Євсеєв С. П., Король О. Г. Кібербезпека: сучасні технології захисту : навч. посіб. Львів : Новий Світ-2000, 2020. 324 с.