МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “МЕТОДИ ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНУВАННЯ СИСТЕМИ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Вадим МОЙСЕЄВ
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-41

Вадим МОЙСЕЄВ
Ім’я, ПРІЗВИЩЕ

Керівник: Михайло ЗАПОРОЖЧЕНКО
Доктор філософії з кібербезпеки Ім’я, ПРІЗВИЩЕ

Рецензент: _____
_____ Ім’я, ПРІЗВИЩЕ

Київ 2026

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра управління кібербезпекою та захистом інформації

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УКБЗІ
_____ Світлана ЛЕГОМІНОВА
“____”_____2026 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Мойсеєву Вадиму Ігоровичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Методи забезпечення функціонування системи менеджменту інформаційної безпеки організації”,
керівник кваліфікаційної роботи ЗАПОРОЖЧЕНКО Михайло, доктор філософії з кібербезпеки
(ПРІЗВИЩЕ, Ім’я, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологійвід “20“ лютого 2026 р. №51.

2. Строк подання кваліфікаційної роботи “12” травня 2026р.
3. Вихідні дані до кваліфікаційної роботи: *нормативні стандарти з інформаційної безпеки, наукові джерела, аналітичні звіти щодо кіберзагроз, операційні характеристики інфраструктури об'єкта дослідження.*
4. Перелік питань, які мають бути розроблені:
   4.1. Дослідити теоретичні засади, еволюцію та нормативні вимоги до побудови систем менеджменту інформаційної безпеки.
   4.2. Проаналізувати методи операційного управління захистом активів, роль людського фактора та оцінювання результативності системи.
   4.3. Розробити прикладний інструментарій моніторингу СМІБ через систему показників (KPI) та модель оцінювання зрілості процесів.
   4.4. Оцінити відповідність процесів захисту на умовному підприємстві та сформувати дорожню карту їх удосконалення.
5. Перелік ілюстративного матеріалу: *презентація PowerPoint*
6. Дата видачі завдання “5“ березня 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2026	
2.	Збір та аналіз літератури.	30.03.2026	
3.	Аналіз теоретичних основ функціонування та розвитку систем менеджменту інформаційної безпеки в сучасних умовах	08.04.2026	
4.	Дослідження методологічних підходів до побудови операційних процесів СМІБ та управління ризиками	15.04.2026	
5.	Практична розробка та впровадження комплексу організаційно-технічних заходів із підвищення зрілості СМІБ та оцінювання результативності впроваджених змін	22.04.2026	
6.	Формулювання висновків за результатами проведеного дослідження.	29.04.2026	
7.	Оформлення роботи.	06.05.2026	
8.	Оформлення презентації.	11.05.2026	
9.	Отримання рецензії на роботу.	10.06.2026	
10.	Захист в ЕК.	__.06.2026	

Здобувач вищої освіти _____ Вадим МОЙСЕЄВ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Михайло ЗАПОРОЖЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня бакалавра

Направляється здобувач Мойсеєв В.І. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Методи забезпечення функціонування системи менеджменту інформаційної безпеки організації"

Кваліфікаційна робота і рецензія додаються.

Директор ННІКБЗІ _____ Євгенія ІВАНЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач МОЙСЕЄВ Вадим у кваліфікаційній роботі дослідив стан системи менеджменту інформаційної безпеки, класифікував виявлені невідповідності, проаналізував чинники ризику та розробив дорожню карту рекомендацій щодо вдосконалення СМІБ. У практичній частині успішно реалізовано комплекс організаційно-технічних заходів у реальному корпоративному середовищі з оцінкою їх ефективності.

Робота демонструє високий рівень теоретичної підготовки та практичних навичок здобувача. МОЙСЕЄВ Вадим проявив самостійність, відповідальність та вміння застосовувати здобуті знання. Результати дослідження апробовані на конференції.

Все це дозволяє оцінити кваліфікаційну роботу здобувача МОЙСЕЄВА Вадима на оцінку "добре" та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Михайло ЗАПОРОЖЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____"_____2026 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач МОЙСЕЄВ В.І. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри
управління кібербезпекою та
захистом інформації _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

Здобувача вищої освіти МОЙСЕЄВА Вадима
на тему “Методи забезпечення функціонування системи менеджменту інформаційної безпеки організації”

Актуальність. В умовах зростання кількості кіберзагроз та складності IT-інфраструктури, ефективне функціонування системи менеджменту інформаційної безпеки (СМІБ) стає визначальним чинником стабільності бізнес-процесів. Традиційні підходи до захисту потребують адаптації до динамічного середовища, де ключову роль відіграє своєчасне виявлення вразливостей та мінімізація ризиків на операційному рівні. Дослідження, присвячене розробці комплексу організаційно-технічних заходів та їх практичному впровадженню, має вагоме прикладне значення для зміцнення кіберстійкості організацій.

З огляду на це, вдосконалення методів функціонування СМІБ відповідно до вимог міжнародних стандартів є актуальним і своєчасним науковим завданням.

Позитивні сторони.

1. У роботі здійснено комплексний аналіз стану системи менеджменту інформаційної безпеки, ідентифіковано критичні процеси та класифіковано виявлені невідповідності.
2. Представлено методологічно обґрунтований підхід до аналізу кореневих причин інцидентів, що дозволило сформувати цілісну дорожню карту рекомендацій щодо вдосконалення СМІБ.
3. Проведено практичне впровадження комплексу організаційно-технічних заходів у реальному корпоративному середовищі, що підтвердило можливість підвищення рівня зрілості інформаційної безпеки підприємства.

Недоліки.

Доцільним було б доповнити роботу детальнішим оглядом та порівняльним аналізом спеціалізованих технічних засобів (зокрема, систем автоматизації управління патчами або платформ для моніторингу конфігурацій), що сприяють підвищенню ефективності операційних процесів СМІБ.

Зазначене зауваження має уточнюючий характер і не впливає на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки “_____”, а здобувач МОЙСЕЄВ Вадим заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент:
_____ _____ _____
підпис Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню вимог міжнародного стандарту ISO/IEC 27001:2022 до функціонування системи менеджменту інформаційної безпеки (СМІБ). Робота складається зі вступу, трьох розділів, що містять 6 рисунків, висновків і списку використаних джерел із 40 найменувань. Загальний обсяг роботи становить 80 сторінок, з яких 5 сторінок займає список використаних джерел.

Мета роботи **–** комплексний аналіз та систематизація методів забезпечення функціонування системи менеджменту інформаційної безпеки організації на теоретико-методологічному, операційному та практичному рівнях.

Об'єкт дослідження **–** система менеджменту інформаційної безпеки організації.

Предмет дослідження – методи забезпечення функціонування системи менеджменту інформаційної безпеки організації.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та синтезу, порівняльного аналізу, класифікації, а також системного підходу до моделювання показників результативності СМІБ.

Галузь застосування. Запропоновані підходи та результати аналізу можуть бути використані підприємствами й організаціями під час розробки, впровадження та підготовки до сертифікації власної системи менеджменту інформаційної безпеки. Особливо корисними ці рішення є для адаптації наявних систем захисту до актуальних вимог ISO/IEC 27001:2022 та підвищення загального рівня кіберстійкості.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, СИСТЕМА МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, СМІБ, ISO/IEC 27001:2022, ОЦІНЮВАННЯ РИЗИКІВ, ЗАХОДИ ЗАХИСТУ, АУДИТ БЕЗПЕКИ.

ABSTRACT

The qualification thesis is devoted to the study of the ISO/IEC 27001:2022 international standard requirements for the functioning of an information security management system (ISMS). The thesis consists of an introduction, three chapters including 6 figures, conclusions, and a list of references comprising 40 sources. The total volume of the work is 80 pages, of which 5 pages are occupied by the list of references.

The purpose of the study **is** a comprehensive analysis and systematization of methods for ensuring the functioning of an organization's information security management system at the theoretical, methodological, operational, and practical levels.

The object of the study **is** the information security management system of an organization.

The subject of the study is the methods of ensuring the functioning of an organization's information security management system.

Research methods. To solve the aforementioned scientific task, the study used methods of analysis and synthesis, comparative analysis, classification, as well as a systematic approach to modeling ISMS performance indicators.

Field of application. The proposed approaches and analysis results can be used by enterprises and organizations during the development, implementation, and preparation for the certification of their own information security management system. These solutions are especially useful for adapting existing security systems to the current ISO/IEC 27001:2022 requirements and increasing the overall level of cyber resilience.

Keywords: INFORMATION SECURITY, INFORMATION SECURITY MANAGEMENT SYSTEM, ISMS, ISO/IEC 27001:2022, RISK ASSESSMENT, SECURITY CONTROLS, SECURITY AUDIT.

ЗМІСТ

ВСТУП

Актуальність теми. За даними Verizon Data Breach Investigations Report 2023, понад 74% підтверджених витоків даних включають людський елемент — помилки персоналу, соціальну інженерію або викрадені облікові дані. Проте на практиці часто виникає розрив між формальною відповідністю вимогам міжнародних стандартів, зокрема ISO/IEC 27001, та реальною захищеністю активів на операційному рівні. Важливо не лише впроваджувати технічні рішення, а й формувати культуру безпеки серед персоналу та ефективно управляти процесами моніторингу й аудиту. Вдосконалення методів забезпечення функціонування СМІБ допоможе організації перевести управління безпекою з "паперового" формату у площину реальної та вимірюваної кіберстійкості.

Мета роботи – комплексний аналіз та систематизація методів забезпечення функціонування системи менеджменту інформаційної безпеки організації на теоретико-методологічному, операційному та практичному рівнях.

Об'єкт дослідження – система менеджменту інформаційної безпеки організації.

Предмет дослідження – методи забезпечення функціонування системи менеджменту інформаційної безпеки організації.

Для досягнення цієї мети в роботі необхідно виконати наступні завдання:

1. Дослідити теоретичні засади, еволюцію та нормативні вимоги до побудови систем менеджменту інформаційної безпеки.

2. Проаналізувати методи операційного управління захистом активів, роль людського фактора та оцінювання результативності системи.

3. Розробити прикладний інструментарій моніторингу СМІБ через систему показників (KPI) та модель оцінювання зрілості процесів.

4. Оцінити відповідність процесів захисту на умовному підприємстві та сформувати дорожню карту їх удосконалення.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та синтезу, порівняльного аналізу, класифікації, а також системного підходу до моделювання показників результативності СМІБ.

Практичне значення одержаних результатів. Застосування напрацювань дасть змогу здійснити обґрунтований вибір методів та інструментів забезпечення інформаційної безпеки на операційному рівні відповідно до цілей бізнесу, ризик-профілю та ресурсних можливостей підприємства.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 25 лютого 2026 року.

Розділ 1 ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ТА НОРМАТИВНІ ЗАСАДИ ФУНКЦІОНУВАННЯ СМІБ

У межах першого розділу розглянуто теоретико-методологічні та нормативні засади, що визначають сутність, архітектуру й умови функціонування системи менеджменту інформаційної безпеки організації. Досліджено концептуальну основу СМІБ у контексті міжнародних стандартів серії ISO/IEC 27000 — від витоків британської нормативної бази до чинної редакції ISO/IEC 27001:2022, — що дозволяє простежити еволюцію підходів до управління інформаційною безпекою та обґрунтувати актуальність системного погляду на цю проблематику. Детально проаналізовано вимоги стандарту ISO/IEC 27001:2022 як нормативного підґрунтя для побудови, впровадження та підтримки СМІБ, зокрема в частині структурних змін Додатку А та нових категорій заходів захисту. Окрему увагу приділено ризик-орієнтованому підходу як методологічній основі функціонування системи — розкрито процес ідентифікації, аналізу та оцінювання ризиків інформаційної безпеки у взаємозв'язку з вимогами ISO/IEC 27005 та загальною методологією управління ризиками за ISO 31000. Теоретичний фундамент, сформований у цьому розділі, забезпечує концептуальну та нормативну основу для дослідження методів забезпечення функціонування СМІБ, що є предметом розгляду наступних частин роботи.

1.1 Сутність, архітектура та еволюція СМІБ у межах стандартів серії ISO/IEC 27000

Понад 70% організацій, що зазнали витоку даних у 2023 році, мали задокументовані політики інформаційної безпеки — і все одно були скомпрометовані. Ця статистика IBM Cost of Data Breach Report наочно демонструє головну проблему галузі: середня вартість витоку досягла 4,45 мільйона доларів США, що на 15% перевищує показник 2020 року, а причиною

у більшості випадків виявляються організаційні прогалини та людський чинник, а не технічні вразливості [25]. Тривалий час підприємства обмежувалися точковими технічними заходами — антивірусним програмним забезпеченням, міжмережевими екранами, системами контролю доступу. Єдиної управлінської рамки, яка б пов'язувала ці інструменти у цілісну систему, не існувало. Саме ця прогалина і стала поштовхом до формування концепції СМІБ.

В Україні проблема набула особливої гостроти з 2022 року. Масштабні кібератаки на об'єкти критичної інфраструктури, державні установи та фінансовий сектор показали: технічна захищеність окремих вузлів інформаційної системи не рятує від скоординованого впливу [30]. Відповіддю є системний підхід до управління інформаційною безпекою, оформлений у вигляді СМІБ [4].

Система менеджменту інформаційної безпеки — це сукупність політик, процедур, процесів та засобів контролю, спрямованих на захист інформаційних активів організації відповідно до її бізнес-цілей та ризик-апетиту. Відповідно до стандарту ISO/IEC 27000:2018, СМІБ є частиною загальної системи менеджменту, що ґрунтується на підході з урахуванням бізнес-ризиків і призначена для створення, впровадження, функціонування, моніторингу, перегляду та вдосконалення інформаційної безпеки [3].

Ключова відмінність СМІБ від традиційних підходів — її управлінська природа. Система зосереджена не лише на технічних аспектах захисту, а й на процесах, людях, політиках та організаційній культурі. Вона встановлює чіткі ролі та відповідальності, формує механізми прийняття рішень щодо ризиків і забезпечує документованість процесів безпеки.

Необхідно розмежовувати поняття інформаційної безпеки та кібербезпеки — їх нерідко ототожнюють у практичному вжитку. Інформаційна безпека охоплює захист інформації у будь-якій формі: електронній, паперовій, усній. Кібербезпека зосереджена виключно на захисті цифрових активів. СМІБ є ширшою за обома цими поняттями і включає їх як складові [21].

Цільовою функцією СМІБ є забезпечення трьох фундаментальних властивостей інформації — так звана тріада CIA. Конфіденційність означає, що доступ мають виключно авторизовані особи. Цілісність гарантує точність і незмінність інформації протягом усього її життєвого циклу. Доступність забезпечує санкціонований доступ у потрібний момент. Практика свідчить про характерну диспропорцію: організації традиційно інвестують у конфіденційність непропорційно більше, ніж у доступність та цілісність, хоча саме порушення доступності у хмарних середовищах генерує найбільші прямі фінансові втрати через SLA-санкції [5].

Поряд із тріадою CIA розглядаються розширені властивості. Автентичність підтверджує справжність інформації та її джерела. Підзвітність забезпечує відстеження дій суб'єктів щодо інформаційних активів. Незаперечність виключає можливість відмови від вчинених дій. Надійність характеризує стабільність поведінки системи в штатних і нештатних умовах [5].

Архітектура СМІБ охоплює три рівні управління. Стратегічний рівень — де вище керівництво визначає цілі безпеки та розподіляє відповідальність. Стандарт ISO/IEC 27001:2022 у пункті 5 прямо зобов'язує керівництво інтегрувати вимоги СМІБ у бізнес-процеси. Без такої підтримки бюджети на безпеку скорочуються, а відповідальні особи залишаються без реальних повноважень. Тактичний рівень — де відбувається розробка процедур, управління ризиками та формування програм навчання персоналу. Тут стратегічні цілі перетворюються на конкретні плани дій. Операційний рівень — де реалізуються технічні та організаційні заходи захисту, здійснюється моніторинг подій і управління інцидентами щодня.

Центральним елементом архітектури є циклічна модель PDCA. Фаза планування передбачає визначення контексту, оцінювання ризиків та формування вимірюваних цілей. Фаза виконання охоплює впровадження заходів захисту та навчання персоналу. Фаза перевірки включає моніторинг, аудити та аналіз з боку керівництва. Фаза дії передбачає усунення невідповідностей та

ініціативи з постійного вдосконалення [17]. Взаємозв'язок ієрархії управління організацією з фазами безперервного циклу СМІБ візуалізовано на рисунку 1.1.

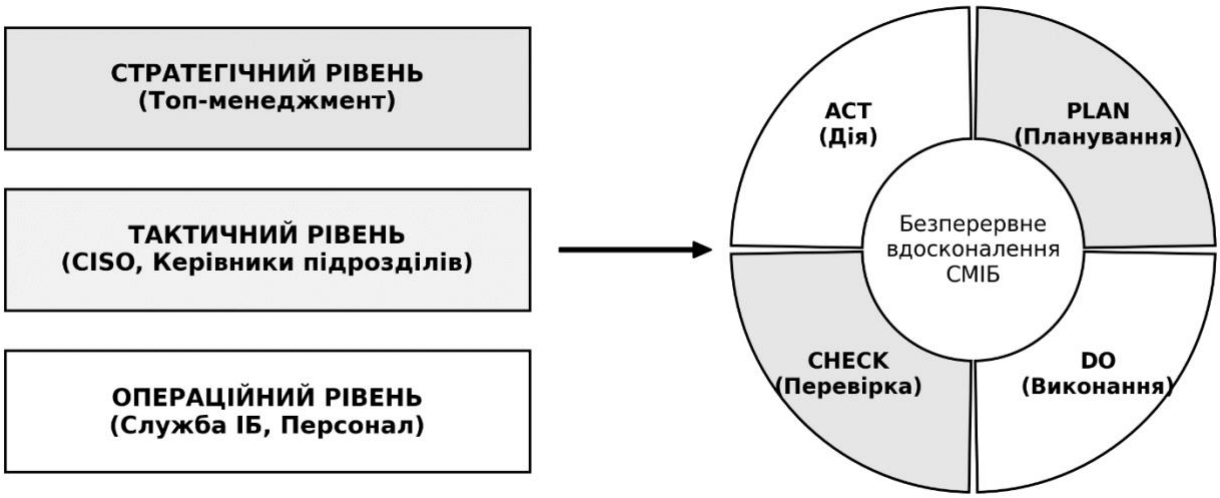

Рис. 1.1. Архітектура СМІБ: ієрархія управління та цикл PDCA

Важливим структурним елементом є реєстр інформаційних активів. Без чіткого розуміння того, які саме активи підлягають захисту та яку цінність вони мають для бізнесу, неможливо ані управляти ризиками, ані обґрунтовано розподіляти інвестиції в безпеку.

Становлення міжнародної нормативної бази у сфері управління інформаційною безпекою охоплює понад три десятиліття. Витоки сягають 1993 року, коли Британський інститут стандартів розпочав розробку практичних настанов з управління захистом інформації. У 1995 році опубліковано BS 7799 Part 1 — перелік кращих практик. У 1998 році з'явилась Part 2, що визначила вимоги до системи менеджменту та заклала основу для майбутньої незалежної сертифікації [28].

Примітно, що перехід від BS 7799 до ISO/IEC 27001:2005 зайняв понад десять років. Це свідчить: міжнародний консенсус щодо управлінської природи безпеки формувався поступово і нелегко. У 2000 році BS 7799 Part 1 прийнято як ISO/IEC 17799:2000 — початок глобального визнання системного підходу. У 2005

році BS 7799 Part 2 став ISO/IEC 27001:2005 — першим документом із формальними вимогами до СМІБ як об'єкта незалежної сертифікації. У 2007 році ISO/IEC 17799 перейменовано на ISO/IEC 27002, що дало початок нумерованій серії стандартів.

Редакція ISO/IEC 27001:2013 принесла суттєве структурне оновлення відповідно до Єдиної структури ISO (High Level Structure). Це забезпечило узгодженість із ISO 9001 та ISO 14001 і спростило впровадження інтегрованих систем менеджменту: зникло дублювання документації та управлінських структур.

Чинна редакція ISO/IEC 27001:2022 внесла найбільш значущі зміни за десятиліття. Кількість заходів захисту скорочено з 114 до 93. Структура переорганізована з 14 на 4 тематичні розділи: організаційні заходи (37 контролів), кадрові (8), фізичні (14) та технологічні (34). Введено 11 нових заходів — безпека хмарних сервісів, розвідка загроз, безпечне кодування та управління конфігураціями. Для кожного заходу в ISO/IEC 27002:2022 запроваджено атрибутивну схему, що класифікує контролі за типом (превентивний, детективний, коригувальний) та властивостями безпеки [6, 11].

Серія ISO/IEC 27000 налічує понад 40 стандартів. Базові — ISO/IEC 27000 зі словником термінів, 27001 з вимогами до СМІБ, 27002 з настановами щодо реалізації заходів. Управління ризиками регламентує ISO/IEC 27005 у взаємозв'язку з ISO 31000. Вимірювання та аудит охоплюють ISO/IEC 27004 і 27007 відповідно. Галузеві стандарти адресують специфічні сектори: 27017 — хмарні сервіси, 27018 — захист персональних даних у хмарі [7, 8].

Ця розгалужена екосистема є принциповою перевагою підходу ISO/IEC порівняно з альтернативними фреймворками [10, 37]. Організація отримує не лише вимоги, а й повний методологічний апарат: настанови з реалізації заходів, методологію управління ризиками, інструментарій вимірювання та механізм верифікації через аудит. Еволюція стандартів відображає зростаючу стратегічну

роль інформаційної безпеки — від технічної функції до невід'ємного елементу корпоративного управління.

1.2 Аналіз вимог стандарту ISO/IEC 27001:2022 до функціонування СМІБ

Стандарт ISO/IEC 27001:2022 є основним міжнародним нормативним документом, що встановлює вимоги до створення, впровадження, підтримки та постійного вдосконалення СМІБ. На відміну від ISO/IEC 27002, який містить рекомендаційні настанови, ISO/IEC 27001 формулює обов'язкові вимоги — будь-яке відхилення від них є формальною невідповідністю, що фіксується під час аудиту [6, 26]. Структура стандарту відповідає Єдиній структурі ISO і налічує десять розділів, змістовні вимоги яких зосереджені у розділах 4–10. Розуміти їх слід не як послідовний перелік, а як взаємозалежну систему, де кожен наступний елемент спирається на попередній.

Найпоширенішою причиною провалу СМІБ на практиці є не брак технічних рішень, а відсутність управлінського фундаменту. Відповідальність перекладається на ІТ-відділ, бюджети на безпеку скорочуються при першій фінансовій турбулентності, а керівники вищого рівня дізнаються про стан системи лише після інциденту. Саме тому стандарт у розділі 5 безкомпромісно покладає відповідальність на вище керівництво і прямо вказує: ця відповідальність не може бути делегована у повному обсязі. Конкретні зобов'язання охоплюють узгодження політики безпеки зі стратегічним напрямом організації, виділення ресурсів та формування культури безпеки. Призначення осіб, відповідальних за підтримку СМІБ та звітування про її результативність, також закріплено тут.

Проте лідерство саме по собі є порожньою вимогою без розуміння того, що саме захищається і від кого. Цю проблему вирішує розділ 4 — аналіз контексту організації. Зовнішній контекст охоплює правове середовище, ринкову

кон'юнктуру та відносини із зацікавленими сторонами. Внутрішній — організаційну структуру, корпоративну культуру та наявні інформаційні системи. Організація, що пропускає цей етап, будує систему захисту у вакуумі: формально відповідну стандарту, але нерелевантну власним ризикам. Окремо стандарт вимагає ідентифікувати зацікавлені сторони та їхні вимоги — клієнтів, акціонерів, регуляторів, постачальників [6, 16]. Нездатність це зробити призводить до юридичних ризиків та прогалин у захисті, що жодна технічна міра не компенсує.

Управлінський фундамент створює умови. Але реальна безпека або з'являється, або ні — на операційному рівні, де конкретні люди щодня ухвалюють рішення щодо інформаційних активів. Тут стандарт стикається з найскладнішою проблемою: формальні процедури самі по собі не змінюють поведінку.

Розділ 6 вирішує питання ризиків і цілей. Організація зобов'язана визначити критерії прийнятності ризиків, забезпечити відтворюваність результатів оцінювання та ідентифікувати ризики порушення конфіденційності, цілісності та доступності. За результатами формується план обробки ризиків із заходами захисту та власниками ризиків. Цілі безпеки мають бути вимірюваними — для кожної визначаються відповідальні особи, методи вимірювання і терміни. Ця вимога не є автономною: вона замикається на розділі 9 і формує управлінський цикл [15].

Розділ 7 розмежовує два поняття, які організації систематично плутають: компетентність і обізнаність. Компетентність стосується конкретних осіб, чия діяльність безпосередньо впливає на результативність системи — вимоги до їхніх знань визначаються і підтверджуються документально. Обізнаність є ширшою вимогою і поширюється на весь персонал. Програма навчання для аналітика SOC і програма для рядового бухгалтера — це принципово різні заходи. Стандарт це розуміє. Організації, що проводять єдиний річний тренінг для всіх категорій персоналу, цей принцип ігнорують і отримують передбачуваний результат.

Щоб уникнути надмірної бюрократії, стандарт у розділі 7.5 чітко обмежує обсяг обов'язкової документації. Центральним документом є Декларація про застосовність, саме вона є мостом між теоретичним переліком заходів захисту з Додатку А та реальними рішеннями організації щодо кожного з них. Надлишок документів без зв'язку з реальними процесами є таким самим ризиком для СМІБ, як і їх відсутність.

Розділ 8 закріплює операційні вимоги. Особлива увага зосереджена на управлінні зовнішньо наданими послугами: організація несе відповідальність за відповідність постачальників вимогам безпеки. Це потребує включення цих вимог до контрактів і регулярного моніторингу їх виконання — практика, якою більшість організацій нехтує до першого серйозного інциденту через скомпрометованого підрядника.

Найбільш недооціненим блоком стандарту є розділи 9 і 10 — механізми, що відрізняють живу СМІБ від формально задокументованої. Розділ 9 встановлює три механізми оцінювання. Перший — моніторинг і вимірювання. Відсутність формалізованих метрик є однією з найпоширеніших невідповідностей при сертифікаційних аудитах: організація просто не може продемонструвати результативність того, що не вимірює. Другий — внутрішній аудит за запланованими інтервалами. Третій — аналіз з боку керівництва, що зобов'язує регулярно розглядати стан системи з урахуванням результатів аудитів і змін у контексті.

Розділ 10 замикає цикл. Тут стандарт проводить принципову межу між двома поняттями, які організації роками ототожнюють. Корекція — це усунення наслідку: прибрали витік, відновили систему, закрили тікет. Коригувальна дія — це усунення причини: чому витік стався, яка системна вразливість це допустила, як унеможливити повторення. Перший підхід дає відчуття контролю. Другий — реальний контроль. Стандарт вимагає другого. Організації, що роками практикують перший, демонструють незмінний список повторюваних інцидентів при формально сертифікованій СМІБ.

Окремої уваги заслуговує Додаток А у редакції 2022 року. Перелік заходів скорочено з 114 до 93, структуру переорганізовано з 14 доменів на 4 тематичні розділи: організаційні (37 контролів), кадрові (8), фізичні (14) та технологічні (34). Порівняльний аналіз структурних змін наведено у Таблиці 1.1.

Таблиця 1.1

Порівняльний аналіз структури Додатку А стандартів ISO/IEC 27001 редакцій 2013 та 2022 років

Критерій порівняння	**ISO/IEC 27001:2013**	**ISO/IEC 27001:2022**
Загальна кількість заходів захисту	114	93
Кількість структурних розділів	14	4
Принцип групування заходів	Процесно-орієнтований (за 14 напрямами управління безпекою)	Категорійний (Організаційні, Кадрові, Фізичні, Технологічні)
Нові заходи захисту	Базовий набір	Введено 11 нових заходів (розвідка загроз, хмарна безпека тощо)
Атрибутивна класифікація	Відсутня	Запроваджено 5 категорій атрибутів для кожного заходу

Серед 11 нових заходів найбільш показовими є кілька. Розвідка загроз — раніше це вважалося доброю практикою великих компаній, тепер є обов'язковою вимогою для всіх. Управління конфігураціями є відповіддю на статистику: переважна більшість успішних атак на хмарну інфраструктуру використовує помилки конфігурації, а не нові вразливості. Безпека хмарних сервісів нарешті закріплює управління ризиками хмарних обчислень як обов'язковий елемент системи. Ці доповнення не є випадковими. Вони відображають головну тенденцію: межа між фізичною та кіберзагрозою, між внутрішньою інфраструктурою та хмарним середовищем стає дедалі більш умовною [11].

1.3 Ризик-орієнтований підхід як основа функціонування СМІБ

Ризик-орієнтований підхід є методологічною серцевиною сучасної концепції управління інформаційною безпекою. Його принципова відмінність від попередніх підходів полягає у відмові від універсального переліку заходів захисту, що застосовуються однаково до всіх організацій, на користь індивідуалізованої системи захисту, побудованої на аналізі конкретних загроз, вразливостей та наслідків для бізнесу. Стандарт ISO/IEC 27001:2022 закріплює ризик-орієнтований підхід як обов'язкову методологічну основу. Ігнорування цих вимог унеможливлює успішне проходження сертифікації [6].

Концептуальна передумова підходу проста, але часто ігнорується на практиці: абсолютна захищеність є недосяжною і економічно недоцільною метою. Будь-яка організація функціонує в умовах обмежених ресурсів і не може одночасно реалізувати весь можливий спектр заходів захисту. Ризик-орієнтований підхід вирішує цю дилему — надає інструментарій для обґрунтованого розподілу ресурсів відповідно до пріоритетів, визначених на основі об'єктивної оцінки ризиків. Захист концентрується там, де наслідки реалізації загроз є найбільш значущими. Залишкові ризики у менш критичних областях свідомо приймаються.

Термінологічна база підходу закріплена у стандарті ISO/IEC 27000:2018 та узгоджена з ISO 31000. Ризик інформаційної безпеки — це вплив невизначеності на цілі безпеки, що конкретизується як поєднання ймовірності події та її наслідків. Загроза — потенційна причина небажаного інциденту. Вразливість — слабкість активу або заходу захисту, яка може бути використана загрозою. Захід захисту — засіб, що модифікує ризик через зменшення ймовірності, усунення вразливості або пом'якшення наслідків [5, 17]. Взаємозв'язок ключових понять управління ризиками показано на рисунку 1.2.

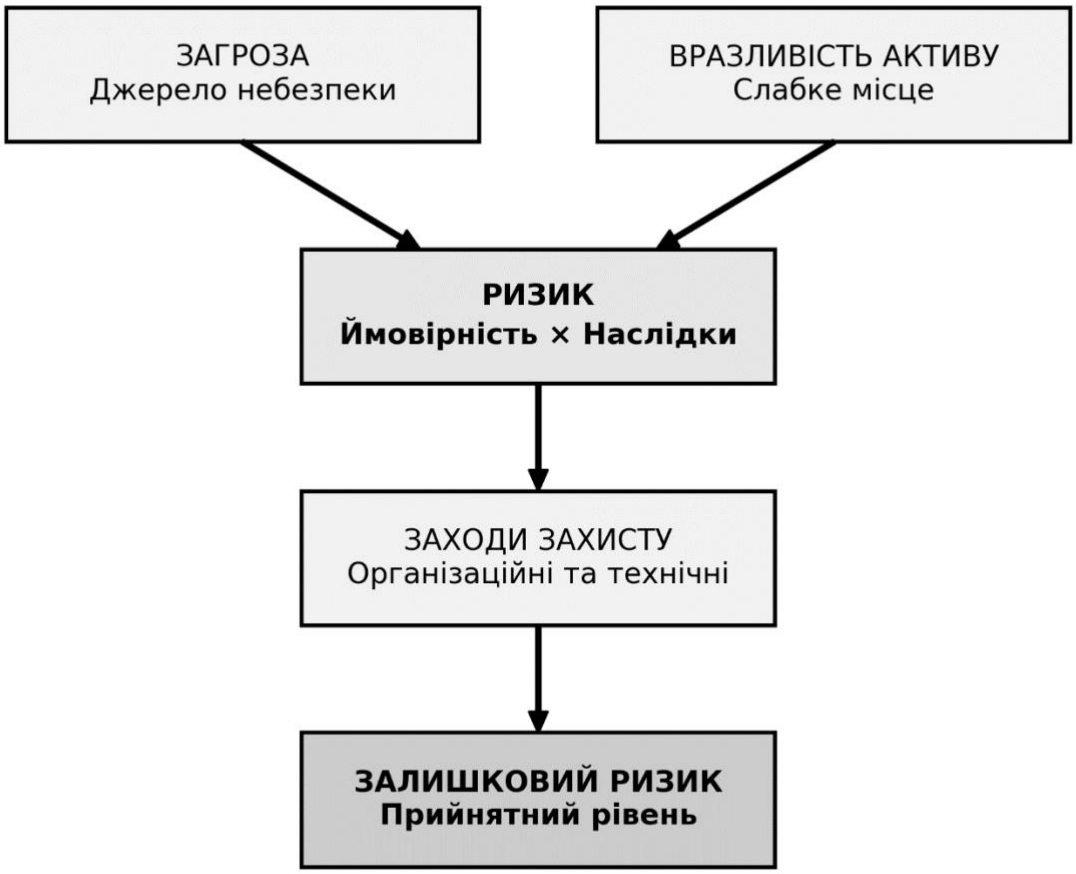

Рис. 1.2. Взаємозв'язок ключових понять управління ризиками

Процес управління ризиками, регламентований ISO/IEC 27005:2022, охоплює кілька послідовних етапів. Встановлення контексту визначає цілі та критерії управління ризиками. Оцінювання включає ідентифікацію, аналіз та порівняльну оцінку. Обробка передбачає вибір і реалізацію варіантів реагування. Моніторинг і перегляд забезпечують актуальність оцінок. Комунікація зі зацікавленими сторонами супроводжує весь процес [13]. Важливо розуміти: це не лінійна послідовність кроків, а ітераційний цикл — кожен новий інцидент або зміна в середовищі організації є підставою для повернення до попередніх етапів.

Ідентифікація ризиків є першим і визначальним етапом. Некоректна або неповна ідентифікація означає, що певні загрози залишаться поза увагою незалежно від того, наскільки ретельно будуть оброблені виявлені ризики [31]. Процес охоплює встановлення переліку активів та їх власників, визначення

загроз для кожного активу, виявлення вразливостей та ідентифікацію потенційних наслідків з точки зору порушення конфіденційності, цілісності та доступності.

На практиці організації поєднують кілька методів ідентифікації — структуровані інтерв'ю з власниками бізнес-процесів, аналіз попередніх інцидентів, галузеві каталоги загроз і результати тестування на проникнення. Жоден з них окремо не забезпечує вичерпного охоплення. Каталоги ENISA та NIST слугують корисними відправними точками, однак потребують адаптації — загроза, критична для банківського сектору, може бути незначущою для виробничого підприємства і навпаки [32].

Аналіз ризиків передбачає оцінювання ймовірності та потенційних наслідків. Залежно від наявності статистичних даних та рівня зрілості організації застосовуються якісні, кількісні або змішані методи [2]. Якісний аналіз оперує описовими шкалами — ймовірність «висока», «середня», «низька», наслідки «критичні», «суттєві», «незначні». Його перевага — простота і можливість залучення експертних суджень без накопичення великих масивів даних. Кількісний аналіз оперує числовими значеннями та фінансовими оцінками наслідків — він дозволяє розраховувати очікувані втрати та обґрунтовувати інвестиції у заходи захисту з позиції економічної доцільності [34]. Практичним інструментом для порівняльної оцінки та пріоритизації є матриця ризиків, наведена у Таблиці 1.2.

Таблиця 1.2

Матриця оцінювання рівня ризиків інформаційної безпеки

Ймовірність / Наслідки	**Незначні (1)**	**Помірні (2)**	**Суттєві (3)**	**Катастрофічні (4)**
Дуже висока (4)	4 (Середній)	8 (Високий)	12 (Високий)	16 (Критичний)
Висока (3)	3 (Низький)	6 (Середній)	9 (Високий)	12 (Високий)
Середня (2)	2 (Низький)	4 (Середній)	6 (Середній)	8 (Високий)
Низька (1)	1 (Прийнятний)	2 (Низький)	3 (Низький)	4 (Середній)

Порівняльна оцінка ризиків передбачає зіставлення результатів аналізу із критеріями прийнятності. Критерії є індивідуальними для кожної організації та відображають її ризик-апетит — готовність приймати певний рівень ризику заради досягнення бізнес-цілей. Це стратегічне рішення вищого керівництва, що безпосередньо визначає обсяг інвестицій у безпеку [13, 17].

Обробка ризиків — етап, де організація ухвалює рішення щодо реагування на кожен ризик, що перевищує поріг прийнятності. ISO/IEC 27005:2022 визначає чотири варіанти. Модифікація — реалізація заходів захисту, що знижують ймовірність загрози або зменшують наслідки. Це найпоширеніший варіант, що охоплює переважну більшість реалізованих заходів. Прийняття — свідоме рішення не вживати додаткових заходів, оскільки ризик відповідає критеріям прийнятності або витрати на захист перевищують потенційні втрати. Уникнення — відмова від діяльності або процесу, що генерує ризик. Наприклад, рішення не переводити критичний бізнес-процес у хмарне середовище через неприйнятний рівень ризиків. Передача — перенесення відповідальності на третю сторону через страхування або договірні механізми.

На практиці ієрархія цих варіантів суттєво відрізняється залежно від галузі та контексту. Для хмарних провайдерів передача ризику через страхування кіберризиків є теоретично привабливим, але найменш поширеним варіантом — через складність актуарної оцінки кіберризиків та обмеженість цього ринку в Україні. Модифікація домінує як основний інструмент, однак у поєднанні з прийняттям залишкових ризиків там, де вартість додаткового захисту перевищує потенційні збитки. Уникнення залишається крайнім заходом: відмова від бізнес-процесу задля зниження ризику — рішення, що потребує узгодження не з CISO, а з радою директорів.

За результатами обробки формується план обробки ризиків — центральний операційний документ СМІБ з переліком заходів захисту, власниками, термінами та очікуваним впливом на рівень ризику. Паралельно формується декларація про застосовність: документ, що перераховує всі заходи з Додатку А ISO/IEC 27001

із обґрунтуванням рішення щодо кожного — включити або виключити. Це один із ключових об'єктів перевірки під час сертифікаційного аудиту.

Після реалізації заходів оцінюється залишковий ризик. Якщо він перевищує поріг прийнятності, організація або реалізує додаткові заходи, або переглядає критерії прийнятності з обґрунтуванням для керівництва. Прийняття залишкових ризиків оформлюється як формальне рішення власників ризиків — це забезпечує підзвітність і прозорість процесу.

Взаємозв'язок між управлінням ризиками та функціонуванням СМІБ є двостороннім. Результати оцінювання визначають склад заходів захисту. Водночас функціонування СМІБ — моніторинг подій, управління інцидентами, аудити — генерує нову інформацію, що є підставою для перегляду оцінок ризиків. Цей зворотний зв'язок забезпечує динамічність системи та її здатність адаптуватися до змін у ландшафті загроз.

Методологічний взаємозв'язок між ISO/IEC 27005 та ISO 31000 є принципово важливим. ISO 31000 встановлює універсальні принципи управління ризиками, застосовні до будь-якого їх типу [33]. ISO/IEC 27005 конкретизує ці принципи стосовно інформаційної безпеки. Така архітектура дозволяє інтегрувати управління ризиками безпеки у загальну корпоративну систему, уникаючи паралельних і несумісних процесів.

Великі організації застосовують GRC-системи — спеціалізовані платформи з централізованим реєстром ризиків, автоматизованим моніторингом і формуванням звітності. Середні та малі частіше обмежуються табличними інструментами та якісними методами. Це прийнятно за умови методологічної послідовності та документування результатів. Проте типова пастка тут одна: оцінювання ризиків перетворюється на документаційну вправу, результати якої не впливають на реальні рішення. Це відбувається тоді, коли процес відокремлений від осіб, що приймають рішення про бюджети, або коли результати не перекладаються у зрозумілу для керівництва бізнес-мову. Формально красивий реєстр ризиків у таблиці Excel, який ніхто не читає після

затвердження — не рідкість. Це і є головна організаційна проблема впровадження підходу.

Ризик-орієнтований підхід не є статичним. Зміна бізнес-моделі, впровадження нових технологій, розширення географії діяльності або фіксація нових типів атак у галузі — кожна з цих подій є підставою для позапланового перегляду оцінок. Стандарт ISO/IEC 27001:2022 закріплює цю вимогу у розділі 6.1.2, зобов'язуючи проводити оцінювання як за запланованими інтервалами, так і при суттєвих змінах. Динамічність процесу це саме та характеристика, що відрізняє зрілу СМІБ від формально сертифікованої системи, яка не відображає актуального стану захищеності організації [6, 13, 17].

Висновки до розділу 1

У першому розділі досліджено теоретико-методологічні та нормативні засади функціонування системи менеджменту інформаційної безпеки. Особливу увагу приділено систематизації підходів до розуміння сутності СМІБ, що дозволило визначити її як управлінську систему, принципово відмінну від набору розрізнених технічних засобів захисту: вона охоплює процеси, людей, технології та організаційну культуру одночасно, реалізуючись через три взаємопов'язані рівні управління у рамках циклічної моделі PDCA.

Простежена еволюція міжнародної нормативної бази від британського BS 7799 до чинного ISO/IEC 27001:2022 відображає поступову трансформацію галузевого розуміння безпеки від технічно орієнтованого переліку заходів до повноцінної управлінської системи із механізмом незалежної сертифікації. Редакція 2022 року є найбільш значущим оновленням за десятиліття: реструктурований Додаток А з 93 заходами у чотирьох тематичних розділах та 11 нових контролів відображають адаптацію нормативної бази до сучасного ландшафту загроз, у якому межа між фізичними та кіберзагрозами, між

внутрішньою інфраструктурою та хмарним середовищем стає дедалі умовнішою.

Аналіз вимог стандарту ISO/IEC 27001:2022 виявив їхній системний взаємозалежний характер: якість виконання кожного елемента безпосередньо впливає на результативність наступного. Встановлено, що найпоширенішими причинами провалу СМІБ на практиці є відсутність реального лідерства вищого керівництва, формальне ставлення до аналізу контексту та підміна системного усунення причин невідповідностей поверхневою корекцією їхніх симптомів.

Ризик-орієнтований підхід обґрунтовано як єдину методологічно коректну основу функціонування СМІБ в умовах обмежених ресурсів. Процес управління ризиками відповідно до ISO/IEC 27005:2022 є ітераційним циклом, що забезпечує динамічну адаптацію системи захисту до змін у середовищі організації. Виявлено характерну практичну проблему: оцінювання ризиків нерідко перетворюється на документаційну вправу, відірвану від реальних управлінських рішень, що нівелює методологічну цінність підходу незалежно від якості його технічної реалізації.

Теоретичний фундамент, закладений у цьому розділі, формує концептуальну та нормативну основу для дослідження конкретних методів забезпечення функціонування СМІБ на операційному рівні, що є предметом розгляду наступного розділу.

Розділ 2 МЕТОДИ ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНУВАННЯ СМІБ

У межах другого розділу досліджено методи, що забезпечують практичне функціонування системи менеджменту інформаційної безпеки на операційному рівні. Розглянуто підходи до операційного управління процесами СМІБ та реалізації заходів захисту як механізму трансформації нормативних вимог і результатів оцінювання ризиків у конкретні організаційні та технічні рішення. Окрему увагу приділено управлінню людським фактором, а саме навчанню, підвищенню обізнаності та формуванню компетентності персоналу, що є критично значущим напрямом з огляду на провідну роль людської складової у переважній більшості зафіксованих інцидентів інформаційної безпеки. Завершальним блоком розділу є аналіз методів моніторингу, вимірювання та оцінювання результативності СМІБ, що забезпечують зворотний зв'язок, необхідний для обґрунтованого прийняття управлінських рішень і реалізації принципу постійного вдосконалення. Сукупність розглянутих методів формує операційний каркас СМІБ, що пов'язує стратегічні цілі інформаційної безпеки з їх практичним втіленням у щоденній діяльності організації.

2.1 Операційне управління процесами СМІБ та реалізація заходів захисту

Операційне управління процесами СМІБ являє собою сукупність скоординованих дій, спрямованих на практичну реалізацію заходів захисту, визначених за результатами оцінювання ризиків та задокументованих у плані їх обробки. Якщо стратегічний та тактичний рівні СМІБ забезпечують нормативну та методологічну основу системи, то операційний рівень є тим середовищем, де абстрактні вимоги стандарту перетворюються на конкретні процедури, технічні конфігурації та організаційні практики, що безпосередньо визначають реальний рівень захищеності організації [40]. Розрив між формальною відповідністю та

фактичною результативністю СМІБ найчастіше виникає на операційному рівні. Причинами є неналежне виконання процедур, послаблений контроль або відсутність механізмів виявлення відхилень. Серед усіх операційних процесів СМІБ управління вразливостями та управління доступом генерують найбільшу частку інцидентів при їхньому неналежному виконанні, що підтверджується свіжими даними галузевих звітів Verizon DBIR — і саме вони потребують першочергової автоматизації на рівні підприємства.

Розділ 8 стандарту ISO/IEC 27001:2022 встановлює вимоги до операційного планування та управління, зобов'язуючи організацію планувати, впроваджувати, контролювати, підтримувати та переглядати процеси, необхідні для виконання вимог інформаційної безпеки. При цьому стандарт не регламентує конкретний спосіб організації цих процесів, надаючи організації свободу у виборі методів відповідно до її розміру, галузевої специфіки та рівня зрілості. Така гнучкість є перевагою підходу ISO/IEC 27001, проте одночасно покладає на організацію відповідальність за самостійне проектування операційної моделі СМІБ.

Фундаментом операційного управління є реєстр інформаційних активів — систематизований перелік усіх ресурсів організації, що підлягають захисту. Активи класифікуються за типами: первинні активи охоплюють інформацію та бізнес-процеси, що мають безпосередню цінність для організації; допоміжні активи включають апаратне забезпечення, програмне забезпечення, мережеву інфраструктуру, персонал та фізичні засоби, що забезпечують обробку та зберігання первинних активів. Для кожного активу визначається власник — особа або підрозділ, відповідальні за забезпечення належного захисту, також рівень класифікації відповідно до корпоративної схеми класифікації інформації. Без актуального реєстру активів операційне управління позбавляється своєї об'єктної основи: неможливо ефективно захищати те, про існування чого або не відомо, або відсутня чітка відповідальність.

Класифікація інформації є обов'язковим організаційним заходом, що визначає рівень захисту, який застосовується до кожної категорії інформаційних активів. Типова корпоративна схема класифікації передбачає чотири рівні: відкрита інформація, що може вільно поширюватися за межами організації; внутрішня інформація, призначена виключно для внутрішнього використання; конфіденційна інформація з обмеженим колом осіб, що мають до неї доступ; та інформація з обмеженим доступом або таємна, розголошення якої може завдати критичної шкоди організації. Схема класифікації має бути підкріплена чіткими процедурами маркування носіїв інформації та правилами поводження з кожним класом — у протилежному разі класифікація залишається номінальною і не впливає на реальну практику обробки інформації [11].

Управління доступом є одним із центральних операційних процесів СМІБ, що безпосередньо реалізує принцип мінімальних привілеїв — кожна особа, процес або система мають отримувати виключно той рівень доступу, що є необхідним і достатнім для виконання їхніх функцій. Операційна реалізація управління доступом охоплює кілька взаємопов'язаних компонентів. Управління ідентифікацією та автентифікацією передбачає унікальну ідентифікацію кожного користувача, застосування надійних механізмів автентифікації, зокрема багатофакторної автентифікації для доступу до критичних систем — та управління обліковими записами протягом усього їхнього життєвого циклу від створення до деактивації. Авторизація та рольова модель доступу забезпечують відповідність наданих прав доступу функціональним обов'язкам користувача, визначеним у рольовій матриці доступу. Моніторинг та журналювання доступу фіксують факти доступу до критичних ресурсів, що є необхідним як для виявлення аномалій, так і для розслідування інцидентів [11].

Управління вразливостями є операційним процесом, що забезпечує своєчасне виявлення та усунення технічних слабкостей в інформаційних системах організації. Процес охоплює регулярне сканування інфраструктури спеціалізованими інструментами — такими як Nessus, Qualys або OpenVAS.

Аналіз виявлених вразливостей із урахуванням їхньої критичності за шкалою CVSS (Common Vulnerability Scoring System), пріоритизацію усунення на основі рівня ризику та контроль за своєчасним застосуванням патчів і оновлень. Стандарт ISO/IEC 27002:2022 у заході захисту 8.8 прямо вимагає від організацій отримання інформації про технічні вразливості використовуваних інформаційних систем, оцінювання їх впливу та вжиття відповідних заходів. На практиці управління патчами є одним із найбільш операційно складних процесів СМІБ, оскільки вимагає балансування між вимогами безпеки та потребами забезпечення безперервності бізнес-процесів, що нерідко є конкуруючими пріоритетами.

Управління інцидентами інформаційної безпеки є критичним операційним процесом, ефективність якого безпосередньо визначає здатність організації мінімізувати наслідки реалізованих загроз. Процес управління інцидентами структурується відповідно до усталеної моделі, що охоплює кілька послідовних фаз [9]. Підготовка передбачає формування команди реагування на інциденти, розробку процедур реагування, підготовку необхідних інструментів та проведення навчань. Виявлення та аналіз охоплюють ідентифікацію подій безпеки з різних джерел — систем виявлення вторгнень, журналів аудиту, повідомлень від персоналу та їх класифікацію за рівнем критичності. Стримування спрямоване на обмеження поширення інциденту та запобігання подальшій шкоді. Усунення передбачає ліквідацію причин інциденту та відновлення нормального функціонування систем. Відновлення забезпечує повернення до штатного операційного режиму. Аналіз після інциденту дозволяє витягти уроки та вдосконалити процедури реагування з урахуванням національних регуляторних вимог [19, 25]. Загальну послідовність етапів цього процесу у вигляді циклічної структури представлено на рисунку 2.1.

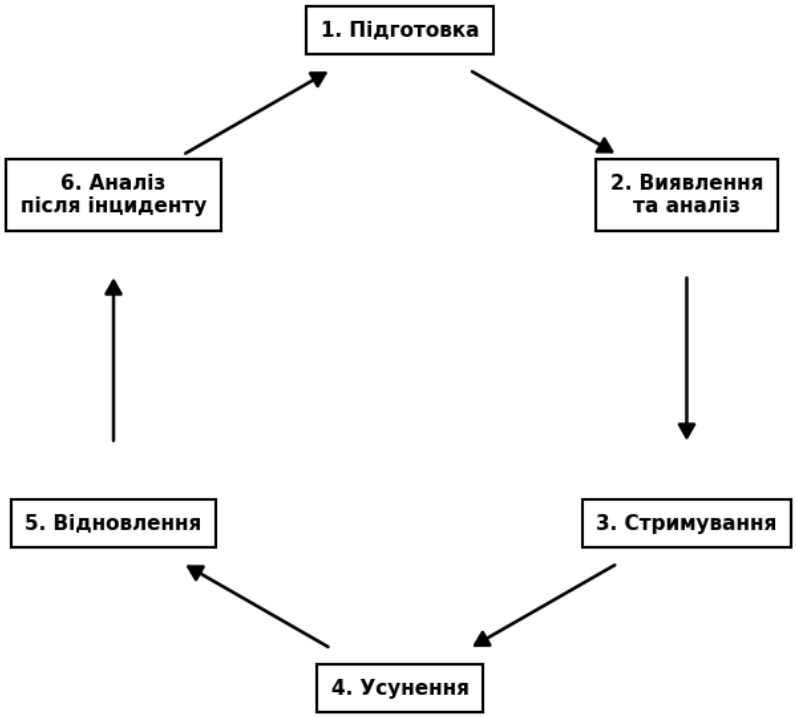

Рис. 2.1. Життєвий цикл управління інцидентами інформаційної безпеки

Управління безперервністю бізнесу та відновленням після катастроф є операційним процесом, що забезпечує здатність організації підтримувати критичні функції в умовах суттєвих збоїв або повністю відновити їх у прийнятні терміни. У контексті СМІБ управління безперервністю реалізується через розробку та регулярне тестування планів забезпечення безперервності інформаційно-комунікаційних технологій (ICT continuity plans), що визначають процедури резервного копіювання, відновлення систем та альтернативні способи обробки інформації на період збою. Новий захід захисту 5.30 у ISO/IEC 27002:2022 прямо вимагає планування готовності ІКТ до забезпечення безперервності бізнесу, встановлюючи зв'язок між системою менеджменту інформаційної безпеки та більш широким контекстом організаційної стійкості.

Управління відносинами із постачальниками набуває дедалі більшого значення в операційному контексті СМІБ, що пов'язано з широким поширенням аутсорсингу ІТ-функцій, використання хмарних сервісів та залежності від розгалужених ланцюжків постачання програмного забезпечення. Компрометація

постачальника може стати вектором атаки на організацію-замовника — практика, яку наочно продемонстрував інцидент із SolarWinds у 2020 році, що зачепив тисячі організацій по всьому світу через скомпрометоване оновлення програмного забезпечення. Операційне управління відносинами із постачальниками передбачає включення вимог інформаційної безпеки до контрактів і угод про рівень обслуговування, проведення оцінювань безпеки постачальників перед встановленням відносин та на регулярній основі протягом дії контракту, а також моніторинг виконання погоджених вимог безпеки [24].

Криптографічний захист інформації є технічним операційним заходом, що забезпечує конфіденційність і цілісність даних при їх зберіганні та передачі. Операційна реалізація криптографічного захисту вимагає розробки та дотримання корпоративної політики щодо використання криптографії, що визначає допустимі алгоритми та довжини ключів, вимоги до управління ключами протягом їхнього життєвого циклу — генерації, розподілу, зберігання, ротації та знищення — а також сфери обов'язкового застосування шифрування. Неналежне управління ключами є поширеною операційною проблемою, що нівелює теоретичну стійкість застосованих криптографічних алгоритмів: ключі, що зберігаються разом із зашифрованими даними або не ротуються протягом тривалого часу, суттєво знижують ефективність криптографічного захисту.

Фізична безпека та захист середовища є операційним компонентом СМІБ, що нерідко недооцінюється організаціями, зосередженими переважно на кіберзагрозах. Несанкціонований фізичний доступ до серверного обладнання, робочих станцій або носіїв інформації може призвести до витоку даних, що за своїми наслідками є рівнозначним успішній кібератаці. Операційні заходи фізичної безпеки охоплюють організацію захищених зон із контрольованим доступом для критичного обладнання, захист від фізичних загроз навколи

шнього середовища — пожежі, затоплення, перебоїв у електропостачанні, а також забезпечення безпечного знищення або повторного використання носіїв інформації. Редакція ISO/IEC 27002:2022 доповнила перелік фізичних заходів

захисту вимогами щодо моніторингу фізичної безпеки, що відображає зростаючу увагу до гібридних загроз, що поєднують фізичний та кіберкомпоненти.

Операційне управління мережевою безпекою охоплює реалізацію заходів захисту на рівні мережевої інфраструктури організації. Сегментація мережі за допомогою демілітаризованих зон, VLAN та мікросегментації обмежує можливості горизонтального переміщення зловмисника у випадку компрометації одного із сегментів. Фільтрація мережевого трафіку засобами міжмережевих екранів наступного покоління (NGFW) та систем запобігання вторгненням (IPS) забезпечує контроль дозволених комунікацій. Безпечне управління віддаленим доступом через VPN або системи нульової довіри (Zero Trust Network Access) є особливо актуальним в умовах поширення гібридних моделей роботи, за яких межа між корпоративною та зовнішньою мережею стає умовною [23].

Концепція DevSecOps передбачає інтеграцію практик безпеки на всіх етапах життєвого циклу розробки — від проектування архітектури до тестування та розгортання. Для організацій, що поєднують надання хмарних послуг з розробкою програмного забезпечення — як у випадку модельного підприємства ТОВ «ТехКлауд», аналіз якого наведено у наступних розділах — впровадження DevSecOps є не просто теоретичною рекомендацією, а гострою операційною необхідністю. Захід захисту 8.28 у новій редакції ISO/IEC 27002:2022 «Безпечне кодування» чітко закріплює вимоги щодо обов'язкового застосування принципів безпечного кодування, що відображає визнання вразливостей програмного забезпечення як самостійного класу критичних ризиків [38].

Операційне управління конфігураціями є процесом, що забезпечує підтримку еталонних безпечних конфігурацій для всіх компонентів інформаційної інфраструктури — серверів, робочих станцій, мережевого обладнання, баз даних та хмарних сервісів [22]. Неналежно налаштовані системи є одним із найбільш поширених векторів атак: дослідження Gartner свідчать, що переважна більшість успішних атак на хмарну інфраструктуру використовує помилки конфігурації, а не нові вразливості [29]. Захід захисту 8.9 «Управління

конфігурацією» є ще одним новим елементом ISO/IEC 27002:2022, що закріплює обов'язковість формалізованого підходу до управління конфігураціями як операційного заходу захисту [1].

Взаємозалежність операційних процесів СМІБ визначає необхідність їх розгляду як єдиної системи, а не набору ізольованих заходів. Реєстр активів живить процес управління ризиками, результати якого визначають пріоритети управління вразливостями та доступом. Управління інцидентами генерує дані, що є підставою для перегляду оцінок ризиків і коригування конфігурацій. Управління постачальниками впливає на результати оцінювання ризиків ланцюжка постачання. Криптографічний захист підтримує режим конфіденційності, встановлений класифікацією активів. Будь-який розрив у цих взаємозалежностях, зокрема відсутність актуалізації реєстру активів після суттєвих змін в інфраструктурі, послаблює всю операційну систему захисту незалежно від якості її окремих компонентів.

2.2 Управління людським фактором: навчання, обізнаність і формування компетентності персоналу

Людський фактор посідає особливе місце у структурі ризиків інформаційної безпеки — не як периферійний елемент, а як системна детермінанта переважної більшості зафіксованих інцидентів [14]. За даними звіту Verizon Data Breach Investigations Report, понад 74% підтверджених витоків даних включають людський елемент — помилки персоналу, зловживання привілеями, соціальну інженерію або використання викрадених облікових даних. Ця статистика не змінюється принципово протягом останніх років, що свідчить про структурний, а не випадковий характер проблеми. Технічні засоби захисту, якими б досконалими вони не були, не здатні компенсувати відсутність належної обізнаності та компетентності персоналу — саме тому управління людським

фактором є не допоміжним, а центральним напрямом операційного забезпечення функціонування СМІБ [3].

Стандарт ISO/IEC 27001:2022 чітко розмежовує поняття компетентності та обізнаності. У практичній діяльності ці терміни нерідко помилково уподібнюють. Згідно з розділом 7.2 стандарту, компетентність стосується персоналу, чия діяльність впливає на результативність СМІБ. Для таких осіб встановлюються вимоги до знань та навичок. Здобуття кваліфікації забезпечується навчанням або професійним досвідом, а результати підтверджуються документально. Обізнаність відповідно до розділу 7.3 є значно ширшою вимогою. Вона стосується всіх осіб, що працюють під контролем організації, незалежно від їхніх функцій: вони мають розуміти політику інформаційної безпеки, свій особистий внесок у результативність СМІБ та наслідки недотримання її вимог. Розуміння цього розмежування є принципово важливим для проектування програм навчання: заходи з підвищення обізнаності охоплюють увесь персонал, тоді як спеціалізоване навчання з формування компетентності адресоване конкретним ролям з чітко визначеними вимогами [5].

Програма підвищення обізнаності персоналу з інформаційної безпеки є основним інструментом управління людським фактором у більшості організацій. Ефективна програма принципово відрізняється від одноразового річного тренінгу, що є типовою, але малорезультативною практикою. Дослідження у сфері когнітивної психології та навчання дорослих демонструють, що знання, отримані в ході одноразового навчального заходу, швидко втрачаються за відсутності регулярного підкріплення — ефект, відомий як крива забування Еббінгауза. Натомість ефективні програми обізнаності будуються на принципах безперервного навчання, що передбачають регулярні короткі навчальні модулі, практичні симуляції загроз та постійне підкріплення ключових повідомлень через різноманітні канали комунікації. Стандарт ISO/IEC 27001:2022, однак, не встановлює мінімальної частоти або жорстких графіків навчання — він лише вимагає впровадження «доцільних» заходів обізнаності. Це залишає організаціям

надмірну свободу дій, яка на практиці часто реалізується через мінімально необхідні, суто формальні одноразові тренінги, що не мають реального впливу на поведінку співробітників [27, 28].

Проектування програми підвищення обізнаності починається з аналізу цільової аудиторії та ідентифікації специфічних ризиків, пов'язаних із різними категоріями персоналу. Керівники вищої ланки є мішенями для атак типу «китобійний фішинг» (whaling) та компрометації корпоративної електронної пошти (BEC), що вимагає спеціалізованого навчання з розпізнавання таких загроз. Фінансовий персонал піддається підвищеному ризику шахрайства із платіжними дорученнями та соціальної інженерії з боку зловмисників, що видають себе за керівників або контрагентів. Технічний персонал потребує поглибленого розуміння безпечних практик розробки, управління привілейованим доступом та процедур реагування на інциденти. Персонал, що працює з персональними даними клієнтів, має бути навчений специфічним вимогам захисту даних відповідно до чинного законодавства.

Змістове наповнення програм обізнаності охоплює кілька ключових тематичних блоків, актуальність яких визначається результатами оцінювання ризиків та аналізом попередніх інцидентів. Фішинг та соціальна інженерія залишаються пріоритетними темами навчання з огляду на їхню провідну роль як вектора первинного проникнення в інформаційні системи організацій. Навчання з розпізнавання фішингу повинно охоплювати не лише класичні ознаки атак, як-от помилки у тексті чи підозрілі адреси. Необхідно навчати персоналу виявляти й сучасні цільові атаки, де зловмисники використовують персоналізований підхід та ретельно підготовлені легітимні повідомлення.

Безпека паролів та управління обліковими даними є темою, практична реалізація якої безпосередньо залежить від поведінки персоналу. Незважаючи на широку обізнаність про необхідність використання надійних паролів, повторне використання паролів у різних сервісах, використання легко вгадуваних комбінацій та несвоєчасна зміна скомпрометованих облікових даних

залишаються поширеними практиками. Навчання з цієї теми має включати практичну демонстрацію використання менеджерів паролів та багатофакторної автентифікації, а не лише теоретичні вимоги до складності пароля.

Безпечне поводження з інформацією та носіями охоплює правила класифікації, маркування, зберігання та знищення інформаційних активів. Особливої актуальності ця тема набуває в контексті поширення гібридних моделей роботи, за яких корпоративна інформація обробляється на персональних пристроях, передається через незахищені мережі та зберігається у несанкціонованих хмарних сервісах — явище, що отримало назву «тіньові IT» (shadow IT). Фізична безпека робочого місця —практика чистого стола та чистого екрана, захист від підглядання у публічних місцях, безпечне знищення паперових документів — також є компонентом навчання, що нерідко залишається поза увагою програм, зосереджених виключно на кіберзагрозах.

Процедури звітування про інциденти та підозрілі події є темою навчання, від якої безпосередньо залежить час виявлення інцидентів. За даними IBM Cost of Data Breach Report, середній час між початком витоку даних та його виявленням у 2023 році становив 204 дні. Значна частина цього часу пояснюється тим, що персонал або не розпізнає ознак інциденту, або не повідомляє про підозрілі події через страх негативних наслідків або невпевненість у правильності своїх підозр. Враховуючи це, ефективне навчання з цієї теми має не лише пояснювати процедуру звітування, а й формувати культуру безпеки, у якій своєчасне повідомлення про інцидент сприймається як позитивна поведінка, а не як визнання помилки.

Методи та формати реалізації програм обізнаності суттєво впливають на їхню результативність. Електронне навчання (e-learning) є найбільш поширеним форматом завдяки масштабованості та можливості стандартизації змісту, проте у форматі тривалих обов'язкових модулів воно нерідко сприймається персоналом як бюрократична формальність, що мінімізує реальне засвоєння матеріалу. Мікронавчання являє собою короткі, сфокусовані навчальні модулі тривалістю

3–5 хвилин на одну конкретну тему, що демонструє вищу ефективність із точки зору засвоєння та утримання знань і краще інтегрується у щоденний робочий ритм персоналу.

Симульовані фішингові кампанії є практичним інструментом оцінювання реальної сприйнятливості персоналу до фішингових атак та одночасно ефективним навчальним механізмом. Методологія проведення симуляцій передбачає надсилання тестових фішингових повідомлень без попередження персоналу, відстеження реакції — кількості кліків за посиланнями, введених облікових даних, повідомлень про підозрілі листи, а також надання негайного навчального зворотного зв'язку тим, хто виявив сприйнятливість. Результати симуляцій слугують кількісним показником ефективності програми обізнаності та дозволяють ідентифікувати підрозділи або категорії персоналу, що потребують додаткового навчання [3, 27].

Гейміфікація та інтерактивні формати навчання набувають поширення як засіб підвищення залученості персоналу до програм обізнаності. Симуляції сценаріїв інцидентів, змагання Capture the Flag та рейтинги підрозділів підвищують залученість персоналу. Такі методи формують позитивну мотивацію до навчання, на відміну від традиційного проходження обов'язкових модулів. Очна взаємодія у форматі воркшопів, рольових ігор та розбору реальних кейсів є незамінною для формування поведінкових навичок — особливо у контексті навчання розпізнаванню соціальної інженерії, де відпрацювання практичних реакцій є більш ефективним, ніж теоретичне вивчення ознак маніпуляції.

Формування компетентності персоналу, відповідального за функціонування СМІБ, є окремим і більш складним завданням порівняно з підвищенням загальної обізнаності. Особи, що виконують функціональні ролі у рамках СМІБ це спеціалісти з інформаційної безпеки, аналітики SOC, аудитори, власники ризиків, — потребують глибоких фахових знань та практичних навичок, здобуття яких вимагає системного підходу до розвитку компетентності. Організації використовують кілька механізмів формування компетентності:

зовнішнє навчання та здобуття галузевих сертифікацій, внутрішнє навчання силами досвідчених фахівців, участь у конференціях та галузевих заходах, а також практичне навчання на робочому місці під керівництвом наставника.

Галузеві сертифікації є визнаним механізмом підтвердження компетентності у сфері інформаційної безпеки. Сертифікація CISSP (Certified Information Systems Security Professional) від (ISC)² є широко визнаним підтвердженням компетентності у сфері управління інформаційною безпекою. CISM (Certified Information Security Manager) від ISACA орієнтована на управлінський аспект інформаційної безпеки. ISO/IEC 27001 Lead Implementer та Lead Auditor є спеціалізованими сертифікаціями, безпосередньо пов'язаними з впровадженням та аудитом СМІБ. Для технічних фахівців актуальними є сертифікації у сфері тестування на проникнення, таких як CEH та OSCP, а також у сферах аналізу захищеності хмарних середовищ і криміналістики [28].

Вимірювання результативності програм навчання та обізнаності є обов'язковою умовою їх вдосконалення та обґрунтування інвестицій перед керівництвом. Модель Кіркпатріка, широко застосовувана для оцінювання навчальних програм, передбачає чотири рівні оцінювання: реакція учасників на навчання, рівень засвоєння знань, зміна поведінки на робочому місці та вплив на бізнес-результати. На практиці більшість організацій обмежуються опитуваннями та тестами. Однак з точки зору ризик-менеджменту важливішими є третій і четвертий рівні оцінювання, що аналізують реальні зміни в поведінці та їхній вплив на загальну безпеку.

Кількісні показники результативності програм обізнаності включають відсоток персоналу, що пройшов навчання у встановлені терміни; результати тестувань знань до та після навчання; динаміку частки кліків за посиланнями у симульованих фішингових кампаніях; кількість повідомлень персоналу про підозрілі події та частку підтверджених реальних загроз серед них; кількість інцидентів, спричинених людськими помилками, у динаміці. Якісні показники охоплюють оцінку змін у культурі безпеки через опитування персоналу,

результати спостережень за дотриманням процедур безпеки на робочих місцях, а також оцінку компетентності ключових ролей СМІБ через практичні вправи та аудит документації.

Формування культури безпеки є стратегічною метою управління людським фактором, що виходить за межі окремих навчальних заходів. Культура безпеки визначається як сукупність цінностей, переконань та поведінкових норм, що визначають ставлення персоналу до питань інформаційної безпеки у щоденній діяльності. Організація з розвиненою культурою безпеки характеризується тим, що персонал дотримується вимог безпеки не через страх покарання, а через розуміння їхньої доцільності та особисту відповідальність за захист інформаційних активів. Формування такої культури вимагає послідовних зусиль протягом тривалого часу, демонстрації лідерства з боку керівництва, відкритої комунікації щодо інцидентів та уроків з них, а також визнання та заохочення відповідальної поведінки персоналу у сфері безпеки.

2.3 Методи моніторингу, вимірювання та оцінювання результативності СМІБ

Моніторинг, вимірювання та оцінювання результативності виступає механізмом, що перетворює СМІБ із статичного набору задокументованих процедур на динамічну управлінську систему, здатну адаптуватися до змін у ландшафті загроз і внутрішньому середовищі організації. Без систематичного збору та аналізу даних про функціонування системи керівництво організації позбавлене об'єктивної інформації для прийняття обґрунтованих рішень щодо пріоритетів безпеки, розподілу ресурсів та напрямів вдосконалення. Саме тому розділ 9 стандарту ISO/IEC 27001:2022 присвячений виключно оцінюванню результативності і охоплює три взаємопов'язані механізми: моніторинг і вимірювання, внутрішній аудит та аналіз з боку керівництва.

Концептуальною основою вимірювання результативності СМІБ є принцип, відомий у менеджменті як «що вимірюється — тим управляється». Організації, що не мають формалізованої системи метрик інформаційної безпеки, фактично управляють системою наосліп — рішення приймаються на основі суб'єктивних відчуттів або реакції на вже реалізовані інциденти, а не на підставі аналізу тенденцій та об'єктивних показників. Відсутність вимірюваних метрик також унеможливлює демонстрацію цінності СМІБ для вищого керівництва та обґрунтування бюджетних запитів на заходи безпеки — аргумент, що є особливо актуальним в умовах конкуренції за ресурси між функціями інформаційної безпеки та іншими бізнес-підрозділами.

Стандарт ISO/IEC 27004:2016 надає детальні методологічні настанови щодо побудови системи моніторингу та вимірювання результативності СМІБ. Відповідно до цього стандарту, процес вимірювання охоплює визначення об'єктів вимірювання — атрибутів процесів, заходів захисту або результатів СМІБ, що підлягають оцінюванню; вибір базових мір, що кількісно або якісно характеризують об'єкт вимірювання; визначення похідних мір, що отримуються шляхом комбінування базових; встановлення індикаторів — числових значень або діапазонів, що використовуються для прийняття рішень; а також визначення аналітичних результатів і механізму їх доведення до відповідних осіб [15].

Класифікація метрик інформаційної безпеки може здійснюватися за кількома підставами. За рівнем управління метрики поділяються на стратегічні, що характеризують загальний стан захищеності організації та використовуються вищим керівництвом; тактичні, що відображають результативність окремих програм та процесів СМІБ і використовуються менеджерами інформаційної безпеки; та операційні, що характеризують функціонування конкретних технічних засобів захисту і використовуються технічним персоналом. За типом вимірювання метрики поділяються на кількісні, що виражаються числовими значеннями, та якісні, що описують стан об'єкта через категоріальні шкали. За спрямованістю розрізняють випереджаючі метрики, що характеризують зусилля

з профілактики інцидентів, та запізнілі метрики, що відображають результати реалізованих подій.

Операційні метрики відображають поточний стан технічних засобів захисту та операційних процесів СМІБ. До типових операційних метрик належать: відсоток систем із актуальними патчами безпеки; середній час між виявленням вразливості та її усуненням у розбивці за рівнями критичності; кількість відкритих вразливостей критичного рівня в інфраструктурі; відсоток облікових записів із увімкненою багатофакторною автентифікацією; кількість заблокованих спроб несанкціонованого доступу; обсяг трафіку, відфільтрованого системами захисту від шкідливого програмного забезпечення. Ці показники характеризують ефективність реалізованих технічних заходів захисту і слугують операційним індикатором стану інфраструктури безпеки.

Метрики управління інцидентами є критично важливим компонентом системи вимірювання, оскільки безпосередньо характеризують здатність організації виявляти та реагувати на реалізовані загрози. Середній час виявлення інциденту (Mean Time to Detect, MTTD) відображає оперативність ідентифікації подій безпеки з моменту їх виникнення. Середній час реагування на інцидент (Mean Time to Respond, MTTR) характеризує швидкість локалізації та усунення наслідків інциденту після його виявлення. Кількість інцидентів у динаміці за класами та рівнями критичності дозволяє ідентифікувати тенденції та повторювані патерни, що вказують на системні вразливості. Відсоток інцидентів, що вийшли за межі первинного вектора атаки, характеризує ефективність заходів стримування [19, 27].

Метрики програм навчання та обізнаності відображають результативність заходів з управління людським фактором. Частка персоналу, що пройшов навчання у встановлені терміни, є базовим показником охоплення програми. Динаміка частки кліків за посиланнями у симульованих фішингових кампаніях є одним із найбільш об'єктивних показників реальної поведінкової сприйнятливості персоналу до соціоінженерних атак. Кількість повідомлень

персоналу про підозрілі події відображає рівень залученості співробітників у процес виявлення загроз. Результати тестувань знань до та після навчання характеризують засвоєння змісту навчальних програм. Відсоток інцидентів, причиною яких є людська помилка, у динаміці є запізнілою метрикою, що відображає сукупний вплив усіх заходів з управління людським фактором.

Стратегічні метрики забезпечують вище керівництво агрегованими даними для управлінських та інвестиційних рішень. До ключових показників належать: рівень зрілості СМІБ, частка контрольованих критичних ризиків, динаміка витрат на інциденти та відповідність регуляторним вимогам. Окремим важливим завданням є забезпечення адресності навчальних заходів, що потребує диференційованого підходу до різних груп працівників. Відповідну матрицю сегментації навчальних програм наведено в таблиці 2.1.

Таблиця 2.1

Сегментація навчальних програм з інформаційної безпеки за категоріями персоналу

Категорія персоналу	**Специфічні ризики та вектори загроз**	**Ключові теми навчання**	**Форма та періодичність**
Вище керівництво (Топ-менеджмент)	Цільовий фішинг (whaling), компрометація корпоративної пошти (BEC), соціальна інженерія	Стратегічні ризики ІБ, правова відповідальність, захист мобільних пристроїв та каналів зв'язку	Індивідуальний інструктаж, воркшопи (1 раз на рік)
Фінансовий відділ та бухгалтерія	Фішинг, шахрайство з платіжними документами, підробка рахунків контрагентів	Верифікація платежів, розпізнавання маніпуляцій, безпечна робота з банківським ПЗ	Мікронавчання, тести, симуляції фішингу (щоквартально)
IT-спеціалісти та розробники	Вразливості нульового дня, атаки на ланцюжок постачання, помилки конфігурації	Принципи безпечного кодування (OWASP), DevSecOps, безпечне адміністрування інфраструктури	Спеціалізовані курси, Capture the Flag (2 рази на рік)
Рядові операційні співробітники	Масовий фішинг, шкідливе ПЗ, втрата носіїв інформації, соціальна інженерія	Політика чистого стола, гігієна паролів, правила поводження з інформацією, звітування про інциденти	Електронні курси, регулярні фішингові симуляції (щомісячно)

Внутрішній аудит СМІБ є другим механізмом оцінювання результативності, закріпленим у розділі 9.2 стандарту ISO/IEC 27001:2022. На відміну від моніторингу та вимірювання, що забезпечують безперервний потік операційних даних, внутрішній аудит здійснюється за запланованими інтервалами і спрямований на системну перевірку відповідності СМІБ вимогам стандарту та власним вимогам організації. Стандарт встановлює обов'язкові вимоги до програми аудиту: вона має охоплювати частоту, методи, відповідальності та вимоги до планування та звітування з урахуванням важливості аудиторських процесів і результатів попередніх аудитів [16].

Принципи незалежності та об'єктивності є ключовими для забезпечення результативності внутрішнього аудиту. Стандарт вимагає, щоб аудитори не перевіряли власну роботу, однак не встановлює обов'язкової організаційної незалежності аудиторської функції від функції інформаційної безпеки. На практиці організації вирішують цю проблему по-різному: залучають аудиторів з інших підрозділів, ротують аудиторів між підрозділами, або використовують зовнішніх консультантів для доповнення внутрішніх аудиторських ресурсів. Компетентність аудиторів є не менш критичним фактором — аудитор, що не має глибокого розуміння вимог ISO/IEC 27001 та специфіки аудиторського процесу, не здатний виявити системні невідповідності та сформулювати змістовні спостереження.

Методологія проведення внутрішнього аудиту СМІБ структурується у кілька послідовних фаз. Підготовка аудиту охоплює визначення сфери та цілей аудиту, формування аудиторської групи, розробку плану аудиту та підготовку аудиторських контрольних списків на основі вимог стандарту та специфіки організації. Проведення аудиту включає збір аудиторських свідчень через вивчення документації, інтерв'ю з відповідальними особами та спостереження за операційними практиками. Формування аудиторського звіту передбачає класифікацію виявлених невідповідностей — на значущі та незначущі — та фіксацію спостережень і можливостей для вдосконалення. Моніторинг

виконання коригувальних дій забезпечує реальне усунення виявлених невідповідностей, а не їх формальне «закриття» у документації.

Типові невідповідності, що виявляються під час внутрішніх аудитів СМІБ, свідчать про системні слабкості, характерні для організацій на різних стадіях зрілості системи. Неактуальність реєстру інформаційних активів через відсутність процедури його регулярного перегляду є однією з найбільш поширених невідповідностей. Відсутність задокументованих свідчень проведення оцінювання ризиків або їх невідповідність фактичним обставинам організації є критичною невідповідністю, що безпосередньо впливає на обґрунтованість вибору заходів захисту. Недостатнє документування компетентності персоналу, відповідального за СМІБ, є поширеною проблемою, що виявляється у відсутності задокументованих свідчень навчання та підтвердження кваліфікації. Відсутність або неповнота декларації про застосовність є критичною невідповідністю, оскільки цей документ є обов'язковим і центральним для сертифікаційного аудиту.

Аналіз з боку керівництва є третім механізмом оцінювання результативності СМІБ відповідно до розділу 9.3 стандарту та є тим елементом системи, що забезпечує стратегічний погляд на її функціонування. Стандарт встановлює обов'язковий перелік вхідних даних для аналізу: статус виконання рішень попереднього аналізу; зміни у зовнішньому та внутрішньому контексті, релевантні для СМІБ; зворотний зв'язок щодо результативності інформаційної безпеки, включаючи тенденції у невідповідностях та коригувальних діях, результати моніторингу та вимірювання, результати аудитів та ступінь досягнення цілей інформаційної безпеки; зворотний зв'язок від зацікавлених сторін; результати оцінювання ризиків та статус плану обробки ризиків; а також можливості для постійного вдосконалення.

Практична результативність аналізу з боку керівництва залежить від якості підготовки вхідних даних та реальної залученості вищого керівництва. Формальне проведення аналізу без змістовного розгляду представлених даних та

прийняття конкретних рішень є поширеною проблемою, що перетворює цей важливий механізм на документаційну вправу. Ефективний аналіз з боку керівництва має завершуватися конкретними рішеннями щодо можливостей вдосконалення СМІБ, змін у ресурсному забезпеченні та перегляду цілей інформаційної безпеки — лише за цих умов він виконує свою функцію стратегічного управлінського механізму.

Технологічне забезпечення моніторингу та вимірювання результативності СМІБ охоплює широкий спектр інструментів. Системи управління інформацією та подіями безпеки (SIEM) є центральним технологічним компонентом оперативного моніторингу: вони збирають, нормалізують та кореллюють журнали подій із різнорідних джерел — мережевого обладнання, серверів, кінцевих точок, хмарних сервісів, — забезпечуючи виявлення аномалій та потенційних інцидентів у режимі реального часу. Платформи GRC (Governance, Risk and Compliance) забезпечують централізоване управління реєстром ризиків, планом обробки ризиків, програмою аудиту та метриками результативності, формуючи єдине середовище для управління СМІБ на тактичному рівні [24].

Інструменти автоматизованого сканування вразливостей забезпечують безперервний моніторинг технічного стану інфраструктури та постачають операційні дані для метрик управління вразливостями. Системи виявлення та реагування на кінцевих точках (EDR) та їх розширені варіанти (XDR) забезпечують моніторинг поведінки на рівні робочих станцій та серверів, виявляючи аномальну активність, що може свідчити про компрометацію. Платформи оркестрації, автоматизації та реагування на безпекові загрози (SOAR) автоматизують частину операцій реагування на інциденти, скорочуючи MTTR та звільняючи аналітиків для роботи зі складними інцидентами, що вимагають людського судження.

Звітність за результатами моніторингу та вимірювання є механізмом, що перетворює зібрані дані на управлінську інформацію, придатну для прийняття рішень. Ефективна система звітності передбачає диференційовані звіти для різних рівнів управління: операційні панелі у режимі реального часу для технічного персоналу SOC; щотижневі або щомісячні операційні звіти для менеджерів інформаційної безпеки; квартальні стратегічні звіти для вищого керівництва та членів наглядової ради. Зміст звіту для вищого керівництва має бути адаптований до бізнес-контексту. Ризики мають виражатися у фінансових та операційних термінах, зрозумілих особам, що не є фахівцями у сфері інформаційної безпеки. Трирівневу систему звітності за метриками СМІБ показано на рисунку 2.2.

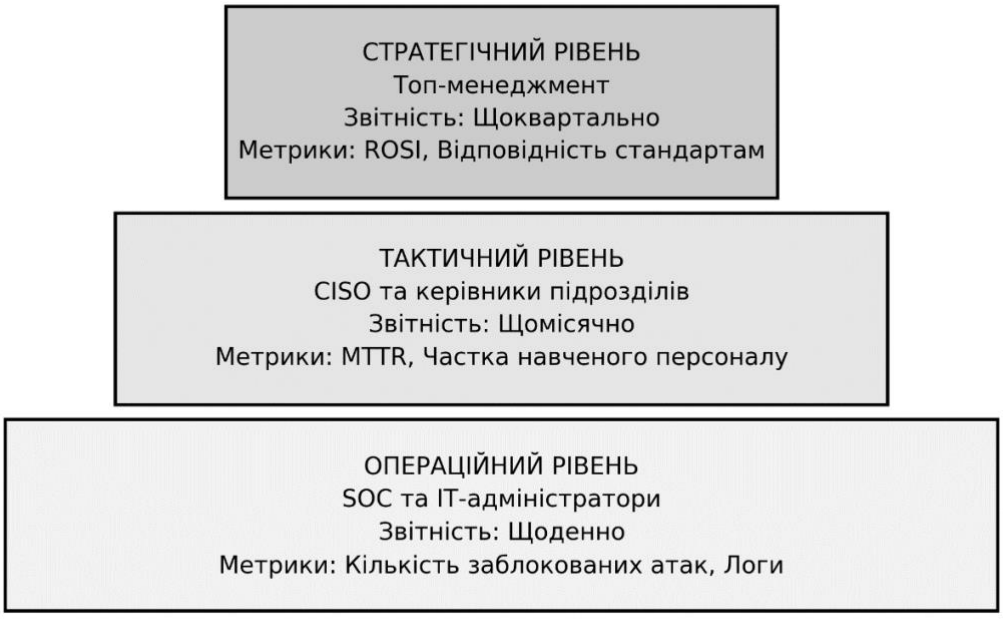

Рис. 2.2. Трирівнева система звітності за метриками СМІБ

Для подолання розриву між теорією та практикою систематизовано методи функціонування СМІБ і розроблено модель, представлену в таблиці 2.2. Ця модель демонструє зв'язок етапів PDCA з вимогами стандарту, інструментами та артефактами, виділяючи критичні процеси управління.

Таблиця 2.2

Систематизація методів забезпечення функціонування СМІБ у прив’язці до циклу PDCA

Етап PDCA	**Вимога або процес СМІБ за стандартом ISO/IEC 27001**	**Метод забезпечення**	**Інструмент реалізації**	**KPI або доказ виконання**
PLAN	Оцінювання ризиків згідно з пунктом 6.1.2	Ризик-орієнтований підхід	Матриця ризиків, системи класу GRC	% оброблених критичних ризиків (>95%)
PLAN	Встановлення цілей інформаційної безпеки за пунктом 6.2	Метод каскадування цілей	Balanced Scorecard (BSC)	Кількість інтегрованих бізнес-метрик (100%)
DO	Операційне управління відповідно до пункту 8.1	Управління вразливостями та конфігураціями	Автоматизовані сканери (Nessus, Qualys), EDR	Середній час закриття критичних вразливостей (<72 год)
DO	Забезпечення компетентності та обізнаності за пунктами 7.2 та 7.3	Управління людським фактором	LMS-платформи, гейміфікація, симуляції фішингу	Показник Click Rate при симуляціях фішингу (<5%)
DO	Управління інцидентами згідно з заходом 5.24 Додатка А	Модель реагування NIST (6 фаз)	Security Operations Center (SOC), SIEM-системи	Показники оперативності: MTTD < 2 год, MTTR < 4 год
CHECK	Моніторинг та вимірювання результативності за пунктом 9.1	Аналіз показників результативності	Операційні дашборди, стратегічні звіти	Досягнення цільового рівня зрілості доменів (>3.5)
CHECK	Проведення внутрішнього аудиту відповідно до пункту 9.2	Незалежна перевірка та спостереження	Чек-листи аудиту, інтерв'ю з персоналом	% закритих у строк аудиторських зауважень (>90%)
ACT	Постійне вдосконалення згідно з пунктами 10.1 та 10.2	Реалізація коригувальних дій	Метод «5 чому», діаграма Ішікави	% виконаних пунктів Дорожньої карти вчасно (>95%)

Висновки до розділу 2

У другому розділі досліджено методи забезпечення функціонування системи менеджменту інформаційної безпеки на операційному рівні. Встановлено, що операційна результативність СМІБ визначається не наявністю задокументованих процедур, а якістю їхньої практичної реалізації та взаємоузгодженістю процесів. Розрив між формальною відповідністю вимогам стандарту та реальною захищеністю організації виникає передусім на цьому рівні через неналежне виконання задокументованих процедур та відсутність механізмів своєчасного виявлення відхилень.

Систематизовано ключові операційні процеси СМІБ — управління активами, класифікацію інформації, контроль доступу, управління вразливостями, реагування на інциденти, забезпечення безперервності бізнесу та управління відносинами із постачальниками. Показано, що ці процеси утворюють єдину взаємозалежну систему: розрив у будь-якому з них ослаблює загальний рівень захищеності незалежно від якості окремих компонентів. Окремо встановлено, що управління вразливостями та управління доступом генерують найбільшу частку інцидентів при неналежному виконанні і потребують першочергової автоматизації.

Досліджено управління людським фактором як центральний, а не допоміжний напрям операційного забезпечення СМІБ. Здійснено принципове розмежування між поняттями обізнаності та компетентності відповідно до вимог стандарту ISO/IEC 27001:2022, що визначає адресність і зміст навчальних заходів для різних категорій персоналу. Встановлено, що ефективні програми підвищення обізнаності будуються на принципах безперервного навчання, сегментації цільових аудиторій та вимірювання реальних поведінкових змін. Стратегічною метою управління людським фактором визначено формування організаційної культури безпеки, за якої персонал дотримується вимог не внаслідок примусу, а через усвідомлення особистої відповідальності.

Проаналізовано методи моніторингу, вимірювання та оцінювання результативності СМІБ як механізму зворотного зв'язку, що охоплює три взаємодоповнюючі механізми: поточний моніторинг і вимірювання, внутрішній аудит та аналіз з боку керівництва. Обґрунтовано необхідність диференціації метрик за рівнями управління — операційними, тактичними та стратегічними, що забезпечує релевантність інформації для прийняття рішень на відповідному рівні організаційної ієрархії. Виявлено характерну проблему: більшість організацій має надлишок операційних метрик при майже повній відсутності стратегічних, що позбавляє вище керівництво інформації для обґрунтованих рішень щодо безпеки.

Результати другого розділу формують операційний каркас СМІБ та створюють методологічну основу для розробки практичного інструментарію моніторингу, оцінювання зрілості та внутрішнього аудиту, що є предметом дослідження третього розділу.

Розділ 3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ТА АУДИТ ФУНКЦІОНУВАННЯ СМІБ

Теоретико-методологічні засади функціонування СМІБ, досліджені у попередніх розділах, утворюють нормативну та концептуальну основу системи, однак самі по собі не гарантують її результативності в операційному середовищі конкретної організації. Практика впровадження СМІБ виявляє стійку закономірність: наявність задокументованих політик, затвердженого реєстру ризиків та отриманого сертифіката відповідності ISO/IEC 27001 не є достатньою умовою реального захисту інформаційних активів. Розрив між формальною відповідністю та фактичною результативністю виникає там, де система менеджменту існує переважно як документаційна конструкція, відірвана від операційних процесів організації та позбавлена механізмів об'єктивного вимірювання свого стану. Подолання цього розриву потребує трьох взаємопов'язаних практичних інструментів: формалізованої системи вимірювань у вигляді KPI, що трансформують абстрактні цілі безпеки у конкретні числові орієнтири; структурованої оцінки зрілості, що дозволяє виявити системні прогалини у розвитку окремих доменів; та внутрішнього аудиту як верифікаційного механізму, що підтверджує або спростовує відповідність задокументованих процедур реальній операційній практиці.

Логіка побудови третього розділу відтворює природну послідовність практичного управлінського циклу: від визначення того, що вимірюється і якими методами, — до оцінювання поточного стану системи — і далі до верифікації виявлених відхилень та розробки обґрунтованих рекомендацій. У підрозділі 3.1 формується система KPI для моніторингу функціонування СМІБ на прикладі модельної організації ТОВ «ТехКлауд». У підрозділі 3.2 на основі п'ятирівневої моделі зрілості оцінюється поточний стан розвитку ключових доменів СМІБ цієї організації. У підрозділі 3.3 результати оцінювання транслюються у ризик-

орієнтовану програму внутрішнього аудиту з формуванням конкретних висновків та практичних рекомендацій для керівництва.

3.1 Формування системи KPI для моніторингу функціонування СМІБ

Об'єктом практичної апробації у цьому підрозділі обрано модельну організацію ТОВ «ТехКлауд» — умовного постачальника послуг хмарного хостингу класу IaaS та PaaS, що одночасно провадить діяльність з розробки спеціалізованого програмного забезпечення для корпоративного сегменту. Вибір організації зазначеного профілю обумовлений специфічністю її ризик-середовища, що поєднує характеристики двох принципово різних операційних моделей: постачальника інфраструктурних послуг із договірними зобов'язаннями щодо безперервності та розробника програмного забезпечення з доступом до вихідного коду та виробничих середовищ клієнтів. Така комбінація формує один із найбільш складних з точки зору управління інформаційною безпекою контекстів і дозволяє продемонструвати методологію формування KPI у повному обсязі її аналітичного потенціалу.

Договірна архітектура ТОВ «ТехКлауд» побудована на угодах про рівень обслуговування, що гарантують клієнтам доступність інфраструктурних сервісів на рівні 99,9% на місяць — показник, що математично відповідає допустимому сукупному простою не більше 8,76 годин на рік. Будь-який інцидент інформаційної безпеки, що призводить до деградації або недоступності клієнтських середовищ понад встановлені пороги SLA, тягне за собою фінансові санкції у формі кредитів на рахунок клієнта, що безпосередньо впливає на фінансові результати компанії. Це встановлює пряму та вимірювану залежність між результативністю СМІБ та фінансовими показниками бізнесу — залежність, що є ключовим аргументом при обґрунтуванні інвестицій у заходи безпеки перед вищим керівництвом.

В рамках надання послуг IaaS та PaaS компанія обробляє та зберігає дані клієнтів у спільному або виділеному хмарному середовищі — персональні дані кінцевих користувачів клієнтських систем, фінансові транзакційні дані, дані систем управління підприємством. Компрометація цих даних генерує регуляторні ризики для самої компанії як оператора та субоператора персональних даних, а також репутаційні ризики, наслідки яких у довгостроковій перспективі суттєво перевищують безпосередні фінансові збитки. Підрозділ розробки програмного забезпечення додає до цього контексту специфічний вектор ризику: розробники мають розширені права доступу до репозиторіїв, CI/CD-пайплайнів та тестових середовищ, що містять реальні або знеособлені клієнтські дані. Компрометація облікових даних розробника через фішингову атаку або впровадження шкідливого коду у процес розробки є реалізованим сценарієм, що спостерігається у галузі та вимагає специфічних заходів контролю [36].

На момент ініціювання розробки системи KPI ТОВ «ТехКлауд» перебуває на стадії стрімкого організаційного та інфраструктурного масштабування. Чисельність персоналу подвоїлася протягом останніх вісімнадцяти місяців переважно за рахунок прийому інженерів-розробників та фахівців з хмарної інфраструктури. Кількість клієнтів зросла на 140%, що потягло за собою пропорційне розширення хмарної інфраструктури та збільшення кількості сторонніх підрядників і постачальників програмних компонентів. Наявна СМІБ компанії функціонує у реактивній моделі: заходи безпеки реалізуються переважно у відповідь на інциденти або вимоги клієнтів при укладанні договорів, а не як результат проактивного управління на основі даних. Відсутність формалізованих метрик результативності унеможливлює об'єктивну оцінку стану захищеності та обґрунтування управлінських рішень щодо розподілу ресурсів безпеки. Керівництво служби інформаційної безпеки не може кількісно відповісти на запитання вищого менеджменту щодо динаміки захищеності інфраструктури або порівняння поточного стану з галузевими орієнтирами —

ситуація, типова для технологічних компаній на стадії масштабування, де операційні пріоритети розвитку продукту системно витісняють інвестиції у зрілість управлінських процесів безпеки.

Перехід від реактивної до проактивної моделі управління потребує насамперед формування системи вимірювань, що забезпечить об'єктивну та регулярну інформацію про стан функціонування СМІБ. Стандарт ISO/IEC 27004:2016 встановлює методологічну основу для побудови таких систем вимірювань, визначаючи ієрархію від базових мір через похідні до індикаторів та аналітичних результатів. Однак сам по собі стандарт не визначає конкретний набір показників — він надає методологічну рамку, у межах якої організація проектує власну систему метрик відповідно до свого контексту, цілей та ризик-профілю [15, 39].

Для проектування системи KPI ТОВ «ТехКлауд» обрано методологічну основу адаптованої концепції збалансованої системи показників Balanced Scorecard, розробленої Р. Капланом та Д. Нортоном як інструмент трансляції стратегії організації у вимірювані операційні орієнтири. Вибір BSC обумовлений кількома принциповими перевагами у контексті завдань ТОВ «ТехКлауд».

По-перше, BSC структурно вирішує проблему розриву між функцією безпеки та бізнесом. Традиційні системи метрик зосереджені на технічних показниках — кількості вразливостей, часі реагування, охопленні патчами, — що є операційно значущими для технічного персоналу, проте не транслюються у мову бізнес-ризиків та фінансових наслідків, зрозумілу вищому керівництву. BSC примушує розглядати діяльність служби безпеки через чотири рівноправні перспективи, жодна з яких не є другорядною. По-друге, концепція BSC відповідає вимозі стандарту ISO/IEC 27001:2022 щодо узгодженості цілей інформаційної безпеки із загальними цілями організації, закріпленій у розділах 4.1 та 6.2. Для ТОВ «ТехКлауд» з її SLA-зобов'язаннями перед клієнтами ця узгодженість є операційною необхідністю: показники безпеки мають безпосередньо відображати здатність компанії виконувати договірні

зобов'язання. По-третє, чотиривимірна структура BSC природно відповідає різноманітності ризик-профілю організації [6].

Фінансова перспектива охоплює показники, що характеризують вартісний вимір інцидентів та ефективність інвестицій у безпеку. Центральним показником цієї перспективи є індекс окупності інвестицій у заходи безпеки (ROSI), що розраховується як відношення запобігнутих втрат — оціненої вартості інцидентів, яких вдалося уникнути завдяки реалізованим заходам, — до фактичних витрат на ці заходи. Позитивне значення ROSI є необхідним елементом обґрунтування бюджетних запитів служби безпеки перед фінансовим керівництвом компанії. Додатковим фінансовим показником є частка бюджету інформаційної безпеки у загальних витратах на IT — індикатор, що дозволяє порівнювати рівень інвестицій у безпеку з галузевими орієнтирами та відстежувати динаміку пріоритетів керівництва.

Перспектива зацікавлених сторін відображає виконання зобов'язань перед зовнішніми стейкхолдерами. Для ТОВ «ТехКлауд» ця перспектива охоплює два критичних показники: рівень відповідності вимогам ISO/IEC 27001 за результатами аудитів та відсоток постачальників і підрядників, охоплених аудитом безпеки. Встановлення цільового значення 100% для охоплення аудитом постачальників відображає специфіку хмарного провайдера, у якого субпідрядники є невід'ємною частиною ланцюжка надання послуги клієнту: вибіркова перевірка постачальників залишає неконтрольовані вектори ризику, що є неприйнятним у контексті договірних зобов'язань щодо захисту клієнтських даних.

Перспектива внутрішніх процесів є найбільш деталізованою та охоплює операційні показники чотирьох ключових процесів СМІБ. Управління інцидентами представлене показниками MTTD та MTTR, безпосередньо пов'язаними із SLA-зобов'язаннями: цільове значення MTTR менше 4 годин виводиться з максимально допустимого часу деградації сервісу, що зафіксований у типових клієнтських договорах. Управління вразливостями характеризується

показником своєчасності усунення критичних вразливостей — цільове значення 95% для вразливостей із рейтингом CVSS ≥ 9.0 протягом 72 годин відображає галузевий стандарт для хмарних провайдерів, що обробляють клієнтські дані. Управління доступом представлене показником швидкості блокування облікових записів звільнених осіб — цільове значення менше 1 години унеможливлює використання активних облікових даних після припинення трудових відносин.

Перспектива навчання та розвитку охоплює показники людського капіталу безпеки: охоплення персоналу навчанням на рівні не менше 98% штату на рік та стійкість до фішингу, що вимірюється відсотком кліків у симульованих кампаніях. Цільове значення Click Rate менше 5% відображає підвищену роль людського фактора в середовищі розробки — розробники мають розширені права доступу, а їхня компрометація через фішинг може призвести до впровадження шкідливого коду безпосередньо у програмні продукти, що постачаються клієнтам.

Встановлення цільових значень здійснювалося за комбінованим підходом, що поєднує галузевий бенчмаркінг, базове вимірювання поточного стану та зворотне обчислення від допустимого рівня ризику. Принциповою вимогою до системи є операційна реалізованість: кожен показник має автоматизоване джерело даних та метод верифікації, що не залежить від суб'єктивних оцінок виконавця. Показники, для розрахунку яких потрібне ручне агрегування даних із несумісних систем, до системи не включалися — такі показники на практиці або не відстежуються регулярно, або відображають неактуальний стан через затримки у консолідації даних. Розроблену комплексну збалансовану систему показників із зазначенням категорії перспективи BSC, найменування KPI, джерела даних та методу оцінювання, а також цільових значень для ТОВ «ТехКлауд» зведено у Таблиці 3.1.

Таблиця 3.1

Ключові показники ефективності (KPI) функціонування СМІБ

Категорія (Перспектива)	**Найменування показника (KPI)**	**Джерело даних / Метод оцінювання**	**Цільове значення**
Фінансова	Індекс окупності інвестицій (ROSI)	(Запобігнуті збитки - Витрати) / Витрати	> 0%
	Частка ІБ-бюджету від витрат на ІТ	Фінансові звіти ІТ-департаменту	7% - 12%
Зацікавлені сторони	Рівень відповідності нормам ISO 27001	Звіти внутрішніх та зовнішніх аудитів	100% відповідність
	Охоплення аудитом постачальників	Реєстр критичних контрагентів	100% перевірено
Внутрішні процеси	Середній час виявлення атак (MTTD)	Логи та інциденти в SIEM-системі	< 2 годин
	Середній час ліквідації інцидентів (MTTR)	Час локалізації загрози за SLA	< 4 годин
	Вчасність усунення вразливостей (CVSS ≥ 9.0)	Сканер вразливостей (Tenable/Nessus)	≥ 95% за 72 год.
	Швидкість блокування звільнених осіб	Логи Active Directory (AD)	< 1 години
Навчання та розвиток	Охоплення персоналу навчанням з ІБ	Платформа навчання (LMS)	≥ 98% штату на рік
	Стійкість до фішингу (Click Rate)	Результати симульованих атак	< 5% кліків

Сформована у Таблиці 3.1 система KPI відображає специфіку операційної моделі ТОВ «ТехКлауд» як постачальника послуг хмарного хостингу та розробника програмного забезпечення. Бізнес-модель компанії характеризується двома визначальними рисами з точки зору управління інформаційною безпекою: безперервністю надання послуг як ключовою договірною зобов'язальністю перед клієнтами та концентрацією клієнтських даних у хмарному середовищі, що підвищує привабливість організації як цілі для зловмисників і збільшує потенційні наслідки реалізації загроз. Саме ці характеристики визначили логіку встановлення цільових значень для кожної групи KPI.

Цільове значення MTTR на рівні менше 4 годин обумовлене не галузевою нормою, а прямими договірними зобов'язаннями компанії перед клієнтами. Типові SLA-угоди для IaaS/PaaS-постачальників передбачають гарантований рівень доступності 99,9% на місяць, що математично відповідає допустимому

простою не більше 8,76 годин на рік. Компрометація інфраструктурного вузла, що залишається нелокалізованою понад 4 години, з високою ймовірністю спричинить порушення гарантованого рівня доступності, що тягне за собою фінансові санкції та репутаційні збитки, що суттєво перевищують витрати на підтримку відповідного рівня оперативності команди реагування. Аналогічна логіка визначає вимогу 100-відсоткового охоплення аудитом постачальників: в архітектурі хмарних послуг субпідрядники є невід'ємними елементами ланцюжка надання послуги клієнту, і компрометація будь-якого з них є прямим вектором атаки на інфраструктуру компанії та клієнтські дані. Цільовий показник Click Rate менше 5% відображає підвищену роль людського фактора в середовищі розробки: розробники мають розширені права доступу до репозиторіїв та виробничих середовищ, а компрометація їхніх облікових даних може призвести до впровадження шкідливого коду безпосередньо у продукти, що постачаються клієнтам.

Архітектура збору даних для розрахунку встановлених KPI базується на інтеграції кількох технологічних компонентів. Центральним є SIEM-система — у конфігурації ТОВ «ТехКлауд» це може бути Splunk, IBM QRadar або Microsoft Sentinel, — що здійснює збір, нормалізацію та кореляцію подій безпеки з усіх компонентів інфраструктури в режимі реального часу. На основі даних SIEM розраховуються показники MTTD та MTTR: система фіксує часову мітку першої події, що свідчить про інцидент, та часову мітку його закриття, забезпечуючи автоматизований розрахунок обох показників без ручного втручання. Управління вразливостями реалізується через платформу Tenable або Nessus, що виконує безперервне сканування інфраструктури із класифікацією виявлених вразливостей за шкалою CVSS. Інтеграція сканера з системою управління завданнями забезпечує автоматичне створення тікетів для кожної критичної вразливості та відстеження термінів їх усунення. Журнали Active Directory є джерелом даних для KPI управління доступом: автоматизовані скрипти або модулі Identity Governance платформи виявляють облікові записи, що

перевищують встановлений термін після деактивації, та формують відповідні звіти. LMS-платформа фіксує факти проходження навчальних модулів персоналом, а результати симульованих фішингових кампаній через платформи типу KnowBe4 або Proofpoint постачають дані для розрахунку показника Click Rate.

Модель звітування за KPI реалізована як трирівнева ієрархічна структура. На оперативному рівні SOC-команда використовує інтерактивні дашборди у режимі реального часу, що відображають поточний статус критичних KPI: кількість відкритих інцидентів із розподілом за рівнями критичності, поточне значення MTTR за останні 24 години, кількість критичних вразливостей без призначеного виконавця. Відхилення від порогових значень відображаються як автоматичні сповіщення без потреби у ручному формуванні звіту. На тактичному рівні CISO отримує щомісячний аналітичний звіт із динамікою всіх KPI у порівнянні з попереднім звітним періодом, аналізом відхилень та їх причин, статусом виконання плану обробки ризиків і результатами завершених аудиторських перевірок. На стратегічному рівні топ-менеджмент отримує квартальний звіт, у якому KPI транслюються у бізнес-терміни: вартість реагування на інциденти у динаміці, рівень відповідності SLA-зобов'язанням у сфері безпеки, ризики, що можуть вплинути на договірні зобов'язання перед клієнтами.

Процедура ескалації при невиконанні KPI є формалізованим триступеневим алгоритмом управлінських дій. При падінні показника усунення критичних вразливостей нижче цільового значення 95% протягом звітного тижня автоматична система моніторингу генерує сповіщення для відповідального інженера та керівника технічного підрозділу із переліком конкретних невиконаних завдань і термінів прострочення. Якщо показник не відновлюється до цільового значення протягом наступних 72 годин, ескалація відбувається на рівень CISO, який ініціює нараду для встановлення причин відхилення та визначення коригувальних дій із відповідальними особами і термінами. При

повторному невиконанні протягом двох послідовних звітних періодів питання виноситься на рівень аналізу з боку керівництва відповідно до вимог розділу 9.3 стандарту ISO/IEC 27001:2022 [6].

Для показників, пов'язаних із договірними зобов'язаннями перед клієнтами — зокрема MTTR та доступності систем, — другий рівень ескалації активується вже через 2 години від моменту виявлення відхилення, а не через 72 години, що відображає критичність цих показників для бізнес-моделі ТОВ «ТехКлауд».

3.2 Оцінювання рівня зрілості функціонування СМІБ

Оцінювання рівня зрілості операційних процесів СМІБ модельної організації здійснено із застосуванням п'ятирівневої шкали (від початкового до оптимізованого рівня), адаптованої до вимог стандарту ISO/IEC 27001:2022 [12, 20]. На відміну від аудиту відповідності, що фіксує бінарний стан виконання вимог, оцінювання зрілості дозволило ідентифікувати фактичну здатність ТОВ «ТехКлауд» до відтворення процесів управління інформаційною безпекою, їх вимірювання та постійного вдосконалення. Діагностична процедура охоплювала документарний аналіз корпоративних політик, серію структурованих інтерв'ю з власниками бізнес-процесів (зокрема з керівником відділу розробки та директором з персоналу), а також вибіркову технічну верифікацію налаштувань хмарної інфраструктури. Візуалізований профіль зрілості базових доменів системи управління інформаційною безпекою ТОВ «ТехКлауд», сформований за результатами комплексного оцінювання, представлено на рисунку 3.1.

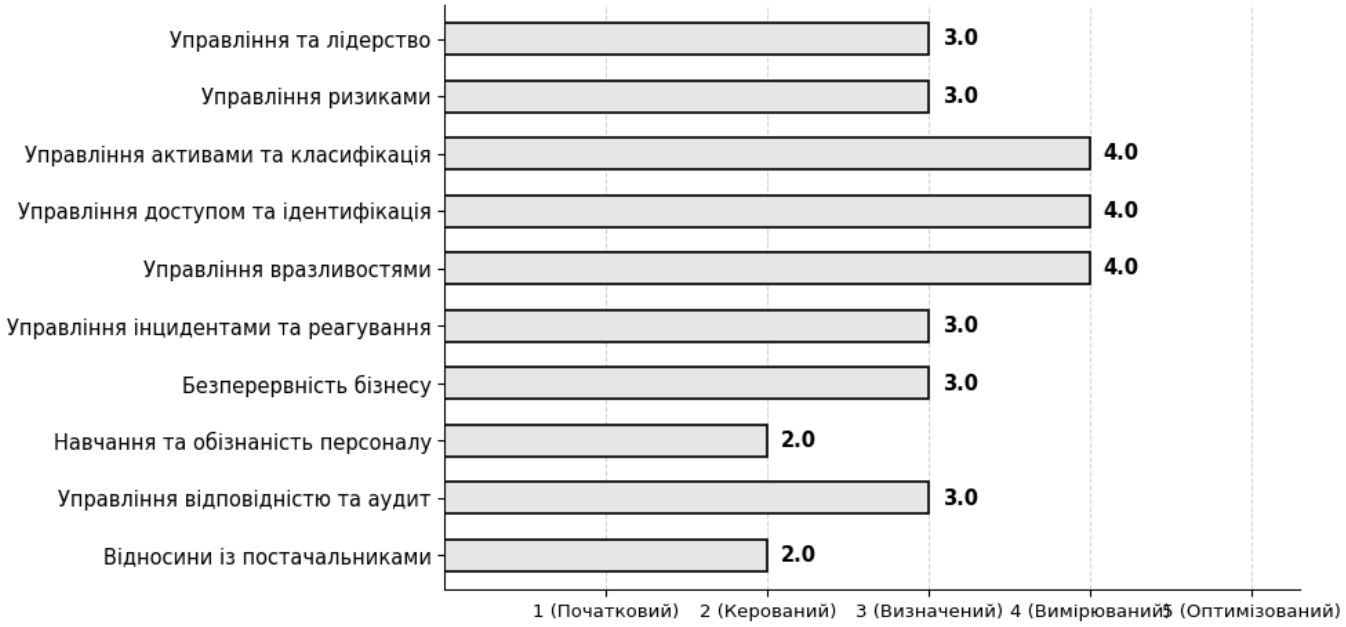

Рис. 3.1. Профіль зрілості процесів СМІБ за доменами

Профіль зрілості СМІБ ТОВ «ТехКлауд», відображений на Рисунку 3.1, демонструє характерну для технологічних компаній на стадії активного зростання асиметрію: технічні домени, що є безпосереднім середовищем операційної діяльності інженерних команд, досягли четвертого рівня зрілості, тоді як організаційні та управлінські домени зафіксовані на третьому рівні, а домени, що потребують системної роботи з персоналом та зовнішніми сторонами, — лише на другому. Така конфігурація профілю є не випадковою, а закономірно відображає пріоритети розвитку організації, у якій інвестиції в технічну інфраструктуру безпеки традиційно випереджають розвиток організаційних практик управління.

Домени «Управління вразливостями» та «Управління доступом» отримали оцінку 4.0, що відповідає вимірюваному рівню зрілості, на якому процеси не лише стандартизовані та документовані, а й систематично вимірюються із застосуванням кількісних метрик для прийняття управлінських рішень. Досягнення цього рівня у зазначених доменах пояснюється безпосередньою технологічною природою відповідних процесів: обидва реалізуються переважно

автоматизованими засобами, що за своєю суттю генерують вимірювані дані як побічний продукт своєї операційної роботи.

У домені управління вразливостями ТОВ «ТехКлауд» впроваджено безперервне автоматизоване сканування всієї хмарної інфраструктури засобами платформи Tenable.io, що забезпечує щоденне оновлення реєстру вразливостей із класифікацією за шкалою CVSS та автоматичним пріоритизуванням за рівнем критичності. Інтеграція платформи управління вразливостями з системою відстеження завдань забезпечує автоматичне створення тікетів, призначення виконавців та моніторинг дотримання встановлених SLA з усунення — 24 години для критичних вразливостей, 72 години для вразливостей високого рівня. Саме наявність автоматизованого вимірювання відсотка вразливостей, усунутих у межах SLA, та автоматичної ескалації при порушенні термінів відрізняє четвертий рівень зрілості від третього, на якому аналогічні процеси існують, але вимагають ручного моніторингу та реагування.

Домен управління доступом досяг четвертого рівня зрілості завдяки впровадженню повноцінної IAM-архітектури на основі рольової моделі доступу (RBAC). Усі права доступу до виробничих середовищ, репозиторіїв вихідного коду та клієнтських даних визначаються виключно через формалізовані ролі, прив'язані до функціональних обов'язків, а не призначаються індивідуально. Платформа управління ідентифікацією здійснює автоматичний моніторинг відхилень від затверджених рольових матриць, фіксує надлишкові права доступу та генерує регулярні звіти для рецертифікації. Квартальна рецертифікація прав доступу є формалізованим процесом із задокументованими результатами, що підтверджують власники відповідних бізнес-процесів. Багатофакторна автентифікація охоплює 100% привілейованих облікових записів та 96% облікових записів звичайних користувачів, що підтверджується автоматичними звітами платформи ідентифікації [11].

Домени «Управління ризиками», «Управління інцидентами» та «Безперервність бізнесу» зафіксовані на третьому рівні зрілості — визначеному

або стандартизованому, — що відповідає наявності задокументованих, послідовно виконуваних процесів у масштабах усієї організації, однак без систематичного кількісного вимірювання їхньої результативності. Визначальною характеристикою третього рівня є залежність якості виконання процесів від компетентності конкретних виконавців, а не від автоматизованих механізмів контролю.

У домені управління ризиками ТОВ «ТехКлауд» підтримує актуальний реєстр ризиків, що охоплює всі ідентифіковані ризики інформаційної безпеки з визначеними власниками, планами обробки та термінами реалізації заходів. Методологія оцінювання ризиків є задокументованою та послідовно застосовується при проведенні планових та позапланових оцінювань. Однак реєстр ризиків ведеться у табличному форматі без застосування спеціалізованої GRC-платформи, що обмежує можливості кореляції ризиків між доменами, автоматичного відстеження змін у ризик-профілі при зміні зовнішнього середовища та формування аналітичної звітності для вищого керівництва. Відсутність автоматизованого зв'язку між реєстром ризиків та оперативними даними про вразливості й інциденти означає, що актуалізація оцінок ризиків залежить від ініціативи відповідального персоналу, а не від автоматичних тригерів.

Домен управління інцидентами відповідає третьому рівню зрілості: процедури виявлення, класифікації, реагування та аналізу після інциденту є задокументованими та дотримуються командою SOC. Проте відсутня формалізована система метрик результативності процесу реагування — MTTD та MTTR розраховуються ситуативно для значущих інцидентів, а не систематично для всіх зареєстрованих подій. Аналіз після інциденту проводиться, однак не має стандартизованого формату, що ускладнює агрегування уроків та виявлення системних тенденцій у динаміці. Домен безперервності бізнесу характеризується наявністю задокументованих планів забезпечення безперервності ІКТ та відновлення після катастроф, що тестуються

на річній основі. Обмеженням третього рівня є те, що результати тестувань не транслюються у вимірювані метрики готовності — цільовий час відновлення (RTO) та цільова точка відновлення (RPO) визначені, проте їх фактичне досягнення під час тестувань не фіксується у стандартизованій звітності.

Домени «Навчання та обізнаність персоналу» та «Відносини із постачальниками» отримали оцінку 2.0, що відповідає керованому рівню зрілості, на якому базові практики існують, але реалізуються нерегулярно, залежать від ситуативних ініціатив і не охоплюють усіх релевантних об'єктів управління. Для ТОВ «ТехКлауд» низький рівень зрілості цих доменів є наслідком конкретних операційних обставин, що формують структурні перешкоди для їх розвитку.

Домен навчання та обізнаності персоналу перебуває на другому рівні зрілості внаслідок екстенсивного зростання чисельності персоналу, що є характерною ознакою технологічних компаній на стадії масштабування. Темп найму нових співробітників — переважно розробників та інженерів хмарної інфраструктури — суттєво перевищує пропускну здатність наявної програми вступного інструктажу з інформаційної безпеки, що реалізується у форматі очного або синхронного навчання. За фіксованих ресурсів служби інформаційної безпеки результатом є накопичення черги нових співробітників, що приступили до виконання обов'язків до проходження базового навчання. За даними останньої симульованої фішингової кампанії, рівень кліків за підозрілими посиланнями серед співробітників зі стажем до шести місяців утричі перевищує аналогічний показник для персоналу з більшим терміном роботи в компанії, що наочно відображає вплив прогалини у вступному навчанні. Відсутня також формалізована програма безперервного навчання для діючого персоналу — навчальні заходи проводяться реактивно після значущих інцидентів або при зміні регуляторних вимог, а не за затвердженим річним планом. LMS-платформа для управління навчанням впроваджена, проте її функціонал використовується неповною мірою: автоматичне призначення навчальних модулів новим

співробітникам не налаштоване, що унеможливлює системне відстеження охоплення.

Домен відносин із постачальниками зафіксований на другому рівні зрілості через системну прогалину у практиках оцінювання безпеки сторонніх постачальників програмного забезпечення та SaaS-рішень. ТОВ «ТехКлауд» активно використовує широкий спектр хмарних SaaS-платформ для забезпечення операційної діяльності — системи управління проектами, комунікаційні платформи, інструменти розробки та моніторингу. При підключенні нових SaaS-рішень відсутня стандартизована процедура оцінювання їхньої безпеки до початку використання: рішення про впровадження приймаються функціональними підрозділами на основі операційної доцільності без обов'язкового погодження зі службою інформаційної безпеки. Реєстр SaaS-рішень, що використовуються в організації, є неповним — явище тіньових IT фіксується при аналізі мережевого трафіку, однак систематичної процедури інвентаризації та категоризації сторонніх сервісів за рівнем критичності не впроваджено. Наявні договори з постачальниками не містять стандартизованих вимог щодо інформаційної безпеки та права проведення аудиту, що унеможливлює верифікацію заявлених постачальниками рівнів захисту.

Виявлена дисперсія балів між доменами — від 2.0 до 4.0 — безпосередньо визначає архітектуру програми внутрішнього аудиту, що описується у підрозділі 3.3. Відповідно до ризик-орієнтованого підходу до планування аудитів, закріпленого у стандарті ISO/IEC 27007:2020, домени з нижчими рівнями зрілості та вищою значущістю для ризик-профілю організації мають отримувати пріоритет в аудиторській програмі [35]. Домени «Навчання та обізнаність персоналу» та «Відносини із постачальниками» поєднують низький рівень зрілості з критичною значущістю для хмарного провайдера — перший є провідним вектором первинного проникнення, другий визначає рівень ризику ланцюжка постачання. Це обумовлює їх включення до першочергових об'єктів аудиторської перевірки з підвищеною інтенсивністю та глибиною дослідження.

Домени четвертого рівня зрілості, навпаки, можуть охоплюватися аудитами з меншою частотою та у вибірковому форматі, що дозволяє оптимально розподілити обмежені аудиторські ресурси організації.

3.3 Внутрішній аудит СМІБ та розробка рекомендацій щодо її вдосконалення

За результатами оцінювання рівня зрілості СМІБ, проведеного у підрозділі 3.2, програму внутрішнього аудиту ТОВ «ТехКлауд» сформовано відповідно до ризик-орієнтованого підходу, закріпленого у стандарті ISO/IEC 27007:2020. Аудиторські ресурси сконцентровано на доменах із найнижчими показниками зрілості та найвищою значущістю для ризик-профілю хмарного провайдера [9]. Першочерговими об'єктами аудиту визначено домени «Навчання та обізнаність персоналу» та «Відносини із постачальниками», що отримали оцінку зрілості 2.0 (керований рівень, на якому базові практики існують, але реалізуються нерегулярно та не охоплюють усіх релевантних об'єктів управління). Додатково до програми включено цільову контрольну перевірку домену управління доступом з метою верифікації актуальності облікових записів в умовах інтенсивного найму та звільнення персоналу, що є системним ризиком для компаній на стадії активного масштабування чисельності.

Підготовка аудиту охоплювала формування аудиторської групи у складі двох внутрішніх аудиторів, що не залучені до безпосередньої реалізації перевірюваних процесів, розробку плану аудиту з визначенням сфери, цілей та критеріїв перевірки, а також підготовку чек-листа на основі вимог стандарту ISO/IEC 27001:2022 та відповідних заходів захисту ISO/IEC 27002:2022. Критеріями аудиту визначено вимоги стандарту ISO/IEC 27001:2022, внутрішні політики та процедури ТОВ «ТехКлауд», а також договірні зобов'язання компанії перед клієнтами щодо захисту їхніх даних. Збір аудиторських доказів здійснювався через три взаємодоповнюючі методи: вивчення документації

(договорів із постачальниками, реєстру SaaS-рішень, LMS-звітів про проходження навчання, внутрішніх політик); структуровані інтерв'ю з HR-менеджером, CISO, власниками бізнес-процесів та трьома розробниками зі стажем до трьох місяців; технічну перевірку (вивантаження з Active Directory облікових записів із датою останньої активності та зіставлення з реєстром звільнених співробітників HR-системи, а також аналіз мережевого трафіку для ідентифікації несанкціонованих SaaS-підключень).Фрагмент чек-листа цільового внутрішнього аудиту із зафіксованими результатами наведено у таблиці 3.2.

Таблиця 3.2

Фрагмент чек-листа цільового внутрішнього аудиту СМІБ ТОВ «ТехКлауд»

Вимога стандарту	**Об'єкт перевірки**	**Метод збору доказів**	**Результат перевірки та фіксація невідповідностей**
ISO/IEC 27001, п. 7.2, 7.3	Проходження вступного навчання новими співробітниками до отримання доступу до систем.	LMS-звіт; зіставлення з HR-даними; інтерв'ю.	Значуща невідповідність. 19 з 34 нових співробітників (56%) отримали доступ до систем до завершення навчання. Середня затримка — 23 робочі дні. LMS не інтегрована з HR-системою.
ISO/IEC 27002, п. 5.19, 5.20	Наявність вимог безпеки у договорах із SaaS-постачальниками.	Аналіз 12 договорів; інтерв'ю з юридичним відділом.	Значуща невідповідність. Жоден із 12 договорів не містить вимог з ІБ, права аудиту або зобов'язань щодо повідомлення про інциденти.
ISO/IEC 27002, п. 5.15, 5.16	Своєчасність деактивації облікових записів звільнених співробітників.	Вивантаження AD; зіставлення з HR-реєстром звільнених.	Значуща невідповідність. 7 активних облікових записів співробітників, звільнених 12–47 днів тому. Для 2 з них зафіксовано спроби автентифікації після звільнення.
ISO/IEC 27001, п. 7.3; ISO/IEC 27002, п. 6.3	Наявність річного плану навчання та регулярних симуляцій фішингу.	Аналіз документації програми навчання; LMS-звіти.	Спостереження. Річний план навчання відсутній. Навчання проводилося двічі — реактивно після інцидентів. Симульовані фішингові кампанії не проводилися.
ISO/IEC 27002, п. 5.21, 5.22	Процедура оцінювання безпеки нових SaaS до початку використання.	Інтерв'ю з менеджерами закупівель; аналіз листування щодо 6 нових SaaS.	Значуща невідповідність. Жодне з 6 нових рішень не проходило оцінювання безпеки. У реєстрі відсутні 8 активних сервісів, виявлених через аналіз трафіку.

Сукупність виявлених невідповідностей підтверджує системний, а не випадковий характер проблем у двох аудиторських доменах. Чотири із п'яти зафіксованих позицій кваліфіковано як значущі невідповідності — відхилення від обов'язкових вимог стандарту, що суттєво впливають на результативність СМІБ та потребують розробки коригувальних дій із встановленими термінами та відповідальними особами [18]. Особливої уваги заслуговує виявлення активних облікових записів двох звільнених співробітників із зафіксованими спробами автентифікації: ця невідповідність виходить за межі суто нормативного порушення і є свідченням реального ризику несанкціонованого доступу, що потребує негайного реагування незалежно від формального аудиторського циклу.

Аналіз кореневих причин проведено для значущої невідповідності щодо відсутності вступного навчання для нових співробітників — як найбільш системної та такої, що має найширший вплив на ризик-профіль організації. Метод «5 чому» застосовано відповідно до методологічних рекомендацій щодо аналізу причин у контексті управління невідповідностями систем менеджменту [18].

1. Чому 56% нових співробітників отримали доступ до виробничих систем до завершення вступного навчання? Тому що адміністратор служби інформаційної безпеки призначає навчальний модуль у LMS вручну після отримання повідомлення від HR-відділу, і цей крок регулярно відкладається через завантаженість іншими операційними завданнями;

2. Чому призначення навчання залежить від ручної дії адміністратора? Тому що LMS-платформа не інтегрована з HR-системою та не отримує автоматичних подій про появу нових співробітників — відсутній API-зв'язок або механізм автоматичної синхронізації;

3. Чому інтеграція між HR-системою та LMS не була реалізована при впровадженні платформи? Тому що LMS впроваджувалася HR-підрозділом виключно як репозиторій навчального контенту; технічне завдання не містило вимоги до автоматизації онбордингу та інтеграцій;

4. Чому технічне завдання на впровадження LMS не містило вимог з інформаційної безпеки? Тому що служба інформаційної безпеки не була залучена до процесу вибору та проектування технічного завдання LMS;

5. Чому служба інформаційної безпеки не залучається до рішень щодо впровадження систем? Тому що в організації відсутня формалізована процедура, що встановлює обов'язкове погодження нових корпоративних систем зі службою інформаційної безпеки.

Таким чином, кореневою причиною невідповідності є не технічне обмеження LMS і не персональна недбалість адміністратора, а системна організаційна прогалина. Коригувальна дія має охоплювати одночасно технічний рівень (інтеграцію між HR-системою та LMS) та організаційний (затвердження процедури обов'язкового погодження нових систем зі службою ІБ).

На основі виявлених невідповідностей та результатів аналізу кореневих причин сформовано дорожню карту рекомендацій для керівництва ТОВ «ТехКлауд», що охоплює чотири пріоритетні напрями з визначеними термінами реалізації. Послідовність етапів реалізації організаційних заходів інформаційної безпеки візуалізовано на рисунку 3.2.

Рис. 3.2. Дорожня карта впровадження рекомендацій для ТОВ «ТехКлауд»

Першою та найбільш терміновою рекомендацією є впровадження автоматизованої інтеграції між HR-системою, LMS та IAM-платформою. Технічна реалізація має передбачати три автоматизованих тригери. При створенні профілю нового співробітника в HR-системі автоматично ініціюється

призначення вступного навчального модуля у LMS та встановлюється обмеження на доступ до виробничих систем до отримання підтвердження про завершення навчання. При зміні посади автоматично перепризначаються права доступу відповідно до нової ролі. При закритті картки співробітника в HR-системі автоматично деактивується обліковий запис в Active Directory. Технічна реалізація інтеграції оцінюється у 30–40 людино-годин. Відповідальним за реалізацію призначається CISO спільно з технічним директором; рекомендований термін — 45 днів [11].

Другою рекомендацією є розробка та впровадження стандартизованої процедури оцінювання безпеки постачальників (Vendor Security Questionnaire). Етап первинного скринінгу передбачає, що будь-який підрозділ, який ініціює підключення нового SaaS-рішення, зобов'язаний заповнити заявку. На її основі служба безпеки присвоює рішенню категорію ризику. Для постачальників критичної категорії опитувальник охоплює питання наявності сертифікації ISO/IEC 27001, практик шифрування даних, процедур повідомлення про інциденти та права замовника на проведення незалежного аудиту. Також передбачається проведення ретроспективної інвентаризації наявних SaaS-рішень.

Третьою рекомендацією є запуск структурованої програми безперервного мікронавчання. Перший компонент передбачає щомісячні навчальні модулі тривалістю 5–7 хвилин, кожен з яких адресує одну конкретну тему безпеки (безпека облікових даних, правила роботи у хмарних середовищах). Короткий формат є принциповим для технічного персоналу [28]. Другий компонент — симульовані фішингові кампанії — проводяться щоквартально. Для розробників сценарії моделюють атаки через підроблені сповіщення від платформ розробки (GitHub, Jira, CI/CD). Третій компонент — вимірювання результативності програми через інтеграцію у систему KPI СМІБ.

Четвертою рекомендацією є формалізація процедури обов'язкового залучення служби інформаційної безпеки до впровадження нових IT-систем.

Процедура закріплює обов'язкове погодження зі службою безпеки на етапі формування технічного завдання. Критерії безпеки мають включатися до стандартного шаблону технічного завдання на рівні обов'язкового розділу [6].

Верифікація результативності реалізованих коригувальних дій планується через повторний аудит відповідних доменів через шість місяців. Очікуваним результатом є підвищення рівня зрілості доменів «Навчання та обізнаність персоналу» та «Відносини із постачальниками» з поточного значення 2.0 до цільового рівня 3.5. Результати повторного аудиту підлягають включенню до матеріалів аналізу з боку керівництва відповідно до вимог розділу 9.3 стандарту ISO/IEC 27001:2022, що забезпечить стратегічний вплив аудиторської діяльності на розвиток СМІБ.

Висновки до розділу 3

У третьому розділі розроблено практичний інструментарій забезпечення функціонування та вдосконалення СМІБ на прикладі модельної організації ТОВ «ТехКлауд» — умовного постачальника послуг хмарного хостингу класу IaaS та PaaS, що одночасно провадить діяльність з розробки програмного забезпечення. Вибір організації зазначеного профілю обумовлений складністю її ризик-середовища, що поєднує договірні зобов'язання щодо безперервності послуг із концентрацією клієнтських даних у хмарному середовищі.

Розроблено систему ключових показників ефективності на основі адаптованої концепції збалансованої системи показників Balanced Scorecard, що охоплює чотири перспективи: фінансову, зацікавлених сторін, внутрішніх процесів та навчання і розвитку. Встановлено, що цільові значення KPI для ТОВ «ТехКлауд» визначаються не галузевими нормами загального характеру, а безпосередньо договірними SLA-зобов'язаннями перед клієнтами: цільове значення MTTR менше 4 годин, 100-відсоткове охоплення аудитом постачальників та Click Rate менше 5% у симульованих фішингових кампаніях

відображають конкретні операційні ризики хмарного провайдера. Обґрунтовано трирівневу модель звітування за KPI та формалізовано процедуру ескалації при невиконанні цільових значень.

Проведено оцінювання рівня зрілості СМІБ ТОВ «ТехКлауд» за п'ятирівневою моделлю у розрізі десяти доменів. Виявлено характерну для технологічних компаній на стадії масштабування асиметрію: технічні домени управління вразливостями та управління доступом досягли четвертого рівня зрілості завдяки автоматизованим інструментам та IAM-архітектурі, тоді як організаційні домени зафіксовано на третьому рівні через відсутність автоматизованого вимірювання, а домени навчання персоналу та відносин із постачальниками отримали лише другий рівень через екстенсивне зростання чисельності персоналу та безконтрольне використання SaaS-рішень без оцінювання безпеки вендорів. Встановлено, що виявлена дисперсія балів безпосередньо визначає пріоритети програми внутрішнього аудиту.

Сформовано ризик-орієнтовану програму внутрішнього аудиту, сфокусовану на доменах із найнижчими рівнями зрілості. За результатами аудиту виявлено чотири значущі невідповідності: відсутність вступного навчання для 56% нових співробітників до отримання доступу до систем, договори із SaaS-постачальниками без вимог інформаційної безпеки, активні облікові записи семи звільнених співробітників із зафіксованими спробами автентифікації, а також відсутність процедури оцінювання безпеки нових SaaS-рішень до початку їх використання. Застосування методу «5 чому» до найбільш системної невідповідності виявило кореневою причиною не технічне обмеження LMS, а відсутність організаційної процедури обов'язкового залучення служби безпеки до прийняття рішень щодо корпоративних систем.

На основі результатів аудиту розроблено дорожню карту з чотирьох пріоритетних рекомендацій: автоматизована інтеграція між HR-системою, LMS та IAM-платформою; впровадження стандартизованої процедури оцінювання безпеки постачальників з Vendor Security Questionnaire; запуск програми

безперервного мікронавчання з щоквартальними симульованими фішинговими кампаніями; формалізація процедури обов'язкового залучення служби безпеки до проектування корпоративних систем. Реалізація рекомендацій спрямована на підвищення рівня зрілості проблемних доменів з поточного значення 2.0 до цільового рівня 3.5 протягом шести місяців.

Результати третього розділу підтверджують практичну цінність розробленого інструментарію та демонструють, що послідовне застосування системи KPI, оцінювання зрілості та внутрішнього аудиту дозволяє організації перейти від декларативної відповідності вимогам стандарту до реально функціонуючого механізму управління інформаційною безпекою.

ВИСНОВКИ

У ході дослідження здійснено комплексний аналіз методів забезпечення функціонування системи менеджменту інформаційної безпеки (СМІБ) організації. Систематизація теоретико-методологічних засад дозволила простежити еволюцію міжнародної нормативної бази від суто інженерних інструкцій британського стандарту до сучасної комплексної управлінської рамки, закріпленої у чинній редакції ISO/IEC 27001:2022. Встановлено, що розширення структури стандарту та впровадження нових одинадцяти заходів захисту, включаючи розвідку загроз і безпечне кодування, відображає тенденцію до мінімізації меж між фізичними та цифровими загрозами у хмарних середовищах. На основі аналізу методологічного взаємозв’язку стандартів ISO/IEC 27005 та ISO 31000 обґрунтовано безальтернативність ризик-орієнтованого підходу як концептуального фундаменту СМІБ, який успішно вирішує проблему обмеженості ресурсів через концентрацію захисту в зонах із найбільш значущими ризиками.

Проведено критичний аналіз підходів до операційного управління процесами СМІБ та доведено, що її реальна результативність визначається не формальною наявністю задокументованих процедур, а якістю їхнього щоденного практичного втілення. Окрему увагу приділено управлінню людським фактором як центральному напряму забезпечення захисту інформаційних активів. На основі розмежування поняття обізнаності та компетентності з'ясовано, що традиційні одноразові навчальні заходи є малоефективними через вплив психологічної кривої забування Еббінгауза. Обґрунтовано доцільність побудови безперервних, сегментованих програм підвищення обізнаності, спрямованих на формування сталої організаційної культури безпеки, де персонал діє усвідомлено й бере особисту відповідальність за захист даних. Додатково систематизовано три взаємодоповнюючі механізми оцінювання — поточний моніторинг,

внутрішній аудит та аналіз з боку керівництва, що трансформують СМІБ у динамічну систему.

У межах практичної реалізації розроблено та апробовано прикладний інструментарій забезпечення функціонування СМІБ на прикладі модельної організації ТОВ «ТехКлауд». Сформовано комплексну систему ключових показників ефективності (KPI) на основі адаптованої концепції Balanced Scorecard, яка дозволяє подолати розрив між функцією безпеки та бізнесом шляхом перекладу технічних метрик у площину фінансових збитків та договірних SLA-зобов'язань. Побудований профіль зрілості виявив характерну для технологічних компаній асиметрію: високий рівень зрілості інфраструктурних доменів супроводжується суттєвим відставанням у сферах навчання персоналу та контролю безпеки хмарних SaaS-постачальників. Запропоновано ризик-орієнтований підхід до проведення внутрішнього аудиту з акцентом на пошук кореневих причин невідповідностей за допомогою методу «5 чому», що забезпечує усунення системних організаційних прогалин, а не лише їхніх зовнішніх симптомів.

Узагальнення результатів дослідження дозволило визначити, що його обмеженням є першочергова спрямованість на специфіку діяльності IT-підприємств та провайдерів хмарних послуг. Перспективи подальших розвідок у цьому напрямі полягають в адаптації розробленої системи моніторингу та оцінювання KPI для організацій інших секторів економіки, зокрема банківського та державного, а також у дослідженні можливостей інтеграції алгоритмів штучного інтелекту для автоматизації процедур внутрішнього аудиту та безперервного аналізу ризиків інформаційної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект : підручник / В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа. — Київ : ДУТ, 2015. — 288 с.

2. Гнатюк С. О., Корченко О. Г., Сейтумеров С. В. Методологія управління ризиками інформаційної безпеки в сучасних ІТС // Захист інформації. — 2021. — Т. 23, № 1. — С. 22–30.

3. ДСТУ EN ISO/IEC 27000:2022 (EN ISO/IEC 27000:2020, IDT; ISO/IEC 27000:2018, IDT). Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів. — Київ : ДП «УкрНДНЦ», 2022. — 35 с.

4. ДСТУ ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT). Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги. — Київ : ДП «УкрНДНЦ», 2023. — 26 с.

5. ДСТУ ISO/IEC 27002:2023 (ISO/IEC 27002:2022, IDT). Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки. — Київ : ДП «УкрНДНЦ», 2023. — 164 с.

6. ДСТУ ISO/IEC 27005:2023 (ISO/IEC 27005:2022, IDT). Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки. — Київ : ДП «УкрНДНЦ», 2023. — 56 с.

7. ДСТУ ISO/IEC 27017:2019. Інформаційні технології. Методи захисту. Настанови щодо засобів контролювання інформаційної безпеки на основі ISO/IEC 27002 для хмарних послуг. — Київ : ДП «УкрНДНЦ», 2020. — 42 с.

8. ДСТУ ISO/IEC 27018:2022. Інформаційні технології. Методи захисту. Звід правил щодо захисту персональних даних у загальнодоступних хмарних середовищах. — Київ : ДП «УкрНДНЦ», 2023. — 35 с.

9. ДСТУ ISO/IEC 27035-1:2019. Інформаційні технології. Методи захисту. Управління інцидентами інформаційної безпеки. Частина 1. Основні принципи. — Київ : ДП «УкрНДНЦ», 2020. — 28 с.

10. ДСТУ ISO/IEC 27701:2022. Інформаційні технології. Методи захисту. Система керування інформацією про конфіденційність. Вимоги та настанови. — Київ : ДП «УкрНДНЦ», 2023. — 60 с.

11. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII [Електронний ресурс]. — Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 26.05.2026).

12. Захарченко С. М., Іванов О. М. Сучасні підходи до оцінювання зрілості процесів кібербезпеки в організаціях // Системи обробки інформації. — 2022. — № 2. — С. 45–51.

13. Корченко О. Г. Системи управління інформаційною безпекою: сучасні виклики та ризик-орієнтований підхід // Кібербезпека: освіта, наука, техніка. — 2023. — № 1. — С. 15–24.

14. Лукова-Чуйко Н. В., Смірнов О. А. Роль людського фактора в забезпеченні інформаційної безпеки підприємства // Кібербезпека: освіта, наука, техніка. — 2021. — № 4. — С. 76–83.

15. Про затвердження Порядку реагування на кіберінциденти, кібератаки та кіберзагрози [Електронний ресурс] : Наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 18.02.2026 № 143. — Режим доступу: https://cip.gov.ua/ (дата звернення: 26.05.2026).

16. Російські кібероперації: Аналітика за перше півріччя 2023 року [Електронний ресурс] / Державна служба спеціального зв’язку та захисту інформації України. — Київ, 2023. — Режим доступу: https://cip.gov.ua/ (дата звернення: 21.05.2026).

17. Смірнов О. А. Управління ризиками інформаційної безпеки відповідно до вимог ISO 27001 // Захист інформації. — 2022. — Т. 24, № 2. — С. 45–52.

18. Сопілко І. М. Інформаційна безпека та кібербезпека: порівняльно-правовий аспект // Юридичний вісник. Повітряне і космічне право. — 2021. — № 2. — С. 110–115.

19. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України"» від 26.08.2021 № 447/2021 [Електронний ресурс]. — Режим доступу: https://zakon.rada.gov.ua/laws/show/447/2021 (дата звернення: 26.05.2026).

20. Чумак В. І. Формування культури інформаційної безпеки на підприємстві // Кібербезпека: освіта, наука, техніка. — 2022. — № 3. — С. 88–94.

21. Annex L: Proposals for management system standards [Електронний ресурс] // ISO/IEC Directives, Part 1 — Consolidated ISO Supplement — Procedures specific to ISO. — 13th ed. — Geneva : ISO, 2022. — Режим доступу: https://www.iso.org/directives-and-policies.html (дата звернення: 26.05.2026).

22. CIS Controls v8 [Електронний ресурс] / Center for Internet Security. — 2021. — Режим доступу: https://www.cisecurity.org/controls/v8 (дата звернення: 26.05.2026).

23. Cisco Cybersecurity Readiness Index 2023 [Електронний ресурс] / Cisco. — 2023. — Режим доступу: https://www.cisco.com/c/en/us/products/security/cybersecurity-readiness-index.html (дата звернення: 26.05.2026).

24. Computer Security Incident Handling Guide : NIST Special Publication 800-61 Rev. 2 / P. Cichonski, T. Millar, T. Grance, K. Scarfone. — Gaithersburg : National Institute of Standards and Technology, 2012. — 79 p.

25. Cost of a Data Breach Report 2023 [Електронний ресурс] / IBM Security. — 2023. — Режим доступу: https://www.ibm.com/reports/data-breach (дата звернення: 26.05.2026).

26. Cybersecurity Capability Maturity Model (C2M2). Version 2.1 [Електронний ресурс] / U.S. Department of Energy. — 2022. — Режим доступу:

https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2 (дата звернення: 26.05.2026).

27. Data Breach Investigations Report 2023 [Електронний ресурс] / Verizon. — 2023. — Режим доступу: https://www.verizon.com/business/resources/reports/dbir/ (дата звернення: 26.05.2026).

28. ENISA Threat Landscape 2023 [Електронний ресурс] / European Union Agency for Cybersecurity. — 2023. — Режим доступу: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (дата звернення: 26.04.2026).

29. Gartner Top Strategic Cybersecurity Trends for 2024 [Електронний ресурс] / Gartner. — 2024. — Режим доступу: https://www.gartner.com/en/cybersecurity (дата звернення: 26.05.2026).

30. Global Cybersecurity Outlook 2023 [Електронний ресурс] / World Economic Forum. — 2023. — Режим доступу: https://www.weforum.org/reports/global-cybersecurity-outlook-2023/ (дата звернення: 26.05.2026).

31. Guide for Conducting Risk Assessments : NIST Special Publication 800-30 Rev. 1 / Joint Task Force Transformation Initiative. — Gaithersburg : National Institute of Standards and Technology, 2012. — 95 p.

32. ISO 19011:2018. Guidelines for auditing management systems. — Geneva : ISO, 2018. — 46 p.

33. ISO 31000:2018. Risk management — Guidelines. — Geneva : ISO, 2018. — 16 p.

34. ISO/IEC 27004:2016. Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation. — Geneva : ISO, 2016. — 56 p.

35. ISO/IEC 27007:2020. Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing. — Geneva : ISO, 2020. — 38 p.

36. Microsoft Digital Defense Report 2023 [Електронний ресурс] / Microsoft. — 2023. — Режим доступу: https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023 (дата звернення: 26.05.2026).

37. NIST Cybersecurity Framework 2.0 [Електронний ресурс] / National Institute of Standards and Technology. — 2024. — Режим доступу: https://csrc.nist.gov/ (дата звернення: 22.05.2026).

38. OWASP Top 10:2021 [Електронний ресурс] / Open Web Application Security Project. — 2021. — Режим доступу: https://owasp.org/Top10/ (дата звернення: 26.05.2026).

39. Performance Measurement Guide for Information Security : NIST Special Publication 800-55 Rev. 1 / E. Chew, M. Swanson, K. Stine. — Gaithersburg : National Institute of Standards and Technology, 2008. — 80 p.

40. Security and Privacy Controls for Information Systems and Organizations : NIST Special Publication 800-53 Rev. 5. — Gaithersburg : National Institute of Standards and Technology, 2020. — 492 p.