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 ВІДПОВІДНОСТІ СИСТЕМИ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ РЕГУЛЯТОРНИМ ВИМОГАМ”

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

_____ Іван ІПАТОВ
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-41
Іван ІПАТОВ
Ім’я, ПРІЗВИЩЕ

Керівник: Іван ОПІРСЬКИЙ
Д.т.н., професор Ім’я, ПРІЗВИЩЕ

Рецензент: Галина ГАЙДУР
Д.т.н., професор Ім’я, ПРІЗВИЩЕ

Київ 2025

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
“____”_____2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Іпатову Івану Андрійовичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Методи забезпечення відповідності системи менеджменту інформаційної безпеки регуляторним вимогам ”,
керівник кваліфікаційної роботи ОПІРСЬКИЙ Іван, д.т.н., професор,
(ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологійвід “24“ лютого 2025 р. №56.

2. Строк подання кваліфікаційної роботи “20” травня 2025р.

3. Вихідні дані до кваліфікаційної роботи: *інформаційна безпека підприємства, методи та засоби забезпечення відповідності СМІБ регуляторним вимогам, міжнародні стандарти, наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:
4.1. Проаналізувати теоретичні засади системи менеджменту інформаційної безпеки та регуляторних вимог.
4.2. Дослідити практичні аспекти забезпечення відповідності СМІБ регуляторним вимогам.
4.3. Вивчити рекомендації щодо вдосконалення системи менеджменту інформаційної безпеки та перспективи розвитку.
Перелік ілюстративного матеріалу: *презентація PowerPoint*

5. Дата видачі завдання “11“ березня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2025	Виконано
2.	Збір та аналіз літератури.	29.03.2025	Виконано
3.	Аналіз теоретичних засад системи менеджменту інформаційної безпеки та регуляторних вимог.	08.04.2025	Виконано
4.	Дослідження практичних аспектів забезпечення відповідності СМІБ регуляторним вимогам.	22.04.2025	Виконано
5.	Вивчення рекомендацій щодо вдосконалення системи менеджменту інформаційної безпеки та перспективи розвитку	08.05.2025	Виконано
6.	Формулювання висновків за результатами проведеного дослідження.	20.05.2025	Виконано
7.	Оформлення роботи.	22.05.2025	Виконано
8.	Оформлення презентації.	03.06.2025	Виконано
9.	Отримання рецензії на роботу.	03.06.2025	Виконано
10.	Захист в ЕК.	__.06.2025	

Здобувач вищої освіти _____ Іван ІПАТОВ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Іван ОПІРСЬКИЙ
(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 Іпатов І.А. 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 відповідності системи менеджменту інформаційної безпеки регуляторним вимогам"

Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач ІПАТОВ Іван у кваліфікаційній роботі проаналізував теоретичні засади системи менеджменту інформаційної безпеки та регуляторних вимог, дослідив практичні аспекти забезпечення відповідності СМІБ регуляторним вимогам, вивчив рекомендації щодо вдосконалення системи менеджменту інформаційної безпеки та перспективи розвитку. ІПАТОВ Іван показав розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, довів володіння методами наукового дослідження, проявив себе як організований, відповідальний виконавець. Результати дослідження апробовані на конференції.

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

Керівник кваліфікаційної роботи _____ Іван ОПІРСЬКИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____" _____2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Іпатов І.А. 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 ІПАТОВА Івана
на тему “ Методи забезпечення відповідності системи менеджменту інформаційної безпеки регуляторним вимогам”

Актуальність. У сучасному цифровому середовищі, де державні інституції, підприємства та приватні особи дедалі частіше стають мішенню кібератак, забезпечення інформаційної безпеки є критично важливим завданням. Із розвитком ІТ-технологій зростає складність інформаційних загроз, що вимагає від організацій системного підходу до управління інформаційною безпекою. Особливе значення в цьому контексті має дотримання регуляторних вимог, які встановлюють стандарти та правила захисту інформації. Невідповідність СМІБ таким вимогам може призвести до серйозних юридичних, фінансових і репутаційних наслідків.
У зв’язку з цим дослідження методів забезпечення відповідності СМІБ регуляторним вимогам є надзвичайно актуальним як з наукової, так і з практичної точки зору.

Позитивні сторони.

1. У роботі досліджено сучасні підходи та методи забезпечення відповідності СМІБ регуляторним вимогам.

2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки. Ключові положення роботи представлено у вигляді рисунків.

3. Автор опрацював значну джерельну базу: близько 50 публікацій, в тому числі англомовних.

4. За результатами дослідження вивчен рекомендації щодо ефективного навчання персоналу з питань інформаційної безпеки.

Недоліки.

Доцільно було б розширити аналіз і класифікацію програмних рішень та інструментів, які використовуються для оцінки відповідності СМІБ встановленим вимогам.

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

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

Рецензент: _____ Галина ГАЙДУР
підпис Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню методів забезпечення відповідності системи менеджменту інформаційної безпеки регуляторним вимогам. Робота складається зі вступу, трьох розділів, що містять 7 рисунків та 8 таблиць, висновків і списку використаних джерел із 62 найменувань. Загальний обсяг роботи становить 74 аркуші, з яких 7 аркушів займають перелік умовних скорочень та список використаних джерел.

Метою роботи є дослідження методів забезпечення відповідності системи менеджменту інформаційної безпеки регуляторним вимогам, аналізі їх ефективності та розробці практичних рекомендацій для підвищення рівня відповідності.

Об'єктом дослідження є система менеджменту інформаційної безпеки на підприємстві.

Предмет дослідження – методи та підходи, які забезпечують відповідність СМІБ вимогам нормативних документів, стандартів і регуляторів.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації, а також методи експертного оцінювання рівня відповідності СМІБ встановленим вимогам.

Як результат у роботі проаналізовано теоретичні засади системи менеджменту інформаційної безпеки та регуляторних вимог, досліджено практичні аспекти забезпечення відповідності СМІБ регуляторним вимогам, вивчено рекомендації щодо вдосконалення системи менеджменту інформаційної безпеки та перспективи розвитку.

Галузь застосування. Розроблені методи можуть бути використані при впровадженні, перевірці та вдосконаленні системи менеджменту інформаційної безпеки з метою забезпечення її відповідності чинним регуляторним вимогам. Застосування запропонованих підходів є доцільним у рамках підготовки до сертифікації за міжнародними стандартами, проведення внутрішніх аудитів, а

також у процесі розробки політик інформаційної безпеки відповідно до вимог національного законодавства та міжнародних норм.

Ключові слова: СИСТЕМА МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, СТАНДАРТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, НОРМАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ, УПРАВЛІННЯ РИЗИКАМИ, GAP-АНАЛІЗ, ОЦІНКА ВІДПОВІДНОСТІ.

ABSTRACT

The qualification work is devoted to the study of methods for ensuring that the information security management system meets regulatory requirements. The work consists of an introduction, three chapters containing 7 figures and 8 tables, conclusions and the list of references containing 62 items. The total volume of the work is 74 pages, of which 7 pages are occupied by the list of abbreviations and the list of references.

The purpose of the study is to investigate methods of ensuring compliance of the information security management system with regulatory requirements, analyse their effectiveness and develop practical recommendations for improving the level of compliance.

The object the study is the information security management system at an enterprise.

The subject of the study is methods and approaches that ensure compliance of the ISMS with the requirements of regulatory documents, standards and regulators.

Research methods. In order to solve the mentioned higher scientific task, the methods of analysis and synthesis, comparison, classification, as well as methods of expert assessment of the level of compliance of the ISMS with the established requirements are used.

As a result, the work analyzed the theoretical foundations of the information security management system and regulatory requirements, investigated the practical aspects of ensuring compliance of the ISMS with regulatory requirements, and studied recommendations for improving the information security management system and development prospects.

Field of application. The developed approaches can be used in the implementation, verification and improvement of the information security management system to ensure its compliance with current regulatory requirements. The application of the proposed approaches is advisable in the framework of preparation for certification according to international standards, conducting internal audits, as well as in the process of developing information security policies in

accordance with the requirements of national legislation and international norms.

Keywords: INFORMATION SECURITY MANAGEMENT SYSTEM, INFORMATION SECURITY STANDARDS, REGULATORY AND LEGAL REGULATION, RISK MANAGEMENT, GAP ANALYSIS, CONFORMITY ASSESSMENT.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ІБ Інформаційна безпека

СМІБ Система менеджменту інформаційної безпеки

ІС Інформаційна система

ПЗ Програмне забезпечення

СУБД Система управління базами даних

НПА Нормативно-правові акти

ISMS Information Security Management System

ISO/IEC 27001 Міжнародний стандарт системи управління інформаційною безпекою

КЗІ Криптографічний захист інформації

ДСЗІ Державна служба спеціального зв'язку та захисту інформації України

ІТ Інформаційні технології

GDPR General Data Protection Regulation

ОВТ Оцінювання відповідності технічних рішень

РВ Регуляторні вимоги

SOC Security Operations Center

SIEM Security Information and Event Management

ВСТУП

Актуальність теми. У сучасних умовах цифрової трансформації підприємства, організації та установи стикаються з постійним зростанням кіберзагроз, що ускладнює забезпечення сталого функціонування бізнес-процесів. У зв'язку з цим системи менеджменту інформаційної безпеки (СМІБ) повинні не лише відповідати актуальним викликам, але й дотримуватися встановлених регуляторних вимог на національному та міжнародному рівнях. Такі вимоги визначають рамки, критерії та механізми, які гарантують цілісність, конфіденційність і доступність інформації.

Зважаючи на динаміку змін у нормативно-правовому середовищі, особливу актуальність набуває системний підхід до забезпечення відповідності СМІБ цим вимогам. Йдеться не лише про технічні заходи, а й про впровадження ефективних управлінських і організаційних методів, які дозволяють виявляти, аналізувати й усувати невідповідності у системі безпеки.

Мета роботи полягає у дослідженні методів забезпечення відповідності системи менеджменту інформаційної безпеки регуляторним вимогам, аналізі їх ефективності та розробці практичних рекомендацій для підвищення рівня відповідності.

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

Предмет дослідження – методи та підходи, які забезпечують відповідність СМІБ вимогам нормативних документів, стандартів і регуляторів.

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання**:

1. Проаналізувати теоретичні засади системи менеджменту інформаційної безпеки та регуляторних вимог.

2. Дослідити практичні аспекти забезпечення відповідності СМІБ регуляторним вимогам.

3. Вивчити рекомендації щодо вдосконалення системи менеджменту інформаційної безпеки та перспективи розвитку.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації, а також методи експертного оцінювання рівня відповідності СМІБ встановленим вимогам.

Практичне значення одержаних результатів. Результати дослідження дозволяють здійснити обґрунтований вибір методів і засобів адаптації СМІБ до регуляторних вимог, сприяють підвищенню ефективності аудиту інформаційної безпеки, а також формуванню політик та процедур відповідно до специфіки діяльності підприємства й вимог законодавства.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 27 лютого 2025 року.

Розділ 1 ТЕОРЕТИЧНІ ЗАСАДИ СИСТЕМИ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА РЕГУЛЯТОРНИХ ВИМОГ

Система менеджменту інформаційної безпеки (СМІБ) є формалізованим механізмом управління політиками, процесами та технічними заходами, спрямованими на забезпечення конфіденційності, цілісності й доступності інформації в межах організації. Її структура, принципи функціонування та вимоги до реалізації регламентуються національними та міжнародними нормативними актами, зокрема стандартом ISO/IEC 27001, регламентом GDPR, вимогами НБУ та іншими галузевими регуляторами. Забезпечення відповідності СМІБ цим вимогам вимагає застосування системного підходу до ризик-менеджменту, внутрішнього аудиту, документування процесів безпеки та оцінки їх ефективності.

1.1 Поняття та структура системи менеджменту інформаційної безпеки

Система менеджменту інформаційної безпеки визначається як частина загальної системи менеджменту організації, яка ґрунтується на оцінці ризиків і має на меті створення, впровадження, експлуатацію, моніторинг, перегляд, підтримку та вдосконалення заходів інформаційної безпеки. Відповідно до стандарту ISO/IEC 27000, СМІБ включає в себе політики, процедури, правила поведінки, а також технічні й організаційні заходи, що забезпечують захист інформаційних активів. Основною метою СМІБ є забезпечення конфіденційності, цілісності та доступності інформації в межах встановлених меж управління [1].

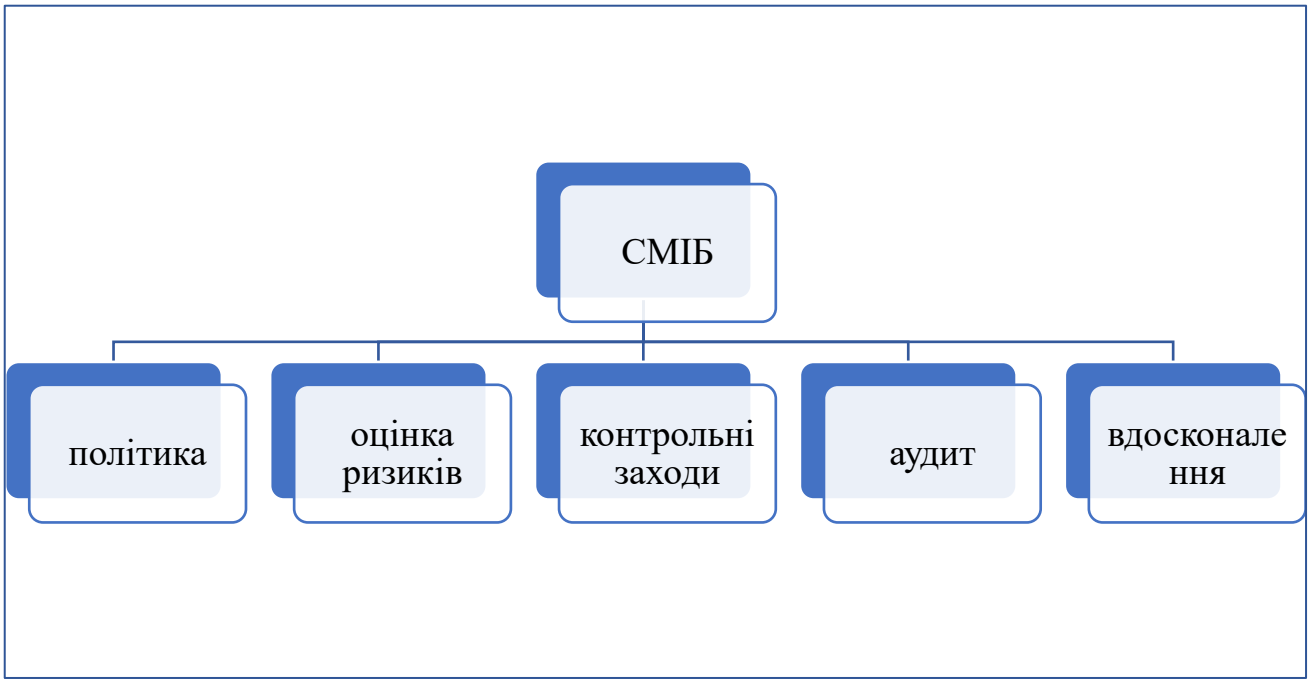

Рис. 1.1 Структура СМІБ

Система менеджменту інформаційної безпеки має кілька ключових характеристик, які відрізняють її від звичайних підходів до технічного захисту. По-перше, СМІБ охоплює не лише технічні аспекти, а й організаційні, правові та людські фактори. Вона базується на принципах управління, аналогічних до інших систем менеджменту, таких як системи управління якістю (ISO 9001) або екологічного менеджменту (ISO 14001). Таким чином, її структура побудована відповідно до логіки планування, реалізації, контролю та вдосконалення – підходу, відомого як цикл PDCA (Plan–Do–Check–Act) [2].

Визначальною особливістю СМІБ є її адаптивність до змін зовнішнього середовища та внутрішніх процесів організації. Система повинна реагувати на зміну законодавчих вимог, поява нових типів загроз, зміни в організаційній структурі, технологічні новації, а також на результати внутрішніх аудитів і зовнішніх перевірок. Успішна реалізація СМІБ можлива лише за умови активної участі вищого керівництва організації, яке несе відповідальність за визначення політики безпеки, виділення необхідних ресурсів і підтримку культури безпеки.

Система функціонує на основі комплексного підходу до управління

ризиками. Для цього на початковому етапі впровадження СМІБ проводиться ідентифікація інформаційних активів, визначення їхньої цінності, оцінка вразливостей, аналіз загроз і розрахунок ризиків. На основі цього формуються заходи контролю, які можуть бути як технічними (наприклад, міжмережеві екрани, системи виявлення вторгнень, антивірусні рішення), так і організаційними (регламенти доступу, процедури резервного копіювання, політики автентифікації). Усі заходи повинні документуватись та бути доступними для персоналу, який відповідає за їх виконання [3].

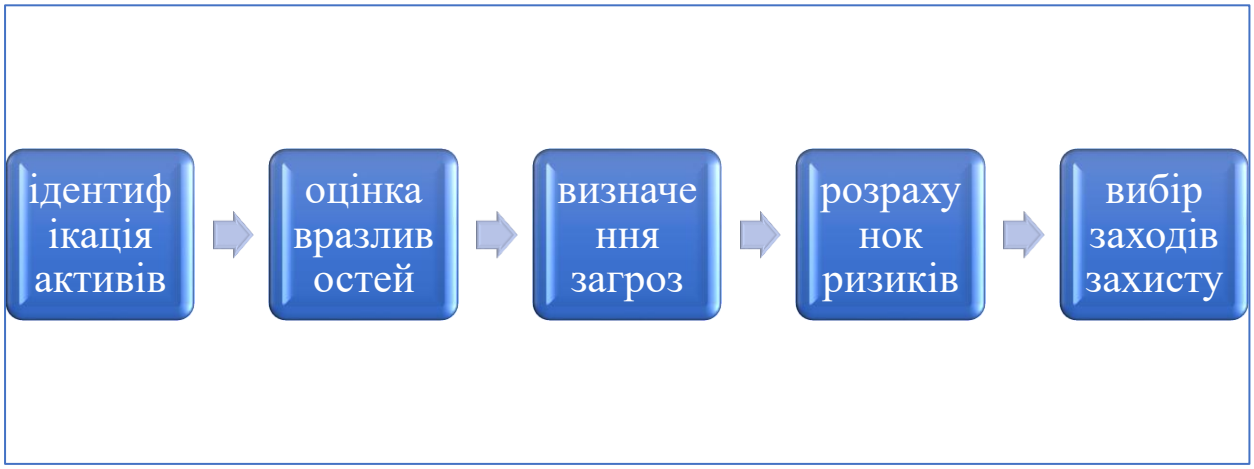

Рис. 1.2 Процес оцінки ризиків у СМІБ

До обов’язкових компонентів СМІБ належать формалізовані політики безпеки, опис процедур та інструкцій, а також призначення відповідальних осіб і структурних підрозділів. Крім того, має бути забезпечене управління інцидентами, тобто виявлення, реєстрація, реагування та аналіз порушень інформаційної безпеки. Окрему увагу слід приділяти питанням моніторингу та оцінювання ефективності заходів безпеки. Це передбачає визначення показників продуктивності, регулярне проведення внутрішніх аудитів, аналіз результатів перевірок та впровадження коригувальних і попереджувальних дій [4].

Таблиця 1.1

Компоненти СМІБ і їхнє призначення

Компонент	Призначення	Документальне оформлення
Політика безпеки	Визначає загальні принципи	Наказ, положення
Оцінка ризиків	Ідентифікація загроз і вразливостей	Звіт, карта ризиків
Контрольні заходи	Реалізація захисту	Регламенти, інструкції
Внутрішній аудит	Перевірка ефективності	Звіт аудитора

З точки зору структури, СМІБ організовується як багаторівнева система, де кожен рівень має свої функції й відповідальність. На стратегічному рівні визначається загальна політика, цілі та межі СМІБ. На тактичному рівні розробляються плани реалізації, обираються засоби захисту, формуються регламенти взаємодії. На операційному рівні здійснюється щоденне управління інформаційною безпекою, моніторинг подій, адміністрування систем, навчання персоналу та підтримка процедур. Усі рівні мають бути взаємопов’язані, що забезпечує цілісність функціонування системи.

Інтеграція СМІБ з іншими системами управління є важливою умовою її ефективності. Наприклад, у банківському секторі СМІБ інтегрується з системою управління ризиками, системами комплаєнсу, управління бізнес-процесами та внутрішнього контролю. У промисловості – з системами технічної безпеки, контролю виробничих процесів та захисту персональних даних. Це дозволяє не лише оптимізувати витрати, а й забезпечити узгодженість між різними функціональними напрямами [5].

СМІБ має відповідати регуляторним вимогам, які можуть бути обов’язковими (національні закони, нормативи регуляторів) або добровільними (міжнародні стандарти, рекомендації галузевих організацій). У практиці українських підприємств до основних регуляторів належать Державна служба спеціального зв’язку та захисту інформації України, Національний банк України,

а також законодавство у сфері захисту персональних даних. З міжнародних стандартів найпоширенішими є ISO/IEC 27001, NIST SP 800-53, COBIT 5, ITIL. Кожен із них передбачає певну структуру, термінологію, принципи побудови та управління СМІБ, але всі вони базуються на ідентичних принципах системного управління ризиками [6].

Таблиця 1.2

Порівняльна таблиця стандартів СМІБ

Стандарт	**Область застосування**	**Особливості**	**Вимоги до відповідності**
ISO/IEC 27001	Універсальний	Ризик-орієнтований підхід	Сертифікація обов'язкова
NIST SP 800-53	США, держ. сектор	Каталоги контролів	Обов'язковий для держустанов
COBIT 5	IT-менеджмент	Бізнес-орієнтована структура	Орієнтація на управління

Наявність сертифікованої СМІБ за стандартом ISO/IEC 27001 є конкурентною перевагою для компаній, які працюють з міжнародними партнерами або обробляють чутливу інформацію. Такий сертифікат підтверджує здатність організації забезпечувати безпеку інформації відповідно до визнаних світових стандартів. У рамках сертифікації проводиться зовнішній аудит, під час якого оцінюється наявність документованої політики, реалізація заходів захисту, компетентність персоналу, ефективність управління ризиками та постійне вдосконалення системи.

Система менеджменту інформаційної безпеки повинна також передбачати навчання та підвищення обізнаності персоналу. Це один з основних елементів ефективного функціонування СМІБ, оскільки людський фактор залишається однією з головних причин порушень безпеки. Навчальні програми мають охоплювати правила користування інформаційними системами, виявлення фішингових атак, реагування на інциденти, а також обов'язки щодо збереження конфіденційної інформації. Проведення регулярного тестування знань та участь

у тренінгах зміцнює культуру безпеки в організації [7].

Ще одним важливим аспектом є забезпечення документованості СМІБ. Усі політики, процедури, результати оцінювання ризиків, звіти аудитів, плани вдосконалення мають бути належним чином зафіксовані. Це не лише підвищує прозорість процесів, а й дозволяє відслідковувати виконання заходів, аналізувати ефективність впроваджених рішень, а також забезпечувати доказову базу у випадку перевірок з боку регуляторів або партнерів. Документування має здійснюватися відповідно до єдиної структури та вимог організації, із визначенням відповідальних осіб за оновлення інформації.

Ефективна СМІБ є не статичним набором правил, а динамічною системою, яка розвивається разом із організацією. Вона повинна враховувати зміни в архітектурі ІТ-систем, впровадження нових програмних продуктів, зміну ролей і відповідальності працівників, вимоги партнерів та клієнтів. Для цього передбачено механізми регулярного перегляду політик, періодичні переоцінки ризиків, оновлення заходів контролю, аналіз інцидентів та планування вдосконалень. Безперервне вдосконалення є фундаментальним принципом, що відрізняє СМІБ від разових проєктів або технічних рішень [8].

Система менеджменту інформаційної безпеки функціонує як цілісна структура, що включає взаємопов’язані елементи, кожен з яких виконує конкретну функцію щодо захисту інформаційних активів. Основу СМІБ складає політика інформаційної безпеки, яка є офіційним документом, затвердженим керівництвом організації. У ній визначаються цілі, принципи, підходи до захисту інформації, а також обов’язки працівників і загальні вимоги до реалізації системи. Політика має бути короткою, чіткою, зрозумілою та регулярно оновлюватися відповідно до змін законодавства, стандартів чи внутрішніх процесів.

Другим важливим елементом є аналіз ризиків. Цей процес включає виявлення інформаційних активів, їх класифікацію за рівнем критичності, виявлення потенційних загроз і вразливостей, а також оцінку ймовірності настання інцидентів і можливих наслідків. Оцінювання ризиків здійснюється за

кількісною або якісною методикою. Результатом цього процесу є ризик-профіль організації, на основі якого приймаються рішення щодо впровадження конкретних заходів контролю. Система управління ризиками має бути безперервною і враховувати динаміку зовнішнього та внутрішнього середовища.

Далі формується набір контрольних заходів, які повинні бути задокументовані та адаптовані до конкретної організації. Заходи безпеки можуть бути адміністративними (регламентування доступу, визначення ролей і відповідальності), фізичними (охорона приміщень, контроль доступу до серверних), технічними (шифрування даних, антивірусні програми, міжмережеві екрани) та процедурними (регламенти реагування на інциденти, інструкції з резервного копіювання). Контрольні заходи мають бути адекватними ризикам, економічно обґрунтованими й узгодженими з бізнес-цілями організації [9].

Наступним компонентом є система документування та процедур. СМІБ передбачає створення повного комплекту документації, що описує функціонування системи. Це можуть бути політики, регламенти, посадові інструкції, методики оцінки ризиків, протоколи інцидентів, результати аудитів, звіти про впровадження заходів, плани навчання тощо. Уся документація повинна зберігатися у визначеному місці, мати контроль версій, бути доступною для співробітників, які беруть участь у забезпеченні інформаційної безпеки. Уніфікована структура документів полегшує аудит і контроль за виконанням вимог.

Ключову роль у функціонуванні СМІБ відіграє організаційна структура управління. У межах організації мають бути чітко визначені ролі, повноваження і відповідальність за різні напрями інформаційної безпеки. Як правило, на рівні керівництва призначається особа, відповідальна за інформаційну безпеку (CISO або аналогічна посада), яка координує діяльність, приймає стратегічні рішення та звітує перед вищим керівництвом. Крім того, можуть бути створені спеціалізовані підрозділи або робочі групи, які відповідають за конкретні напрями – технічну підтримку, аудит, розробку політик, навчання персоналу. Від чіткої координації цих ролей залежить ефективність реалізації системи [10].

Окремим компонентом СМІБ є система навчання та підвищення обізнаності персоналу. Цей процес повинен бути постійним і охоплювати всі рівні працівників – від адміністративного до технічного персоналу. Навчання може включати проведення семінарів, тренінгів, електронних курсів, тестувань, моделювання інцидентів, ознайомлення з політиками та інструкціями. Обізнаність працівників є критичним фактором у запобіганні фішинговим атакам, помилкам при роботі з конфіденційною інформацією та забезпеченні загальної кібергігієни. Ефективна програма навчання повинна бути інтегрована в загальну систему розвитку персоналу й оцінюватися за результатами тестувань або практичних вправ [11].

Система моніторингу і вимірювання ефективності є ще одним структурним елементом СМІБ. Для цього використовуються індикатори продуктивності (KPI), журнали подій, системи моніторингу (наприклад, SIEM), а також регулярні перевірки, інспекції, аналіз журналів та відгуки користувачів. У процесі моніторингу здійснюється виявлення порушень політик, спроб несанкціонованого доступу, збоїв у роботі засобів захисту. Отримані дані дозволяють оперативно реагувати на інциденти, вдосконалювати систему й оцінювати ефективність вжитих заходів.

Інтегральною частиною СМІБ є внутрішній аудит. Його мета – незалежна перевірка відповідності функціонування СМІБ установленим вимогам, стандартам, політикам і процедурам. Аудит проводиться за попередньо затвердженим планом, із залученням внутрішніх або зовнішніх експертів, і має охоплювати всі ключові елементи системи. За результатами аудиту формується звіт із зазначенням невідповідностей, коментарями, а також рекомендаціями щодо вдосконалення. Аудит також є інструментом контролю підготовки до сертифікації СМІБ або перевірок з боку регуляторів [12].

Компонентом, який забезпечує динамічність і адаптивність СМІБ, є механізм коригувальних та попереджувальних дій. У разі виявлення порушень, інцидентів або відхилень від політик організація має реагувати шляхом аналізу причин, формулювання заходів, призначення відповідальних, контролю

виконання. Коригувальні дії спрямовані на усунення наслідків та запобігання повторенню проблем, тоді як попереджувальні – на виявлення й усунення потенційних ризиків до їх реалізації. Ці процеси повинні бути чітко задокументовані й інтегровані в загальну систему менеджменту.

Серед додаткових, але важливих компонентів СМІБ можна назвати управління інцидентами інформаційної безпеки. Це спеціальний процес, який охоплює фіксацію, класифікацію, розслідування та ліквідацію наслідків інцидентів, таких як витоки даних, несанкціонований доступ, зараження шкідливим ПЗ. Управління інцидентами також включає інформування відповідальних осіб, документування події та оцінку її впливу на організацію. Наявність відповідних інструкцій та сценаріїв реагування забезпечує швидку і скоординовану дію всіх залучених працівників.

Таблиця 1.3

Основні структурні компоненти СМІБ і їх призначення

Компонент	**Призначення**	**Документальне оформлення**
Політика ІБ	Визначення загальних принципів захисту інформації	Політика безпеки, положення
Оцінка ризиків	Виявлення активів, загроз, вразливостей і визначення рівня ризику	Звіт з аналізу ризиків
Контрольні заходи	Впровадження технічного й організаційного захисту	Реєстр контролів, регламенти
Документація	Опис усіх процесів та процедур	Регламенти, інструкції, протоколи
Навчання персоналу	Підвищення обізнаності й компетенцій	Плани, графіки, сертифікати
Моніторинг	Виявлення відхилень та інцидентів	Журнали подій, звіти SIEM
Аудит	Незалежна оцінка відповідності системи	Акт аудиту, список невідповідностей

Структурні компоненти СМІБ складають багаторівневу й інтегровану систему, яка забезпечує ефективне управління інформаційною безпекою в організації. Вони охоплюють політику, ризик-менеджмент, контрольні заходи, документообіг, ролі й відповідальність, навчання, моніторинг, аудит, реагування на інциденти та постійне вдосконалення. Їхнє узгоджене функціонування створює надійне середовище для захисту інформаційних активів відповідно до регуляторних вимог і стандартів [13].

Модель PDCA (Plan–Do–Check–Act) є основою функціонування системи менеджменту інформаційної безпеки і передбачає безперервне вдосконалення через чотири взаємопов'язані етапи. Її використання забезпечує структурований підхід до розробки, впровадження, перевірки та оновлення заходів безпеки. На етапі «Планування» (Plan) визначається політика інформаційної безпеки, встановлюються цілі, формуються вимоги до ресурсів і процедур. У межах цього етапу проводиться ідентифікація інформаційних активів, аналіз загроз, вразливостей та оцінка ризиків. Результатом є звіт про оцінку ризиків і план управління ними. Визначаються ролі, повноваження, відповідальність, межі дії системи та критерії оцінювання ефективності. Також готується план впровадження контрольних заходів, що відповідають виявленим ризикам. Цей етап є критичним, оскільки помилки у плануванні призводять до неефективної реалізації наступних дій.

Другий етап – «Реалізація» (Do) – полягає у впровадженні політики, процедур, інструментів і заходів, визначених на етапі планування. На цьому етапі вводяться в дію регламенти доступу до інформаційних ресурсів, встановлюється необхідне програмне забезпечення, проводиться навчання персоналу, оновлюються фізичні та логічні засоби контролю доступу. Здійснюється інтеграція заходів безпеки у повсякденну діяльність організації. Важливо, щоб усі працівники були ознайомлені з новими правилами та мали доступ до відповідної документації. Результати впровадження фіксуються для подальшого аналізу та коригування. Водночас впроваджуються механізми моніторингу подій безпеки, які забезпечують накопичення інформації для наступного етапу

контролю [14].

Третій етап – «Перевірка» (Check) – включає моніторинг і аналіз результатів реалізації заходів. На цьому етапі здійснюється перевірка відповідності фактичного стану інформаційної безпеки запланованим показникам. Проводяться внутрішні аудити, аналізуються журнали подій, тестуються контрольні механізми, збираються відгуки користувачів. Також порівнюються поточні ризики з початковою оцінкою, що дозволяє визначити ефективність реалізованих заходів. Здійснюється аналіз інцидентів, виявляються причини відхилень, збираються докази щодо дотримання політик. Визначаються слабкі місця, неефективні процеси та можливі напрями покращення. Результати перевірки оформлюються у вигляді звітів, які стають основою для прийняття управлінських рішень.

Останній етап – «Коригування» (Act) – спрямований на вдосконалення СМІБ на основі результатів перевірок. У разі виявлення невідповідностей або інцидентів вживаються коригувальні й попереджувальні дії. Це може включати оновлення політик, вдосконалення процедур, впровадження нових технічних рішень, повторне навчання персоналу, а також перегляд методик оцінки ризиків. На цьому етапі відбувається адаптація СМІБ до змін у законодавстві, вимогах замовників, структурі організації або зовнішніх загрозах. Крім того, формуються нові цілі, що враховують попередній досвід і поточні потреби. Етап коригування є завершенням поточного циклу PDCA і водночас початком нового, що забезпечує безперервне вдосконалення системи [15].

Життєвий цикл СМІБ за моделлю PDCA не є одноразовою дією, а безперервним процесом. Цей підхід дозволяє організації підтримувати систему у актуальному стані, оперативно реагувати на зміну умов і загроз, а також постійно підвищувати рівень захисту. Застосування моделі PDCA також спрощує проходження сертифікацій за стандартами ISO/IEC 27001, оскільки вона повністю відповідає його логіці. Успішне впровадження цієї моделі потребує не лише технічних знань, а й високого рівня організаційної культури, підтримки з боку керівництва, мотивації працівників і чітко визначених процесів взаємодії

між підрозділами. Це дає змогу сформувати ефективну, адаптивну і стійку до загроз систему управління інформаційною безпекою, здатну відповідати сучасним регуляторним вимогам і викликам цифрового середовища [16].

Таблиця 1.4

Опис етапів життєвого циклу СМІБ за PDCA

Етап	Основні дії	Очікуваний результат
Plan	Визначення політики ІБ, аналіз ризиків, постановка цілей	Затверджена політика, план впровадження
Do	Реалізація заходів безпеки, навчання персоналу, інтеграція контролів	Функціонуючі заходи, проінформований персонал
Check	Аудити, моніторинг, аналіз ефективності	Звіти про відповідність, виявлені невідповідності
Act	Коригувальні дії, оновлення політик, планування покращень	Вдосконалена система, нові цілі

1.2 Міжнародні стандарти та нормативно-правові акти у сфері ІБ

Основу міжнародного підходу до управління інформаційною безпекою становить серія стандартів ISO/IEC 27000, серед яких центральним є ISO/IEC 27001. Остання редакція 27001:2022 встановлює вимоги до створення, впровадження, підтримки й постійного вдосконалення системи управління інформаційною безпекою на базі ризик-орієнтованого підходу . Стандарт визначає структуру документації, процедури оцінки ризиків та класифікації активів, а також 10 клауза-хабів, зокрема «Планування», «Підтримка», «Оцінка ефективності» та «Удосконалення» . Додаток А містить 93 заходи контролю, що згруповані за чотирма категоріями: організаційні, людські, фізичні та технічні.

Паралельно з ISO/IEC 27001 застосовується ISO/IEC 27002 як практичне керівництво щодо вибору та впровадження контролів, що співвідноситься з

Додатком А. Остання редакція ISO/IEC 27002:2022 узгоджена з оновленим Annex A стандарту 27001, включаючи нові напрямки, такі як розвідка загроз, безпека хмарних сервісів, моніторинг фізичної безпеки, secure coding та data leakage prevention. Ці доповнення дозволяють адаптувати СМІБ до сучасних технологічних викликів [17].

ISO/IEC 27701 є розширенням 27001/27002 і присвячене управлінню персональними даними (PII). Стандарт вводить поняття Privacy Information Management System (PIMS) і пропонує контролі для організацій-контролерів і процесорів даних з урахуванням GDPR. Цей стандарт допомагає інтегрувати вимоги захисту даних у загальну інформаційну безпеку організації і забезпечує можливість сертифікації.

Крім ISO-стандартів, у міжнародній практиці застосовуються й інші моделі. NIST Cybersecurity Framework широко використовується в приватному секторі, особливо в США, і пропонує структуру для ідентифікації, захисту, виявлення, реагування й відновлення після інцидентів . У Європейському Союзі діє директива NIS2, що встановлює вимоги до кібербезпеки для операторів критичної інфраструктури – включаючиincident reporting та cybersecurity governance – ефективно уніфікуючи підходи держав-членів . Акти Digital Operational Resilience Act (DORA) та Cyber Resilience Act (CRA) встановлюють вимоги до стійкості інформаційної інфраструктури і розробки безпечного програмного забезпечення відповідно [18].

Таблиця 1.5

Порівняльна таблиця міжнародних підходів

Критерій	**ISO/IEC 27001:2022**	**NIST Cybersecurity Framework (CSF)**	**NIS2 Directive (EU)**	**DORA / CRA (EU)**
Тип документу	Міжнародний стандарт	Методологічна рамка (гайдлайн)	Європейська директива	Європейські регламенти
Ціль	Створення СМІБ на основі ризик-орієнтованого підходу	Управління кіберризикам и на рівні організацій	Гармонізація вимог кібербезпеки для операторів критичних послуг	Підвищення кіберстійкості фінансових/цифрових продуктів

Продовження таблиці 5

Цільова аудиторія	Будь-яка організація (публічна/приватна)	Переважно приватний сектор (США)	Оператори критичної інфраструктури, цифрові сервіси	Фінансові установи, постачальники ПЗ/ІТ-послуг
Обов'язковість	Добровільна (але може бути вимогою партнерів чи законодавства)	Добровільна (рекомендована урядом США)	Обов’язкова для країн-членів ЄС	Обов’язкова в ЄС
Основні розділи / функції	10 клауза-хабів + Annex A (93 контролі)	5 функцій: Identify, Protect, Detect, Respond, Recover	Governance, Risk Management, Incident Reporting	ICT Risk Management, Operational Resilience, Threat Intelligence
Контрольні заходи	Annex A: 4 категорії (організаційні, технічні тощо)	Каталоги контрольних заходів по кожній функції	Загальні вимоги + технічні/організаційні заходи	Деталізовані вимоги до тестування, реєстрації, звітності
Інцидент-менеджмент	Присутній (частина Annex A)	Окрема функція “Respond”	Чіткі строки повідомлення про інцидент (24 години)	Жорсткі вимоги до репортингу інцидентів
Аудит / сертифікація	Сертифікація можлива (ISO 27001)	Немає офіційної сертифікації	Національні органи проводять моніторинг	Регулятори контролюють дотримання правил
Зв'язок з GDPR / конф. даними	Частково, розширено через ISO/IEC 27701	Побічно (опціонально)	Визнає важливість відповідності GDPR	Безпека персональних і фінансових даних як вимога
Гнучкість впровадження	Висока (адаптується до організації)	Дуже висока (framework-based)	Середня (директива – національна адаптація)	Низька – регламент із прямою дією
Фокус на хмару / сучасні технології	Частково (через 27002:2022)	Є оновлення у версіях 2.0+	Немає прямого акценту	Прямі вимоги до постачальників ПЗ, хмар, API, ланцюга постачання

GDPR регламентує обробку персональних даних у ЄС і має «безпеку за замовчуванням» як один із ключових принципів. Вимагає технічних і організаційних заходів захисту, оцінки ризиків, реєстрації порушень та документального підтвердження відповідності GDPR. Організації зобов’язані інформувати регулятора у випадку порушення протягом 72 годин, інакше

застосовуються штрафи до 20 млн € або 4 % річного обороту.

Окремо згадуються Digital Services Act і Digital Markets Act, які вводять вимоги до прозорості, модерації алгоритмів і захисту неповнолітніх, а також AI Act – майбутній європейський закон про регулювання штучного інтелекту.

В українському законодавчому просторі головною є Закон України «Про основні засади забезпечення кібербезпеки України», що визначає поняття, принципи, суб'єктів і завдання державної кібербезпеки . Закон покладає обов’язки щодо захисту державних інформаційних ресурсів та визначає координацію між органами державної влади. Додаткові правила–підзаконні акти Служби спеціального зв’язку (СЗЗІ)–регламентують захист телекомунікацій, криптозасоби (регламент затверджено у 2007-2008 рр.) . Також існують норми щодо класифікації інформаційних систем критичної інфраструктури та порядок оцінки їхньої кіберзахищеності (постанови Кабміну № 563/943/1109/1176) [19] .

Закон «Про захист персональних даних» встановлює принципи обробки, зобов’язує офіційні організації повідомляти про порушення, передбачає адміністративну та кримінальну відповідальність (штрафи від 170 до 34 000 грн) . Закон «Про електронні довірчі послуги», «Про електронні документи», «Про інформацію», «Про телекомунікації» також містять норми щодо захисту інформації, зокрема зобов’язують організації забезпечувати технічний захист, зберігання електронних підписів, публічність інформації [20].

НБУ як регулятор фінансового сектора видає технічні регуляції щодо кібербезпеки банків, зокрема з питань управління ризиками, аудитів, організації SOC/SIEM, інформування про інциденти. Аналогічний підхід застосовують регулятори у сфері енергетики та критичної інфраструктури.

Важливим нормативним моментом є прийняття постанови 11 лютого 2025 року про встановлення порядку надання хмарних і дата-центрових послуг для держорганів, що передбачає вимоги щодо захисту держінформації, договірних стандартів і відповідальності постачальників .

Легальний фреймворк СМІБ – це поєднання міжнародних стандартів і національних нормативів, орієнтованих на ризик-орієнтований підхід,

відповідність найкращим практикам і технологічну адаптивність. Впровадження ISO/IEC серії, NIS2 та місцевих законів вимагає належного узгодження політик, регулярних аудитів, тренінгів персоналу та адаптивної документації. Сертифікація за 27001 та 27701 створює довіру до організації, дозволяє системно управляти ризиками та захистити інформацію відповідно до регулятивних очікувань [21].

1.3 Огляд методів оцінювання відповідності СМІБ регуляторним вимогам

Оцінювання відповідності системи менеджменту інформаційної безпеки СМІБ регуляторним вимогам є складним процесом, що включає в себе аналіз, перевірку, тестування та документування практик, політик і технологічних рішень, які організація застосовує для захисту інформації. Така оцінка проводиться з метою встановлення, наскільки ефективно організація дотримується вимог чинного законодавства, галузевих стандартів, внутрішніх політик, а також вимог замовників або партнерів. Методи оцінювання відповідності відрізняються за своєю глибиною, спрямованістю, а також підходами до виявлення та документування невідповідностей.

Одним із базових методів оцінювання відповідності є аудит інформаційної безпеки. Це формалізований процес, під час якого перевіряються процеси, документи, технічні засоби та людські ресурси на предмет відповідності заздалегідь визначеним критеріям. Такий аудит може бути внутрішнім або зовнішнім. Внутрішній аудит проводиться власними фахівцями організації або найманими консультантами й часто має на меті підготовку до зовнішнього аудиту чи сертифікації. Зовнішній аудит зазвичай здійснюється незалежною організацією з відповідною акредитацією. Основні етапи аудиту включають планування, проведення перевірок, збір доказів, формування висновків та підготовку звіту. На цьому етапі використовуються такі методи, як інтерв’ювання персоналу, аналіз документів, спостереження за виконанням

процедур, технічне тестування захисних механізмів [22].

Важливе місце серед методів оцінювання займає аналіз відповідності політик і процедур СМІБ вимогам стандартів, таких як ISO/IEC 27001, NIST SP 800-53, GDPR, HIPAA, PCI DSS та ін. Такий аналіз передбачає вивчення документів системи управління безпекою, оцінювання їхньої структури, змісту та актуальності, а також перевірку того, чи втілені задекларовані політики в реальних процесах. Наприклад, для оцінювання відповідності вимогам ISO/IEC 27001 перевіряється наявність контексту організації, визначення ризиків, планів обробки ризиків, процедур моніторингу та вдосконалення системи. Особлива увага приділяється доказовій базі: кожен пункт стандарту повинен бути підкріплений політикою, інструкцією, протоколом або журналом подій.

Оцінювання відповідності також здійснюється шляхом тестування технічних засобів інформаційної безпеки. Це включає сканування вразливостей, тестування на проникнення, аналіз конфігурацій систем, перевірку логування та моніторингу, а також симуляцію інцидентів. Ці методи дозволяють оцінити фактичний рівень захисту та ефективність впроваджених заходів. Наприклад, в рамках перевірки відповідності вимогам GDPR можуть перевірятись налаштування систем зберігання персональних даних, доступи до них, журналювання дій користувачів, а також процедури видалення або передачі даних на запит суб’єкта персональних даних.

Ще одним важливим методом є оцінка ризиків, яка є ключовим компонентом практично будь-якої СМІБ. В процесі оцінювання відповідності перевіряється, чи проведена формалізована оцінка ризиків, яким чином обрані критерії для їх оцінювання, як здійснюється ранжування загроз, і чи впроваджено відповідні заходи для їх мінімізації. Також оцінюється ефективність методик, що використовуються для повторного перегляду ризиків. Відповідність регуляторним вимогам у цьому аспекті передбачає не лише формальну наявність матриць ризиків, але і доведення зв’язку між результатами оцінки та заходами, реалізованими в організації [23].

Метод опитування та анкетування персоналу також часто використовується для перевірки обізнаності співробітників щодо політик інформаційної безпеки, правил поводження з інформацією, сценаріїв реагування на інциденти. Такі оцінки особливо важливі у відповідності до стандартів, що висувають вимоги до навчання персоналу та підвищення його обізнаності (наприклад, ISO/IEC 27001, NIST CSF). Анкетування дозволяє отримати кількісні показники, на основі яких можливо оцінити ефективність програм навчання, а також виявити потенційні слабкі місця в системі безпеки, що пов'язані з людським фактором [24].

Ще один метод – моделювання процесів. Він передбачає побудову моделей основних бізнес-процесів, пов'язаних із обробкою інформації, та їхню перевірку на відповідність вимогам захисту. Такий підхід дозволяє не лише оцінити формальну відповідність політик і процедур, але й встановити, наскільки інтегровані вимоги інформаційної безпеки у повсякденну діяльність організації. Наприклад, у процесі обробки запитів користувачів до служби підтримки може бути змодельований шлях доступу до даних, права користувачів, способи автентифікації, процедури фіксації запитів. Всі ці елементи мають відповідати як внутрішнім політикам, так і зовнішнім вимогам, таким як ISO 27701 або GDPR.

Метод аналізу журналів подій і логів дозволяє перевірити, наскільки системи організації здатні забезпечити прозорість та контроль над діями користувачів і процесів. Особливо це важливо у випадках, коли регуляторні вимоги містять положення про обов'язкову реєстрацію подій безпеки, спроб доступу, змін конфігурацій, виявлення інцидентів. Оцінюється не лише наявність логів, але і їхній обсяг, цілісність, доступність для аналізу, механізми зберігання та архівування, а також налаштування систем SIEM, якщо вони використовуються. На практиці важливо, щоб журналювання було охоплювальним і відповідало нормам з точки зору захисту персональних даних і вимог доступу до таких журналів [25].

Методи контрольного аналізу постачальників і зовнішніх партнерів дозволяють перевірити, наскільки зовнішні учасники інформаційного обміну

відповідають вимогам безпеки, що застосовуються в організації. Це особливо важливо в контексті відповідності вимогам таких стандартів, як ISO/IEC 27036, які регулюють взаємодію з третіми сторонами. Оцінювання може включати перевірку договорів, угод про рівень обслуговування (SLA), політик щодо безпеки постачальників, а також результати аудитів або сертифікацій постачальників. Також може перевірятися виконання вимог щодо звітування про інциденти, доступу до даних, захисту каналів передачі інформації [26].

У сфері кібербезпеки поширеним є застосування методів автоматизованої оцінки відповідності, що базуються на використанні спеціалізованих програмних засобів. До таких засобів належать системи аналізу відповідності конфігурацій (наприклад, Tenable Nessus, Qualys, Rapid7 InsightVM), які дозволяють автоматично перевіряти системи на наявність відомих вразливостей, невірних налаштувань, незахищених сервісів тощо. Ці інструменти можуть бути інтегровані в CI/CD-процеси і виконувати постійний моніторинг відповідності. Також доцільно використовувати засоби для перевірки відповідності хмарної інфраструктури, наприклад, AWS Config або Microsoft Defender for Cloud, які дозволяють оцінити налаштування середовищ за допомогою попередньо визначених шаблонів відповідності.

Оцінювання відповідності вимагає також застосування методів аналізу інцидентів і розслідувань. Після настання інциденту перевіряється, наскільки ефективно були реалізовані процедури реагування, фіксації, локалізації, повідомлення відповідних сторін, збереження цифрових доказів, усунення наслідків. Якщо організація заявляє про відповідність вимогам, що стосуються управління інцидентами (наприклад, ISO/IEC 27035), вона має мати відповідні плани реагування, журнал подій, систему інформування зацікавлених сторін та проведену післяінцидентну оцінку. Фактичні дії мають бути узгоджені з планами і стандартами [27].

Поряд із класичними методами дедалі більшого поширення набуває застосування maturity models – моделей зрілості системи безпеки. Такі моделі, як COBIT, CMMI for Security або NIST Cybersecurity Framework Implementation

Tiers, дозволяють провести самооцінку або зовнішню оцінку рівня зрілості системи, включаючи компоненти відповідності. Модель зрілості надає змогу визначити, чи здійснюються заходи безпеки на реактивному, контрольованому чи оптимізованому рівні. Такий підхід особливо ефективний для довгострокового стратегічного планування вдосконалення СМІБ.

У деяких випадках методи оцінки включають проведення бенчмаркінгу, тобто порівняння практик організації з галузевими найкращими практиками або з конкурентами. Бенчмаркінг дозволяє визначити, чи відповідає система управління безпекою сучасним очікуванням і трендам, навіть якщо формально вимоги дотримані. Наприклад, у фінансовому секторі можуть оцінюватися практики багатофакторної автентифікації, процедур управління ключами, або політик резервного копіювання у порівнянні з передовими банками [28].

Значущим також є застосування правового аналізу, що дозволяє перевірити відповідність локальному законодавству у сфері захисту інформації, конфіденційності, обробки персональних даних, транскордонної передачі інформації. Це включає аналіз нормативно-правових актів, судової практики, висновків регуляторних органів. Важливо, щоб організація мала внутрішні юридичні експертизи або контракти з відповідними консультантами, що дозволяє оперативно адаптувати політики та процедури до змін у законодавстві.

Загалом ефективна оцінка відповідності СМІБ регуляторним вимогам базується на поєднанні кількох методів – документального аналізу, технічного тестування, спостереження, інтерв’ювання, моделювання, аудитів та автоматизованого моніторингу. Комплексний підхід дозволяє досягти максимальної об’єктивності та достовірності результатів, на основі яких можна не лише підтвердити відповідність, але й виявити сфери для вдосконалення, підвищити рівень безпеки, а також забезпечити довіру з боку партнерів, клієнтів та регуляторів [29].

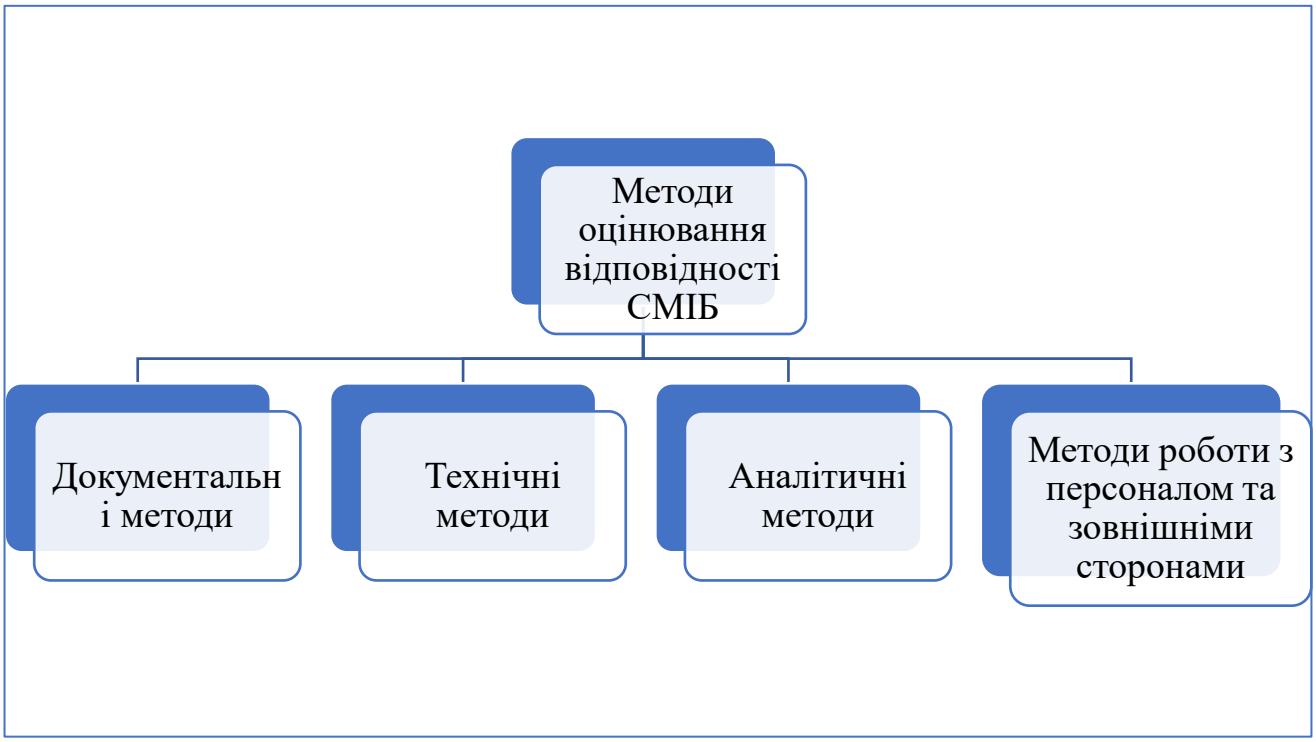

Рис. 1.3 Класифікація методів оцінювання відповідності

Висновки до розділу 1

У першому розділі було здійснено комплексний аналіз фундаментальних аспектів СМІБ та її взаємозв'язку з міжнародними стандартами й регуляторними вимогами. Розгляд поняття СМІБ дозволив сформувати цілісне уявлення про її структуру, основні елементи, принципи функціонування, а також визначити її роль як інструменту забезпечення безперервного управління ризиками, пов'язаними з інформаційними активами. Особливу увагу приділено циклічному підходу PDCA (Plan-Do-Check-Act), який є базовою моделлю управління для забезпечення стійкості та постійного вдосконалення СМІБ.

Було досліджено нормативну основу, що регламентує вимоги до систем інформаційної безпеки. Зокрема, розглянуто провідні міжнародні стандарти, такі як ISO/IEC 27001, ISO/IEC 27002, NIST SP 800-53, а також регуляторні акти, включно з GDPR, ЗУ «Про захист персональних даних» та іншими нормативами, що визначають вимоги до обробки, зберігання й захисту інформації. Це

дозволило окреслити нормативне поле, в межах якого функціонує СМІБ, та визначити основні напрямки її адаптації під законодавчі вимоги.

Розглянуто методи оцінювання відповідності СМІБ регуляторним вимогам. Проаналізовано різноманітні підходи – від документального аудиту та технічного тестування до аналізу ризиків, використання моделей зрілості та автоматизованих інструментів оцінки. Такий огляд дав змогу сформувати уявлення про практичні механізми, за допомогою яких організації можуть контролювати ефективність функціонування СМІБ, виявляти невідповідності, адаптувати захисні заходи до змін у середовищі загроз і забезпечувати постійну відповідність законодавчим нормам і галузевим стандартам.

Розділ 2 ПРАКТИЧНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ВІДПОВІДНОСТІ СМІБ РЕГУЛЯТОРНИМ ВИМОГАМ

2.1 Виявлення ризиків невідповідності нормативним вимогам

Виявлення ризиків невідповідності нормативним вимогам є критично важливою складовою процесу управління інформаційною безпекою в сучасних організаціях. У контексті динамічного нормативно-правового поля, що постійно змінюється під впливом нових викликів, технологій та загроз, здатність своєчасно ідентифікувати потенційні порушення вимог є запорукою стійкості підприємства, мінімізації фінансових втрат і збереження репутації. Виявлення таких ризиків передбачає систематичний аналіз внутрішніх процесів, процедур, технічних засобів і організаційної структури на предмет відповідності чинним законодавчим актам, міжнародним стандартам, галузевим нормам та угодам з контрагентами.

Процес виявлення ризиків невідповідності передбачає декілька послідовних етапів, серед яких ключову роль відіграє вивчення нормативного поля. До нього належать закони, регламенти, постанови, стандарти і політики, що регулюють обробку персональних даних, забезпечення конфіденційності, доступу до інформаційних систем, зберігання логів, звітності з інцидентів, проведення аудитів, сертифікацію систем безпеки, ліцензійні вимоги, вимоги до криптографічного захисту та інші сфери. При цьому джерела вимог можуть бути як зовнішніми (державні органи, міжнародні організації, партнери), так і внутрішніми (власні політики компанії, контракти, етичні кодекси). Збір і класифікація цих вимог є основою для подальшого зіставлення з поточними практиками організації [30].

Після формування повного переліку релевантних нормативних вимог проводиться аудит на відповідність – аналіз того, як наявні процеси, системи та процедури відповідають цим вимогам. Часто для цього використовуються контрольні списки (checklists), складені на основі стандартів типу ISO/IEC 27001,

NIST, GDPR, PCI DSS або локальних актів. Наприклад, якщо норматив вимагає логування доступу до критичних ресурсів, перевіряється, чи є система збору логів, чи включено відповідні функції, чи здійснюється моніторинг та аналіз подій. Якщо мова йде про захист персональних даних, досліджується, як здійснюється обробка таких даних, чи є механізми отримання згоди, обмеження доступу, зберігання та знищення [31].

Одним з ефективних підходів до виявлення ризиків є методологія GAP-аналізу, коли на основі вимог формується цільовий (бажаний) стан, і проводиться порівняння з поточним станом системи. Всі виявлені розбіжності (GAPи) класифікуються як потенційні ризики невідповідності. Важливим є не лише виявлення самих невідповідностей, а й оцінка їх критичності – тобто ймовірності реалізації загрози та впливу на організацію. Наприклад, відсутність шифрування для передачі чутливої інформації через Інтернет є висококритичним ризиком у контексті вимог GDPR, тоді як відсутність регулярного навчання персоналу може бути середнім або низьким ризиком, залежно від масштабу компанії та її ролі в ланцюзі обробки даних.

Важливим аспектом є аналіз практик третіх сторін, що взаємодіють з організацією. Якщо певні функції, наприклад, обробка персональних даних або технічне обслуговування інфраструктури, передано на аутсорсинг, необхідно перевірити відповідність цих постачальників зовнішнім нормативним вимогам, а також положенням договорів. Контракти повинні містити пункти про відповідальність сторін, механізми контролю та аудиту, процедури повідомлення про інциденти, обмеження доступу до даних та вимоги до технічного захисту.

Ключовою частиною процесу є ідентифікація ризиків, пов’язаних із змінами у законодавстві або впровадженням нових вимог. Регулярний моніторинг змін у нормативному середовищі – обов’язковий елемент забезпечення відповідності. Йдеться не лише про офіційні публікації та роз’яснення регуляторів, а й про професійні аналітичні ресурси, консультації з юридичними службами або зовнішніми експертами. Наприклад, запровадження

нової директиви ЄС щодо кіберстійкості може спричинити необхідність перегляду внутрішніх політик інформаційної безпеки, зміну архітектури мережі або впровадження додаткових процедур інцидент-менеджменту.

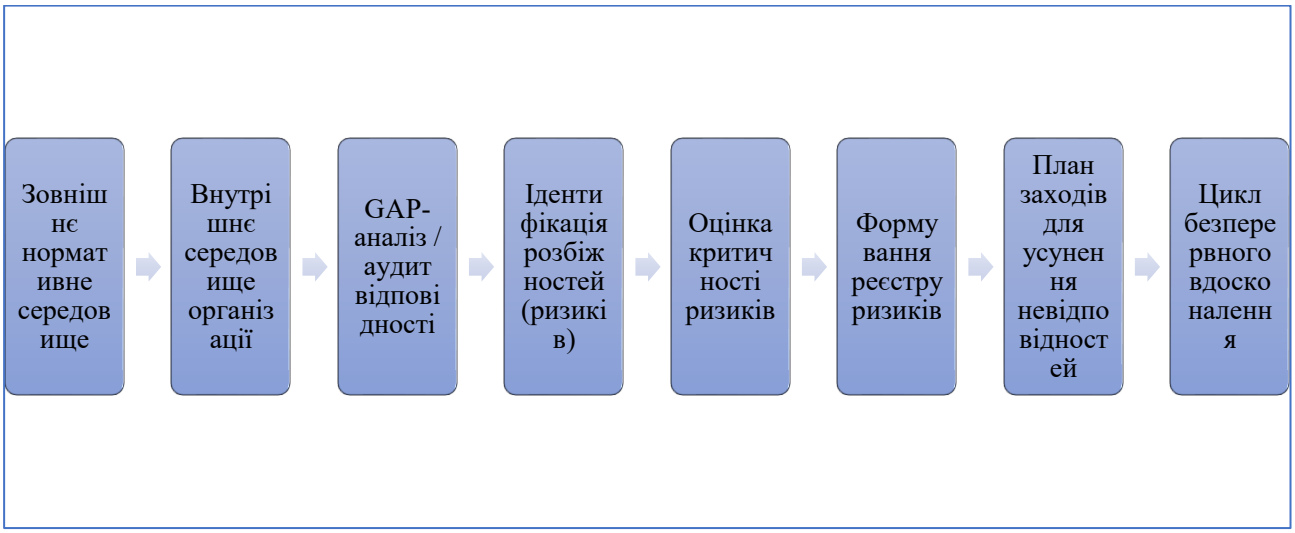

Рис. 2.1 Схема процесу виявлення ризиків невідповідності нормативним вимогам

Також важливо враховувати внутрішні організаційні зміни як джерело ризиків невідповідності. Зміна структури управління, масштабування діяльності, впровадження нових інформаційних систем, оновлення політик, міграція на хмарні сервіси або відкриття нових ринків може призвести до втрати контролю над дотриманням нормативних вимог. Наприклад, під час розгортання нової CRM-системи, у яку імпортуються особисті дані клієнтів, необхідно перевірити, чи є можливість обмеження доступу за ролями, логування дій користувачів, чи реалізовано механізм видалення даних за запитом. Якщо цього не зробити, організація наражається на ризик порушення норм захисту персональних даних.

У складних IT-системах одним з найчастіших джерел ризику є невідповідність налаштувань безпеки технічних компонентів вимогам стандартів. Це може стосуватися неправильної конфігурації мережевих екранів, застарілих протоколів шифрування, відкритих портів, відсутності оновлень безпеки, недостатніх політик автентифікації. Для виявлення таких невідповідностей застосовуються технічні засоби перевірки конфігурацій, сканери вразливостей, системи моніторингу подій, SIEM, аудит логів. Дані з цих

джерел повинні інтегруватися у загальну модель управління ризиками для оцінки, наскільки технічна невідповідність може призвести до юридичних наслідків [32].

Особливу увагу слід приділяти документуванню процесів – відсутність належним чином оформлених політик, інструкцій, журналів і звітів про аудит також є ризиком невідповідності, навіть якщо самі процеси функціонують коректно. Регулятори вимагають не лише наявності механізмів захисту, а й підтвердження їх реалізації через документацію. Це стосується, зокрема, планів реагування на інциденти, внутрішніх розслідувань, оцінок впливу на захист даних (DPIA), журналів доступу до інформації, протоколів навчання персоналу.

Оцінка ризиків невідповідності також повинна враховувати людський фактор. Недостатня обізнаність персоналу з вимогами політик безпеки, несумлінне виконання обов’язків, помилки при обробці даних – все це може спричинити порушення вимог навіть за наявності формальних механізмів контролю. Проведення навчань, іспитів, тестування на знання вимог, моделювання інцидентів і регулярна комунікація з працівниками значно знижують імовірність реалізації таких ризиків [33].

Виявлені ризики невідповідності підлягають класифікації за рівнем критичності та формалізації у вигляді реєстру ризиків. Кожному ризику має бути присвоєно унікальний ідентифікатор, описано джерело, вплив, ймовірність виникнення, поточні засоби контролю, а також запропоновано рекомендації щодо усунення або зниження ризику. На основі такого реєстру формується план управління ризиками, що передбачає впровадження технічних, адміністративних і юридичних заходів з метою забезпечення відповідності. Часто ці заходи поділяються на превентивні (навчання, політики), детективні (моніторинг, аудит), компенсуючі (резервні механізми) та коригуючі (реагування на інциденти, зміни конфігурацій).

Процес виявлення ризиків невідповідності має бути безперервним. Він вимагає регулярного перегляду політик, повторного аудиту, оновлення ризик-реєстрів, адаптації до нових вимог. Інформаційна безпека і нормативна

відповідність не є статичними станами – це постійний цикл оцінки, моніторингу, вдосконалення. Забезпечення системного підходу до виявлення ризиків невідповідності нормативним вимогам дозволяє організації не лише уникнути штрафів і санкцій, а й підвищити рівень довіри клієнтів, партнерів і суспільства до її діяльності.

2.2 Використання методів аудитів, GAP-аналізу та контролю

Використання методів аудитів, GAP-аналізу та контролю є ключовим механізмом у забезпеченні відповідності нормативним вимогам, управлінні ризиками інформаційної безпеки та впровадженні ефективної системи захисту даних в організації. Ці методи дозволяють не лише виявити існуючі проблеми й невідповідності, а й сформувати чітку картину поточного стану систем безпеки, оцінити рівень зрілості процесів, а також визначити необхідні дії для досягнення цільового стану. Їх інтеграція в практику кіберзахисту забезпечує прозорість, системність і доказову базу для прийняття управлінських рішень.

Аудит є інструментом системної перевірки процесів, систем, політик та контролів на предмет їх відповідності встановленим вимогам, стандартам і найкращим практикам. Він може бути як внутрішнім, коли перевірка здійснюється власними спеціалістами компанії, так і зовнішнім, коли її виконують незалежні експерти чи сертифікаційні органи. Аудит може охоплювати як загальну систему управління інформаційною безпекою, так і окремі її компоненти, наприклад, аудит управління доступом, аудит політик безпеки, аудит використання криптографії або аудит відповідності вимогам GDPR [34].

Під час аудиту застосовується формалізований підхід, що включає планування, визначення об’єкту перевірки, підготовку аудитора, збір доказів, аналіз даних, складання звіту та формування висновків. Аудитор використовує контрольні списки, інтерв’ю, аналіз документації, перевірку логів, тестування налаштувань, верифікацію політик і конфігурацій, технічне сканування,

перевірку журналів безпеки. Основне завдання – виявити порушення, слабкі місця, пропущені процеси, а також визначити причини цих відхилень. Наприклад, у випадку, коли внутрішня політика безпеки вимагає зміну паролів кожні 90 днів, але аудит логів показує, що це не виконується, фіксується невідповідність, її причина може полягати у неправильному налаштуванні доменних політик або в обхідних діях користувачів.

Окремо слід відзначити, що аудит – це не одноразова дія, а частина циклічного процесу. Після завершення аудиту складається детальний звіт з описом виявлених проблем, їх критичності, доказів, а також рекомендацій щодо усунення. Потім відбувається моніторинг впровадження коригувальних дій, повторна перевірка і оновлення статусу в реєстрі ризиків. У складних організаціях може застосовуватись аудит другого рівня, коли здійснюється перевірка ефективності виконаних рекомендацій. Це дозволяє не лише усунути порушення, а й переконатись у довгостроковій стабільності заходів [35].

Метод GAP-аналізу тісно пов’язаний з аудитом, однак має дещо іншу мету – визначення розриву між поточним станом системи та бажаним станом, зафіксованим у стандартах або вимогах. У практиці інформаційної безпеки це означає співставлення існуючих процесів з вимогами стандартів типу ISO/IEC 27001, NIST SP 800-53, COBIT, SOC 2, PCI DSS або внутрішніх нормативів компанії. Визначення GAPів відбувається через систематичне опитування, аналіз політик, перевірку конфігурацій, спостереження за процесами. Для кожної вимоги формується таблиця відповідності, де вказується, чи виконується вона повністю, частково або не виконується зовсім.

Результатом GAP-аналізу є матриця відповідності, де кожен пункт вимог пов’язується з поточним рівнем реалізації в організації. Наприклад, вимога “захищений доступ до вебінтерфейсу адміністратора” може мати статус “частково реалізовано”, якщо автентифікація є, але не використовується двофакторна перевірка. Така деталізація дозволяє не лише виявити проблеми, а й визначити обсяг робіт для повної відповідності. GAP-аналіз є інструментом стратегічного планування, оскільки дозволяє обґрунтувати інвестиції в

кібербезпеку, визначити пріоритетність заходів і сформувати дорожню карту розвитку системи.

Таблиця 2.1

Порівняльна характеристика аудиту, GAP-аналізу та контролю

Критерій	**Аудит**	**GAP-аналіз**	**Контроль**
Мета	Перевірка відповідності вимогам	Виявлення розривів між поточним і цільовим станом	Постійний моніторинг і управління відхиленнями
Частота проведення	Періодично (раз на рік, пів року)	Переважно одноразово або на початку проекту	Постійно або регулярно (щодня, щотижня)
Методика	Інтерв'ю, перевірка документів, тестування	Порівняння з еталоном, аналіз вимог	Автоматичний або ручний нагляд за подіями
Результат	Звіт з невідповідностями і рекомендаціями	Матриця відповідності та перелік GAPів	Виявлення інцидентів, звіт про стан системи
Інструменти	Контрольні списки, аудит-репорти	GAP-матриці, вимоги стандартів	SIEM, DLP, лог-менеджери, журнали подій
Основна роль	Незалежна перевірка	Стратегічне планування змін	Оперативне реагування на відхилення

Контроль є постійним, безперервним процесом нагляду за станом безпеки та відповідності. Це не лише перевірки в рамках аудитів, а й щоденні, щотижневі або щомісячні процедури технічного, адміністративного або процедурного моніторингу. Контроль включає як автоматизовані засоби – SIEM-системи, моніторинг журналів подій, контроль політик доступу, IDS/IPS, системи запобігання втраті даних (DLP), так і ручні процедури – аналіз логів, періодичне опитування співробітників, перевірку документів, тестування резервного

копіювання, аудит інвентаризації обладнання.

Завдання контролю – своєчасно виявляти відхилення від нормального стану, запобігати реалізації загроз, мінімізувати наслідки інцидентів. Наприклад, система контролю може автоматично фіксувати спроби входу з заблокованого облікового запису, зміну прав доступу, встановлення нового програмного забезпечення або підозрілі підключення до мережі. Всі ці події аналізуються і, залежно від критичності, передаються на розгляд відповідальним особам. Контроль дозволяє виявити не лише технічні порушення, а й організаційні – наприклад, невиконання внутрішніх регламентів, затримку з оновленням документації або відсутність звітності про інциденти [36].

Контроль може бути проактивним і реактивним. Проактивний контроль зосереджений на попередженні проблем – наприклад, регулярне тестування резервного копіювання, перевірка відповідності налаштувань політик, аудит привілеїв користувачів. Реактивний контроль активується у відповідь на подію – наприклад, аналіз журналів після виявлення інциденту або проведення службового розслідування. Обидва типи є необхідними в загальній системі захисту.

Впровадження ефективних методів аудитів, GAP-аналізу і контролю передбачає наявність формалізованих процедур, розподіл відповідальності, автоматизацію перевірок та аналітики, інтеграцію з ризик-менеджментом. Важливою частиною є ведення реєстрів аудитів, звітів GAP-аналізу, журналів перевірок і протоколів контролю. Ці документи є доказовою базою під час перевірок з боку регуляторів або судових процесів.

Особливої уваги потребує інтеграція результатів аудитів і GAP-аналізу в процес прийняття рішень. Організація має створити механізм, за яким виявлені проблеми не просто фіксуються, а перетворюються на завдання для відповідальних осіб із зазначенням строків, пріоритетів і критеріїв виконання. Це може бути реалізовано через систему управління завданнями, ризик-менеджментову платформу або інтеграцію в загальний цикл PDCA (Plan-Do-Check-Act). В ідеалі, процеси контролю й аналізу повинні не лише відповідати

вимогам, а й створювати додану вартість для бізнесу – сприяти ефективності, зниженню витрат, підвищенню довіри з боку клієнтів і партнерів.

Важливим фактором є культура безпеки в організації. Аудит, GAP-аналіз і контроль повинні сприйматись не як формальні процедури перевірки, а як інструменти розвитку та підвищення стійкості. Для цього необхідно забезпечити розуміння з боку персоналу, проводити навчання, стимулювати ініціативність, використовувати результати перевірок як основу для вдосконалення, а не для покарання. У такому середовищі методи аналізу й контролю стають частиною повсякденної практики, а не примусовим зовнішнім регламентом.

2.3 Впровадження заходів щодо покращення відповідності

Впровадження заходів щодо покращення відповідності системи менеджменту інформаційної безпеки (СМІБ) регуляторним вимогам є ключовим етапом забезпечення сталої кіберстійкості підприємства та формування довіри з боку партнерів, клієнтів і державних органів. Цей процес охоплює широке коло дій, починаючи від аналізу вхідних вимог і завершуючи верифікацією впроваджених змін. Успішне впровадження заходів потребує інтеграції технічних, організаційних, правових та управлінських компонентів, координації з внутрішніми і зовнішніми стейкхолдерами, а також чіткого документального супроводу кожного етапу [37].

Першим кроком впровадження заходів є деталізація і трансляція зовнішніх регуляторних вимог у внутрішнє нормативне поле організації. Це може включати вимоги міжнародних стандартів, таких як ISO/IEC 27001, 27002, 27701, вимоги до обробки персональних даних згідно з GDPR, локальні закони про захист критичної інфраструктури, а також галузеві регламенти, наприклад, NIS2 для операторів важливих послуг. На цьому етапі юридичний та інформаційно-безпековий підрозділи спільно працюють над тим, щоб уніфікувати ці вимоги та визначити їх значення для бізнес-процесів організації. Важливо створити реєстр регуляторних вимог, який буде постійно оновлюватися, а також визначити

відповідальних осіб за дотримання кожної з них.

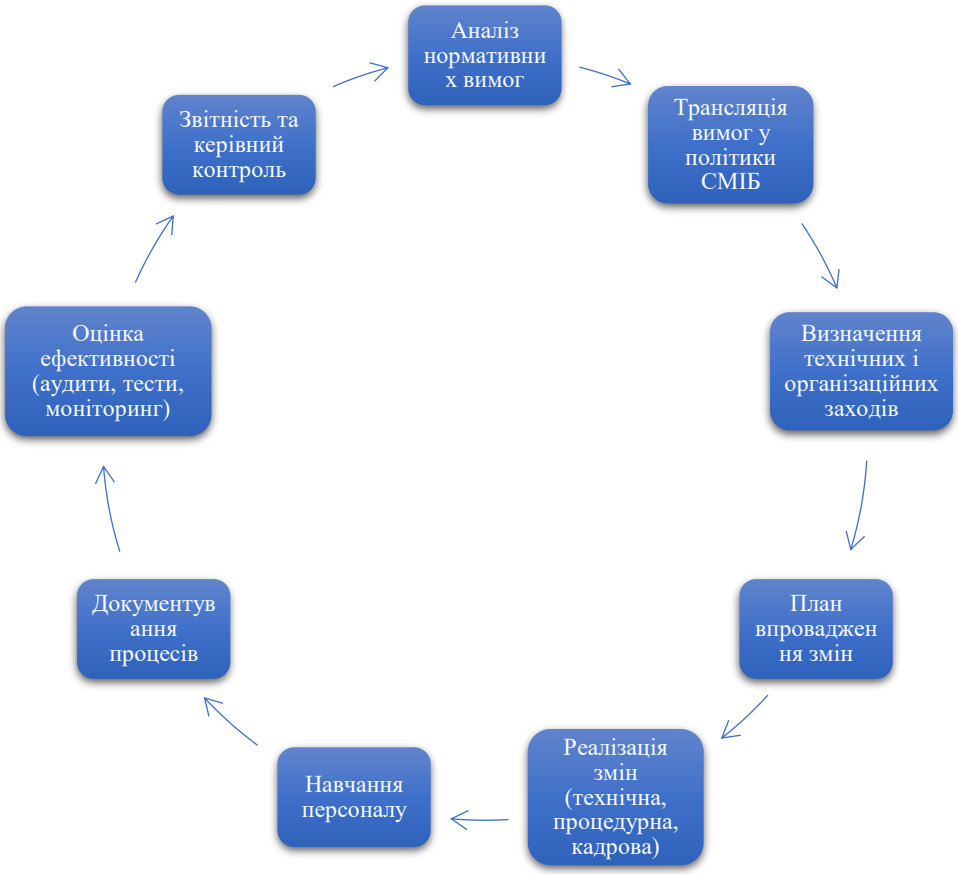

Рис. 2.2 Етапи впровадження заходів відповідності СМІБ регуляторним вимогам

Наступним етапом є адаптація політик СМІБ до встановлених вимог. Політики безпеки мають бути не лише формально оновлені, але й відображати конкретні управлінські, технічні та процедурні рішення. Наприклад, у відповідь на вимоги про ведення реєстру інцидентів необхідно не лише створити такий реєстр, а й інтегрувати його з процесами інцидент-менеджменту, автоматизувати його ведення через систему SIEM або іншу платформу, забезпечити періодичну перевірку записів і формалізувати вимоги до їх архівування. Якщо законодавство вимагає зберігання журналів доступу до інформаційних систем протягом 12 місяців, організація має переглянути політику логування, оцінити обсяг необхідного сховища, налаштувати політики retention у відповідних системах і забезпечити контроль за їх цілісністю [38].

Одним із найважливіших блоків є впровадження технічних заходів відповідності. Це охоплює налаштування та використання засобів

аутентифікації, криптографії, журналювання, контролю доступу, ізоляції середовищ, моніторингу та виявлення аномалій. Зокрема, для відповідності вимогам до захисту персональних даних може знадобитися реалізація шифрування на рівні зберігання та передачі даних, контроль доступу до реєстрів ПД, ведення журналів активності адміністраторів, а також функція псевдонімізації. Якщо регулятор вимагає забезпечення можливості виявлення витоку даних, організація має впровадити DLP-системи, налаштувати політики контент-фільтрації, верифікувати маршрути поширення документів та провести тестування засобів запобігання несанкціонованій передачі файлів.

Організаційні заходи включають оновлення ролей, відповідальностей і процедур. Важливо, щоб внутрішні регламенти чітко визначали, хто відповідальний за обробку інцидентів, хто проводить оцінку ризиків, хто координує взаємодію з наглядовими органами, хто забезпечує аудит відповідності. Впровадження нових вимог нерідко потребує створення нових посад, підрозділів або навіть функцій. Наприклад, введення офіцера з захисту даних (Data Protection Officer) є обов’язковим для певних категорій компаній відповідно до GDPR. Всі зміни мають бути задокументовані, доведені до відома працівників і закріплені у посадових інструкціях [39].

Ключову роль у впровадженні заходів відіграє підвищення обізнаності персоналу. Жодна політика чи технічний засіб не будуть ефективними, якщо працівники не розумітимуть своїх обов’язків, не будуть обізнані про загрози, не знатимуть, як діяти в разі інциденту або підозри на витік. Тому організація має впровадити програму навчання і підвищення кваліфікації з урахуванням вимог регуляторів. Це може бути обов’язкове первинне навчання при прийомі на роботу, регулярні оновлення знань, тематичні тренінги, розсилки, навчальні відео, тестування знань. Також доцільно проводити моделювання інцидентів, фішинг-тести, навчання за сценаріями реальних подій.

Іншим важливим аспектом є документування процесу впровадження. Організація має створювати і підтримувати у актуальному стані всі необхідні документи, які підтверджують відповідність вимогам: політики, процедури,

протоколи перевірок, звіти про навчання, результати аудитів, акти впровадження технічних змін. Особливо критичним є забезпечення простежуваності рішень — коли на вимогу можна пред'явити, які дії були виконані, коли, ким і з якої причини. Для цього часто використовуються системи управління документацією, системи контролю версій, електронні реєстри.

Оцінка ефективності впроваджених заходів має здійснюватися систематично. Це може включати регулярні внутрішні аудити, незалежну перевірку відповідності, ревізію політик, аналіз результатів контролю, опитування персоналу, технічне тестування, зокрема, пентести. Результати цієї оцінки слугують підставою для уточнення заходів, їх удосконалення або корекції. Якщо під час оцінки виявлено, що захід формально впроваджений, але не працює (наприклад, процедура повідомлення про інциденти існує, але ніхто нею не користується), організація має ініціювати перегляд підходу: від зміни методики навчання до технічної автоматизації повідомлень [40].

Процес впровадження має бути інтегрований у цикл постійного вдосконалення СМІБ. Це означає, що організація не повинна обмежуватись разовими діями у відповідь на нові вимоги, а має створити механізм постійного моніторингу змін у зовнішньому середовищі, регулярного оновлення політик, проведення GAP-аналізу і коригування системи управління. У рамках PDCA-циклу впровадження заходів — це частина фази "Do", що повинна узгоджуватись із фазами "Plan" (оцінка вимог, ризиків), "Check" (оцінка ефективності, аудит) і "Act" (коригувальні дії). Такий підхід дозволяє забезпечити не лише відповідність, а й сталість у підтриманні цієї відповідності.

Особливу увагу слід звертати на впровадження засобів обліку та звітності. Багато регуляторів вимагають регулярного подання звітів про інциденти, оцінку ризиків, реалізацію заходів захисту, аудитів, результати тестувань. Тому організація має впровадити централізовану систему звітності, яка дозволяє швидко зібрати потрібну інформацію, сформувати звіт у відповідному форматі і надати його у встановлений термін. Це може бути спеціалізована платформа GRC (Governance, Risk and Compliance), система автоматизованої звітності або

модуль у SIEM, що дозволяє агрегувати дані з різних джерел.

Не менш важливим є врахування впливу впроваджених заходів на бізнес-процеси. Деякі вимоги можуть суттєво змінити логіку роботи підрозділів, збільшити час на виконання операцій, викликати опір персоналу. Тому на етапі планування заходів необхідно проводити оцінку впливу (impact assessment), балансувати між вимогами безпеки і зручністю користувача, а також проводити обґрунтування змін перед керівництвом. У деяких випадках доцільно застосовувати підхід “privacy by design” або “security by design”, коли вимоги впроваджуються на етапі проектування рішень, що дозволяє уникнути конфлікту між безпекою і продуктивністю [41].

Впровадження заходів щодо відповідності має бути прозорим і підзвітним. Керівництво організації має отримувати регулярну інформацію про статус впровадження, ключові ризики, проблеми, що виникають, і потреби в ресурсах. Це забезпечується через систему внутрішньої звітності, ключові показники ефективності (KPI), засідання наглядових комітетів з безпеки, використання дашбордів, звітів керівника з ІБ. Також необхідно налагодити механізм зворотного зв’язку, за яким працівники можуть повідомляти про недоліки, проблеми з реалізацією заходів або неочікувані наслідки змін.

Висновки до розділу 2

У другому розділі було розглянуто практичні підходи до забезпечення відповідності системи менеджменту інформаційної безпеки (СМІБ) регуляторним вимогам, що є критично важливим для гарантування кіберстійкості, правової захищеності та репутаційної надійності підприємства. Зроблено акцент на важливості виявлення ризиків невідповідності шляхом аналізу нормативно-правового середовища, оцінки впливу потенційних відхилень та формування карти ризиків, яка дозволяє систематизувати загрози, оцінити їх пріоритетність і визначити напрями для подальших дій.

Проаналізовано використання інструментів аудитів, GAP-аналізу та

механізмів контролю, які слугують основою для об’єктивної оцінки стану відповідності СМІБ. Встановлено, що періодичні аудити дозволяють виявляти не лише поточні порушення, але й системні недоліки у процесах безпеки, а GAP-аналіз допомагає визначити розриви між поточним і цільовим станом відповідності. Запровадження контрольних механізмів створює основу для безперервного моніторингу, оперативного реагування та ефективного управління змінами.

Висвітлено комплекс заходів із впровадження змін, які охоплюють оновлення політик, технічне переоснащення, підвищення обізнаності персоналу, формалізацію процедур та створення системи звітності. Окремо підкреслено важливість інтеграції цих заходів у цикл постійного вдосконалення СМІБ згідно з принципами PDCA.

Результати аналізу підтверджують, що системний, документований і контрольований підхід до забезпечення відповідності дозволяє знизити ризики регуляторних санкцій, покращити загальну ефективність СМІБ і забезпечити її сталу адаптацію до динамічних вимог зовнішнього середовища.

Розділ 3 РЕКОМЕНДАЦІЇ ЩОДО ВДОСКОНАЛЕННЯ СИСТЕМИ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1. Пропозиції щодо підвищення ефективності управління інформаційною безпекою

Підвищення ефективності управління інформаційною безпекою вимагає системного підходу, що включає як організаційні, так і технічні заходи. Насамперед необхідно забезпечити формування адаптивної моделі управління інформаційною безпекою, що дозволяє динамічно реагувати на зміни в загрозах та інформаційних технологіях. Одним з головних напрямів є побудова системи інформаційної безпеки як складової загальної системи управління підприємством, із чітким розмежуванням зон відповідальності між підрозділами та автоматизованими системами. Це передбачає інтеграцію інформаційної безпеки у всі бізнес-процеси, що дозволяє зменшити ймовірність інцидентів на ранніх стадіях.

Раціональним кроком є впровадження концепції risk-based approach — підходу на основі ризиків, що передбачає оцінку загроз відповідно до ймовірності їх реалізації та потенційних збитків. Для цього потрібно регулярно проводити аудит інформаційної безпеки та оновлювати карти ризиків. Такий підхід дозволяє ефективно розподіляти ресурси — і фінансові, і кадрові — на захист тих активів, що мають найбільшу цінність для організації. Окрім цього, для досягнення високого рівня управління інформаційною безпекою слід забезпечити автоматизований моніторинг подій безпеки з використанням SIEM-систем, а також платформ типу SOAR, які дозволяють автоматизувати реагування на інциденти [42].

Невід’ємною частиною ефективного управління є побудова культури інформаційної безпеки серед персоналу. Варто впроваджувати безперервне навчання працівників за принципом "людина — перша лінія оборони". Рекомендовано проводити регулярні симуляційні атаки (наприклад, фішингові

кампанії) з подальшим аналізом результатів і коригуванням навчальних програм. Такі заходи дозволяють підвищити обізнаність співробітників щодо актуальних методів соціальної інженерії та навчити їх реагувати на потенційні загрози. Важливо також формалізувати політики безпеки на рівні внутрішніх нормативних документів, щоб кожен співробітник розумів свої обов'язки та межі відповідальності.

Наступним напрямом є централізація управління обліковими записами, правами доступу та автентифікацією. Застосування рішень типу IAM (Identity and Access Management) дозволяє впроваджувати принцип найменших привілеїв (Least Privilege), що істотно знижує ризики від зловживання обліковими записами. Важливою складовою тут є реалізація багатофакторної автентифікації для всіх критично важливих систем. Окремо варто впровадити регулярний контроль за актуальністю прав доступу, з використанням засобів автоматичного виявлення аномалій у поведінці користувачів (User Behavior Analytics).

З метою вдосконалення технологічного рівня безпеки, необхідно застосовувати комплексну сегментацію мережі, що унеможливлює горизонтальне переміщення зловмисника в разі компрометації окремого вузла. Для реалізації цього підходу рекомендовано використовувати віртуальні зони безпеки (security zones) та мікросегментацію за допомогою програмно-визначених мереж (SDN). Також доцільно впровадити політики "zero trust", що базуються на принципі повної недовіри до будь-яких запитів, незалежно від їх походження. У такій моделі кожен запит і транзакція перевіряється на предмет відповідності політикам безпеки, контексту сесії, стану пристрою тощо [43].

У рамках забезпечення безпеки кінцевих пристроїв доцільно використовувати EDR (Endpoint Detection and Response) та XDR (Extended Detection and Response) рішення, які забезпечують високий рівень видимості та контроль над тим, що відбувається на пристроях користувачів. Перевагою таких рішень є можливість виявляти та блокувати складні атаки, зокрема APT, навіть якщо сигнатурні методи виявлення не спрацьовують. Комплексне впровадження таких систем дозволяє зменшити час виявлення загроз та скоротити потенційні

збитки.

Також варто звернути увагу на автоматизацію рутинних операцій із забезпечення інформаційної безпеки. Наприклад, автоматичне оновлення систем та застосування політик керування патчами дає змогу усунути відомі вразливості в найкоротші терміни. Крім того, використання засобів централізованого управління конфігураціями (наприклад, Ansible, Puppet або SCCM) дозволяє стандартизувати налаштування безпеки на великій кількості пристроїв. Автоматизація також охоплює створення бекапів і контроль за їхньою цілісністю та доступністю — критично важливий елемент у контексті протидії атакам типу ransomware.

Управління інформаційною безпекою також неможливе без ефективної системи реагування на інциденти. Доцільно розробити та впровадити формалізовані плани реагування (incident response playbooks), які повинні бути перевірені під час навчальних сценаріїв і адаптовані до конкретних бізнес-процесів організації. Такий підхід дозволяє скоротити час реагування, забезпечити координацію дій між підрозділами та мінімізувати негативні наслідки інцидентів [44].

Водночас важливим напрямом є активне використання інструментів зовнішньої аналітики загроз — Threat Intelligence. Збір, аналіз і кореляція зовнішніх даних про атаки, які циркулюють у мережі, дозволяють своєчасно виявляти нові типи загроз, визначати їхню релевантність до організації та адаптувати систему захисту. Доцільно інтегрувати ці джерела з внутрішніми SIEM або EDR-системами для автоматичної кореляції подій. Особливу увагу слід приділити виявленню ознак попередньої компрометації (IOCs) та поведінкових індикаторів (TTPs), характерних для конкретних атак.

Одним із перспективних напрямів є використання технологій deception (технологій обману), що дозволяють створювати фіктивні сервіси, дані або облікові записи для виявлення шкідливої активності. Вони є ефективним засобом раннього виявлення проникнення та збору інформації про дії зловмисника, мінімізуючи при цьому вплив на реальні сервіси. Застосування таких технологій

дозволяє створити гнучку та адаптивну систему захисту, здатну до самонавчання та швидкої реакції.

Окремо слід звернути увагу на питання відповідності нормативним вимогам і міжнародним стандартам. Впровадження управління інформаційною безпекою відповідно до ISO/IEC 27001 дозволяє систематизувати політики, процедури, контрольні механізми та створити механізм безперервного вдосконалення. Такий підхід також сприяє зміцненню довіри з боку клієнтів і партнерів, особливо у випадках, коли компанія працює в міжнародному середовищі [45].

Підвищення ефективності можливе також завдяки застосуванню аналітики даних та елементів штучного інтелекту. Наприклад, моделі машинного навчання можуть бути використані для виявлення аномалій у поведінці користувачів, мережевому трафіку або структурі даних. Важливо при цьому забезпечити контроль якості даних, які використовуються для тренування моделей, та валідацію їхніх рішень. Інтеграція таких інструментів у наявну інфраструктуру дозволяє досягти проактивного рівня захисту, з фокусом на запобігання інцидентам ще до їх реалізації.

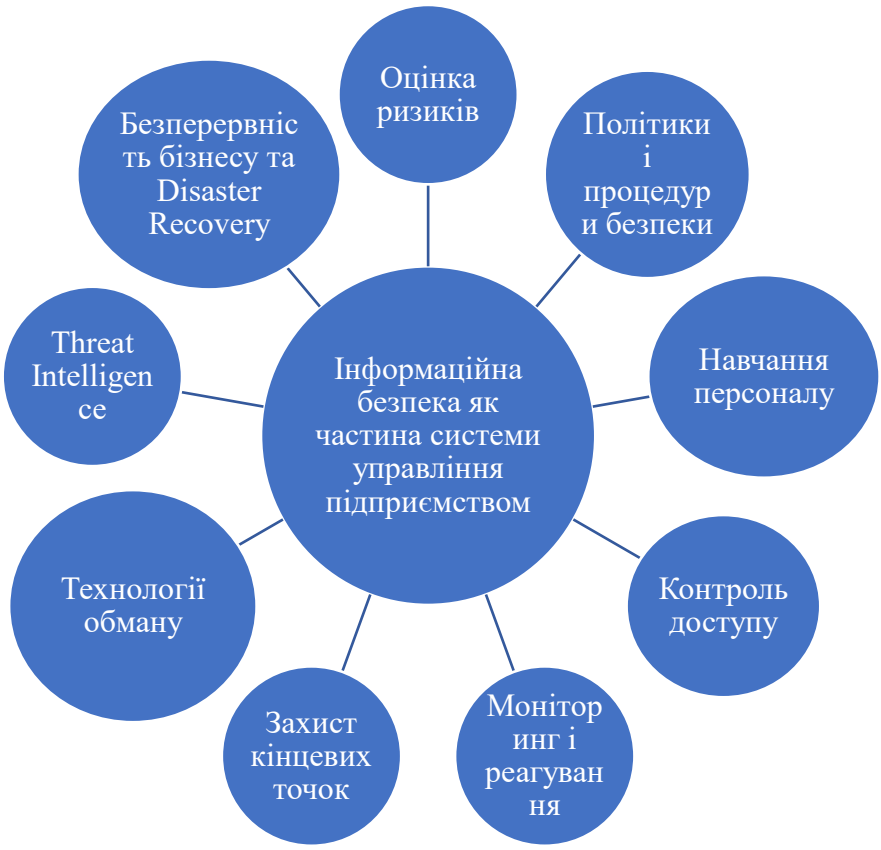

Рис. 3.1 Інтегрована модель управління інформаційною безпекою

Слід забезпечити також безперервність діяльності (business continuity) та відновлення після інцидентів (disaster recovery) як невід'ємні компоненти управління інформаційною безпекою. Плани безперервності повинні охоплювати всі критичні системи та містити чіткі інструкції для персоналу на випадок порушення доступності інформаційних ресурсів. Регулярне тестування цих планів допомагає зберегти оперативність і забезпечити готовність до надзвичайних ситуацій [46].

Варто створити функцію внутрішнього контролю за станом інформаційної безпеки, яка здійснюватиме незалежний моніторинг ефективності реалізованих заходів. Це може бути як внутрішній аудитор, так і зовнішні підрядники з відповідною кваліфікацією. Їхня діяльність повинна бути орієнтована на виявлення недоліків у реалізації політик, оцінку ризиків та розробку рекомендацій з удосконалення процесів безпеки.

3.2. Перспективи впровадження сучасних технологій у сфері ІБ

Сучасні технології стрімко трансформують сферу інформаційної безпеки, змінюючи як характер загроз, так і інструменти захисту. У найближчі роки очікується значне розширення можливостей у забезпеченні інформаційної безпеки завдяки широкому впровадженню штучного інтелекту, машинного навчання, поведінкового аналізу, автоматизації, хмарних технологій, блокчейну, квантової криптографії, біометричних систем і технологій розподіленого моніторингу. Перспективи їх використання пов’язані з не лише технічними можливостями, але й з економічними та організаційними аспектами інтеграції в існуючу інфраструктуру.

Однією з найбільш перспективних технологій є використання штучного інтелекту та машинного навчання для побудови систем виявлення загроз нового покоління. В умовах постійного зростання обсягів даних і складності атак ручний аналіз подій стає неефективним. Алгоритми машинного навчання дозволяють автоматично виявляти аномальні дії в поведінці користувачів або систем, що потенційно свідчить про загрозу. Завдяки здатності самонавчання, такі системи не залежать від фіксованих сигнатур, а виявляють нові, ще невідомі методи атак. Використання моделей поведінкового аналізу (UEBA) дозволяє створювати профілі нормальної активності для кожного користувача, пристрою чи системи й сигналізувати про будь-яке відхилення, яке може свідчити про внутрішню або зовнішню атаку [47].

Ще одним напрямом впровадження є застосування автоматизованих платформ реагування на інциденти, зокрема SOAR-рішень. Такі системи дозволяють не лише збирати, аналізувати та корелювати інформацію з різних джерел, а й ініціювати дії у відповідь — блокування доступу, відключення вузлів, активацію резервних механізмів. Це критично важливо в умовах, коли час реагування є ключовим фактором у мінімізації збитків. Автоматизація усуває затримки, пов’язані з людським фактором, та дозволяє масштабувати захист на великі інфраструктури.

Окрему увагу слід приділити хмарним технологіям, які стали основою цифрової трансформації. З одного боку, вони дають можливість динамічно масштабувати ресурси, але з іншого — створюють нові ризики, пов’язані з розподіленою природою даних, зберіганням конфіденційної інформації поза межами організації та можливими помилками в конфігурації. У зв’язку з цим перспективним є впровадження концепції Cloud Security Posture Management (CSPM), яка забезпечує безперервний контроль за відповідністю хмарної інфраструктури політикам безпеки та дозволяє автоматично виправляти помилки конфігурації. Також активно розвиваються технології CNAPP (Cloud-Native Application Protection Platform), які об’єднують захист робочих навантажень, контейнерів, кластерів Kubernetes, а також API та CI/CD-процесів.

У контексті зростання популярності віддаленої роботи зростає роль біометричних методів автентифікації. Біометрія забезпечує високий рівень впевненості в автентичності користувача та знижує ризики, пов’язані з втратою або компрометацією паролів. Нові алгоритми багатофакторної автентифікації, які комбінують біометрію з поведінковими характеристиками (наприклад, ритмом набору тексту або звичками навігації), забезпечують ще вищий рівень надійності. Перспективним є також використання адаптивної автентифікації, коли система змінює вимоги до входу залежно від контексту: локації, пристрою, часу доби, звичної поведінки користувача тощо [48].

Розвиток технологій блокчейну пропонує нові рішення в галузі захисту даних, цілісності журналів подій, децентралізованої ідентифікації та захищених транзакцій. За рахунок незмінності записів у блокчейні забезпечується високий рівень довіри до збережених даних, що особливо важливо в критичних системах, фінансових установах та при збереженні доказів інцидентів. Також розглядається використання блокчейну для керування доступом — зокрема, для запису та контролю прав доступу в децентралізованій формі.

Не менш важливою є перспектива впровадження квантової криптографії. З розвитком квантових обчислень виникає загроза порушення стійкості традиційних криптографічних алгоритмів, зокрема RSA та ECC. Квантово-

безпечні алгоритми (Post-Quantum Cryptography) та квантова передача ключів (Quantum Key Distribution) покликані вирішити цю проблему. У найближчому майбутньому перед організаціями постане завдання щодо переходу на криптографічні стандарти нового покоління, які будуть захищені від атак квантових комп'ютерів. Хоча практичне впровадження квантових комунікацій ще має обмеження в масштабах і вартості, напрям активно розвивається на рівні державних і дослідницьких програм [49].

Іншим перспективним напрямом є створення інтегрованих систем кібергігієни на рівні організацій. Мова йде не лише про технічні засоби, а й про технології управління поведінкою користувачів через системи гейміфікованого навчання, динамічну адаптацію політик безпеки до зміни ризиків та контексту, автоматизовані перевірки знань та реакцій. Такі підходи дозволяють ефективніше підтримувати високий рівень усвідомленості та дисципліни серед персоналу, що в умовах зростання соціально-орієнтованих атак є критично важливим чинником.

Зростаючу роль відіграють також технології моделювання загроз (Threat Modeling) та моделювання атак (Attack Simulation and Emulation). Такі інструменти дозволяють імітувати реальні сценарії атак з метою оцінки готовності захисних механізмів, виявлення слабких місць і підготовки персоналу. Вони підтримують підхід "постійного чергування оборони" (continuous red/blue teaming), що дає змогу організаціям бути постійно готовими до загроз [50].

Системи розподіленого моніторингу та аналізу журналів подій на основі технологій big data забезпечують здатність обробляти великі обсяги інформації в реальному часі. Це особливо важливо для компаній із глобальною присутністю або високонавантаженими цифровими платформами. Завдяки розподіленій архітектурі можливо здійснювати глибоку кореляцію подій без концентрації всієї інформації в одному центрі. Такі рішення також забезпечують високу відмовостійкість і масштабованість.

Окремої уваги заслуговує застосування цифрових двійників (digital twins)

для симуляції інформаційної безпеки. Це новий напрям, який дозволяє створити віртуальні копії інформаційних систем для тестування змін, політик, оновлень без впливу на продуктивне середовище. Це відкриває можливість більш гнучко впроваджувати інновації в безпеці без ризику для функціонування бізнесу [51].

Ще одна важлива перспектива — це інфраструктура конфіденційних обчислень (Confidential Computing), що забезпечує шифрування даних не лише під час зберігання чи передачі, але й у процесі обробки. Це дозволяє зменшити ризики несанкціонованого доступу на рівні хостингових середовищ або сторонніх операторів хмарних сервісів. Такі технології вже інтегруються в процесори нових поколінь (наприклад, Intel SGX або AMD SEV) і стають стандартом для критичних застосунків.

Таблиця 3.1

Основні перспективні технології інформаційної безпеки та їхні можливості

Технологія	Мета/функціональність	Перспектива впровадження
Штучний інтелект і машинне навчання	Виявлення аномалій, поведінковий аналіз	Висока – активно впроваджується
SOAR	Автоматичне реагування на інциденти	Висока – зростає в великих компаніях
Хмарна безпека (CSPM, CNAPP)	Контроль конфігурацій, захист контейнерів	Середньо-висока – залежить від хмарної зрілості
Біометрія та адаптивна MFA	Надійна автентифікація	Висока – поширюється в корпоративному секторі
Блокчейн	Захист даних, ідентифікація, незмінність журналів	Середня – обмежене застосування
Квантова криптографія	Захист від квантових атак	Низька–середня – перспективна, але не масова
Digital twins	Безпечне тестування політик і змін	Середня – на етапі активного R&D
Confidential Computing	Захист даних під час обробки	Висока – для критичної інфраструктури
Захист API	Контроль викликів, поведінковий аналіз API	Висока – критично важливо в хмарних середовищах

Технології захисту API (API Security) набувають особливого значення у зв’язку з розширенням мікросервісної архітектури та активного використання API в мобільних і веб-додатках. Застосування інструментів для виявлення несанкціонованих викликів API, перевірки їхніх параметрів, автентифікації та

контролю навантаження є критично необхідним для уникнення атак типу API abuse, injection, data exfiltration. Перспективним є поєднання традиційного WAF із спеціалізованими API gateways і ML-модулями поведінкового аналізу [52].

Розвиток сучасних технологій інформаційної безпеки не є ізольованим технічним процесом, а формується на стику інженерії, аналітики, поведінкових наук і управлінських підходів. Впровадження цих технологій потребує стратегічного бачення, поетапного планування та гнучкої адаптації до особливостей організації. Прогнозується, що протягом наступних п’яти років більшість середніх і великих організацій будуть поступово переходити до гібридної моделі захисту, яка поєднує хмарні сервіси, on-premise рішення, автоматизовану аналітику та активну взаємодію з системами зовнішньої кіберрозвідки.

3.3. Стратегічні напрями розвитку СМІБ в умовах цифрової трансформації

Цифрова трансформація організацій змінює природу бізнес-процесів, підходи до управління даними, взаємодію з клієнтами та партнерами. У цих умовах система менеджменту інформаційної безпеки повинна адаптуватися до динамічного середовища, інтегруватися у процеси трансформації та підтримувати гнучкість, масштабованість і безперервне вдосконалення. Основним стратегічним вектором є перехід від статичної моделі контролю до адаптивної, ризик-орієнтованої та проактивної системи, яка використовує дані в режимі реального часу, автоматизовані механізми реагування та аналітику загроз.

Одним із ключових напрямів розвитку СМІБ є інтеграція управління інформаційною безпекою в загальну систему стратегічного управління організацією. Це означає, що цілі безпеки повинні бути синхронізовані з бізнес-цілями, а управління ризиками — частиною стратегічного планування. Така інтеграція передбачає участь керівництва у процесах прийняття рішень у сфері

безпеки, затвердження політик на найвищому рівні, регулярний моніторинг метрик ефективності та звітування про ризики на рівні ради директорів або правління. Це також означає, що інформаційна безпека має розглядатися не як технічна функція, а як фактор конкурентоспроможності, довіри клієнтів і стійкості до зовнішніх впливів [53].

Наступним стратегічним кроком є впровадження моделі безпеки, що базується на принципах Zero Trust. У рамках цифрової трансформації, коли периметр організації стирається через використання хмарних сервісів, мобільних пристроїв і віддаленої роботи, традиційні підходи до доступу стають неефективними. Zero Trust вимагає постійної перевірки кожного суб'єкта доступу, незалежно від його розташування, пристрою чи попередньої автентифікації. Такий підхід передбачає мікросегментацію мереж, контроль поведінки, принцип найменших привілеїв і динамічну зміну політик доступу на основі ризиків [54].

Система менеджменту інформаційної безпеки повинна також розвиватися в напрямі автоматизації процесів. В умовах постійного зростання обсягів даних і кількості інцидентів ручне управління стає неефективним. Використання автоматизованих систем збору подій, аналізу журналів, виявлення аномалій і реагування на інциденти є критично важливим. Це включає інтеграцію платформ типу SIEM і SOAR, використання UEBA для поведінкового аналізу, а також розгортання машинного навчання для виявлення нових загроз. Автоматизація дає змогу скоротити час реагування, зменшити навантаження на аналітиків та підвищити точність оцінки ризиків [55].

Важливим стратегічним вектором є адаптація СМІБ до гібридної IT-інфраструктури, де поєднуються хмарні сервіси, локальні ресурси, контейнери, мікросервіси та зовнішні API. В умовах цифрової трансформації організації розширюють свої цифрові активи за межі традиційної інфраструктури. Це вимагає нових підходів до управління безпекою, включно з постійним моніторингом конфігурацій хмарних ресурсів, контролем доступу до API, захистом CI/CD-процесів та аналізом безпеки віртуальних середовищ. У цьому

контексті ефективною є побудова централізованої системи управління безпекою на основі хмарних платформ безпеки (наприклад, CNAPP, CSPM) [56].

Цифрова трансформація передбачає значне зростання залежності бізнесу від цифрових сервісів і даних, тому СМІБ повинна зосереджуватись на управлінні життєвим циклом даних. Це включає класифікацію, захист, контроль доступу, аудит, моніторинг передачі та знищення даних. Управління даними має ґрунтуватися на принципах конфіденційності, цілісності та доступності. Особливої уваги вимагає захист персональних даних у контексті дотримання законодавства (GDPR, ISO/IEC 27701) та посилення відповідальності за витоки інформації. Необхідно реалізовувати принципи «конфіденційність за замовчуванням» і «мінімізації даних» вже на етапі проєктування систем [57].

Паралельно з цим стратегічним напрямом виступає розвиток культури інформаційної безпеки як елементу організаційної культури в цілому. Навіть найсучасніші технічні засоби втрачають ефективність у разі відсутності усвідомленого ставлення персоналу до загроз і відповідальності. СМІБ повинна включати систематичні програми навчання, тестування, тренування інцидентів, а також елементи мотивації до дотримання політик. Новим підходом у цьому контексті є побудова персоналізованих освітніх маршрутів і використання гейміфікованих моделей навчання, адаптованих до рівня ризиків і посадових обов’язків співробітників [58].

Іншим важливим стратегічним кроком є розвиток адаптивної моделі управління ризиками. У традиційних підходах оцінка ризиків проводиться періодично, що в умовах швидкоплинних змін втрачає актуальність. В новій моделі оцінка ризиків є безперервним процесом, який враховує зміну середовища, контексту, типів активів і поведінку загроз. Такий підхід передбачає використання інструментів динамічного аналізу ризиків, що оновлюються в реальному часі, інтеграцію з інструментами threat intelligence та прогнозну аналітику на основі історичних даних. Це дозволяє приймати рішення на основі актуальної інформації, а не застарілих оцінок [59].

У рамках цифрової трансформації СМІБ повинна підтримувати

інноваційність і гнучкість організації, а не стримувати її розвиток. Це передбачає побудову безпечної платформи для експериментів, швидкого розгортання сервісів, автоматизованих перевірок політик безпеки в DevOps-процесах. У цьому напрямі важливу роль відіграє концепція DevSecOps, яка передбачає інтеграцію безпеки на всіх етапах розробки програмного забезпечення: від початкових вимог до експлуатації. Це дозволяє уникнути ситуації, коли безпека реалізується постфактум, шляхом накладання обмежень на вже реалізований продукт [60].

Не менш важливою є побудова системи виявлення, запобігання та реагування на інциденти на стратегічному рівні. Це включає створення SOC (Security Operations Center) нового покоління, який поєднує в собі автоматизацію, аналітику загроз, функції threat hunting, візуалізацію ризиків і симуляцію атак. Така система дозволяє не лише реагувати на події, а й передбачати загрози, готувати сценарії дій, формувати звіти для керівництва в режимі реального часу. Важливою тенденцією є також поєднання внутрішніх і зовнішніх ресурсів у гібридних SOC, що дає змогу зберігати баланс між контролем і масштабованістю.

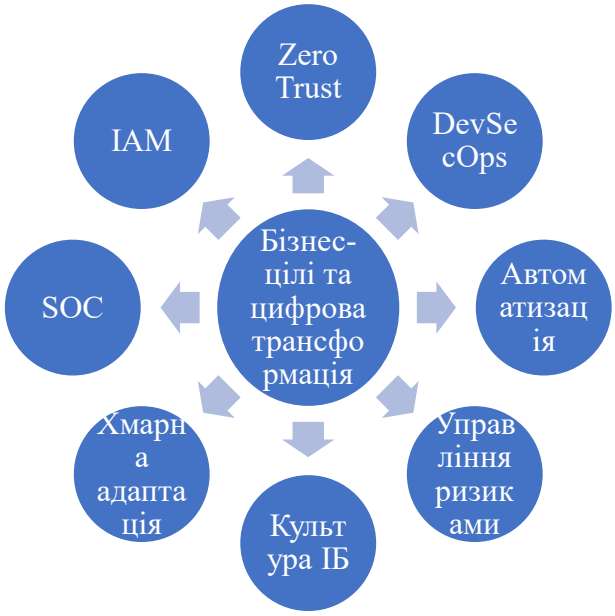

Рис. 3.2 Модель розвитку СМІБ в умовах цифрової трансформації

Важливим компонентом є формування стратегічного партнерства у сфері інформаційної безпеки. Усі організації є частиною екосистеми, тому взаємодія з

іншими учасниками — галузевими центрами обміну інформацією, державними регуляторами, міжнародними організаціями — підвищує рівень готовності до нових викликів. Обмін інформацією про загрози, спільне моделювання сценаріїв атак, участь у міжорганізаційних навчаннях і симуляціях підвищують стійкість не лише окремої компанії, а всієї екосистеми [61].

Одним із перспективних напрямів є застосування інструментів цифрової аналітики в системі управління інформаційною безпекою. Це дозволяє приймати рішення на основі даних, будувати аналітичні моделі ефективності політик, прогнозувати вплив змін, ідентифікувати слабкі місця у системі. Важливим є створення аналітичного шару над СМІБ, що забезпечує візуалізацію ключових метрик у вигляді дашбордів, які розуміють як аналітики, так і топменеджери. Це сприяє ефективному прийняттю рішень, видимості безпеки й підвищенню відповідальності керівництва [62].

Таблиця 3.2

Ключові стратегічні напрями розвитку СМІБ в умовах цифрової трансформації

Напрям розвитку	Основна мета	Ключові інструменти/технології
Інтеграція з бізнес-цілями	Узгодження ІБ з корпоративною стратегією	KPI, ISO 27001, CISO reports
Впровадження Zero Trust	Усунення довіри до внутрішніх мереж	MFA, SDP, мікросегментація
Автоматизація процесів	Підвищення ефективності та швидкості реагування	SIEM, SOAR, UEBA
Адаптація до гібридної інфраструктури	Контроль за складними IT-середовищами	CNAPP, CSPM, API Gateways
Управління даними	Захист на всіх етапах життєвого циклу	DLP, шифрування, класифікація даних
Розвиток культури ІБ	Людський фактор як ланка захисту	Гейміфікація, тренінги, симуляції
Адаптивне управління ризиками	Безперервний моніторинг і реагування	Threat intelligence, risk scoring engines
Інтеграція в DevSecOps	Безпека як частина розробки	SAST, DAST, IaC scanning
Створення SOC нового покоління	Виявлення і попередження складних атак	Threat hunting, MITRE ATT&CK, XDR
Цифрова аналітика	Прийняття рішень на основі даних	BI dashboards, аналітичні моделі, KPI
Управління цифровою ідентичністю	Контроль облікових записів і доступів	IAM, PAM, IDaaS

Окремий стратегічний напрям — розвиток цифрової ідентичності в рамках СМІБ. Це включає управління життєвим циклом облікових записів, рольову модель доступу, політику атестації доступів, механізми багатоетапної автентифікації, а також контроль привілейованих облікових записів (PAM). З огляду на кількість взаємодій між системами, хмарними платформами, підрядниками і користувачами, безпека цифрової ідентичності стає основою всієї моделі доступу. Перспективним є впровадження концепції Identity as a Service (IDaaS) для централізованого управління.

Таким чином, стратегічні напрями розвитку системи менеджменту інформаційної безпеки повинні бути пов’язані з цифровою трансформацією не як з проблемою, а як із джерелом нових можливостей. Успішна СМІБ майбутнього — це система, яка постійно навчається, адаптується, масштабується, реагує в реальному часі й підтримує гнучке управління безпекою як активом організації.

Висновки до розділу 3

У третьому розділі було сформовано рекомендації, спрямовані на вдосконалення СМІБ в умовах сучасних викликів та цифрової трансформації. Представлено пропозиції щодо підвищення ефективності управління інформаційною безпекою, що охоплюють удосконалення політик безпеки, стандартизацію процедур реагування на інциденти, впровадження ризик-орієнтованого підходу, а також зміцнення ролі лідерства і корпоративної культури у сфері ІБ. Акцент зроблено на необхідності створення адаптивної СМІБ, яка динамічно реагує на зміни зовнішнього середовища та внутрішні виклики.

Розглянуто перспективи впровадження сучасних технологій, таких як засоби штучного інтелекту, автоматизовані системи моніторингу, блокчейн-рішення, zero trust-архітектури та інструменти поведінкової аналітики.

Зазначено, що інтеграція таких рішень дозволяє не лише підвищити рівень проактивного захисту, а й оптимізувати управлінські ресурси шляхом автоматизації рутинних процесів. Окремо підкреслено важливість забезпечення сумісності нових технологій із чинною інфраструктурою та нормативними вимогами.

Запропоновано стратегічні напрями розвитку СМІБ у контексті цифрової трансформації, включаючи побудову безпечного цифрового середовища, посилення кіберстійкості, розвиток кадрового потенціалу у сфері ІБ, а також інтеграцію СМІБ у загальну стратегію цифрового розвитку підприємства. Підкреслено, що ефективна СМІБ має бути не лише відповідною до сучасних викликів, але й здатною передбачати майбутні загрози та трансформуватись відповідно до змін бізнес-моделі.

Рекомендації, наведені у третьому розділі, демонструють необхідність поєднання стратегічного бачення, технологічної гнучкості та управлінської рішучості для досягнення високого рівня інформаційної безпеки в умовах швидкої цифровізації та зростаючих регуляторних вимог.

ВИСНОВКИ

У результаті проведеного дослідження сформовано цілісне уявлення про систему менеджменту інформаційної безпеки як ключовий інструмент забезпечення стійкості, керованості та нормативної відповідності в умовах стрімкої цифровізації та зростання кіберзагроз. На підставі аналізу сутності, структури й принципів побудови СМІБ визначено, що вона є не лише технічною чи організаційною складовою, а насамперед — елементом стратегічного управління, який повинен бути інтегрований у загальні бізнес-процеси організації. Виявлено, що ефективна СМІБ базується на системному підході, циклі PDCA (планування, виконання, контроль, удосконалення), управлінні ризиками, а також на обов’язковому дотриманні міжнародних стандартів і регуляторних вимог.

Особливу увагу приділено аналізу ключових нормативних засад, що регулюють діяльність у сфері інформаційної безпеки. Встановлено, що фундаментальними документами для побудови СМІБ є стандарти серії ISO/IEC 27000, які задають уніфіковану рамку для розробки, впровадження, підтримки та вдосконалення СМІБ. Крім того, досліджено національні нормативно-правові акти та галузеві вимоги, які мають враховуватись при реалізації заходів ІБ, зокрема у банківському, телекомунікаційному та державному секторах. Здійснено огляд підходів до оцінювання відповідності СМІБ зазначеним вимогам, включаючи методології сертифікаційного аудиту, самооцінки, тестування політик безпеки та процедур перевірки внутрішнього контролю.

У практичній частині роботи розкрито специфіку застосування інструментів управління відповідністю на рівні організації. Досліджено типові ризики невідповідності, які виникають у результаті змін законодавства, недостатньої компетентності персоналу, технологічної застарілості інфраструктури або слабкого контролю за доступом. Встановлено, що для ефективного виявлення таких ризиків доцільно використовувати методи попередньої оцінки відповідності (GAP-аналіз), регулярні внутрішні та зовнішні аудити, а також

автоматизовані системи моніторингу політик ІБ. Окрема увага приділена процедурі впровадження заходів реагування, серед яких — оновлення політик, підвищення обізнаності персоналу, перегляд схем контролю доступу, оновлення технічних засобів захисту.

У рамках дослідження надано комплексні рекомендації щодо вдосконалення системи менеджменту інформаційної безпеки відповідно до сучасних викликів. Одним із основних векторів удосконалення визначено підвищення ефективності управління за рахунок чіткішого розподілу ролей і відповідальності, посилення стратегічного контролю з боку керівництва, запровадження системної оцінки результативності СМІБ на основі метрик та індикаторів ризику. Показано, що важливою умовою адаптивності СМІБ є використання сучасних технологій, таких як автоматизовані системи реагування, поведінкові аналітики, засоби захисту в хмарних середовищах та платформи для керування цифровими ідентичностями. Зазначено, що ключем до довгострокової стійкості є впровадження підходів Zero Trust, DevSecOps і побудова моделі безпеки, яка функціонує в режимі реального часу.

Окреме місце в роботі посідає дослідження стратегічних напрямів розвитку СМІБ у контексті цифрової трансформації. Доведено, що успішне функціонування системи в сучасних умовах потребує не лише підтримки нормативної відповідності, а й здатності до постійного самовдосконалення, гнучкості та інновацій. СМІБ має еволюціонувати від реактивної моделі до проактивної, що ґрунтується на прогнозуванні загроз, аналізі великих обсягів даних і використанні алгоритмів машинного навчання. Розглянуто необхідність включення СМІБ до загальної цифрової стратегії організації, що дозволяє забезпечити її синергію з іншими бізнес-ініціативами — від хмарної трансформації до автоматизації операцій.

На підставі проведеного аналізу обґрунтовано, що стратегічне управління інформаційною безпекою має базуватися на таких принципах: орієнтація на ризик, орієнтація на бізнес-цілі, безперервність удосконалення, використання перевірених практик і стандартів, інтеграція з IT-архітектурою та адаптивність

до змін. Це дозволяє не лише знизити ймовірність реалізації загроз, а й забезпечити конкурентоспроможність організації в довгостроковій перспективі. Успішна СМІБ виступає не просто бар'єром проти атак, а активним елементом цифрової культури, що формує довіру, підвищує репутацію й відкриває нові можливості для сталого розвитку.

Результати роботи свідчать про необхідність переходу до комплексного, стратегічного й гнучкого підходу до управління інформаційною безпекою. Здійснений теоретичний і практичний аналіз дає змогу не лише зрозуміти поточний стан СМІБ, а й сформулювати обґрунтовані рекомендації щодо її модернізації. Реалізація запропонованих заходів сприятиме підвищенню рівня відповідності нормативним вимогам, покращенню інституційної стійкості та створенню ефективної системи захисту, здатної відповідати на виклики цифрової епохи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Александер Д., Браун А., Фарахмандпур С. Менеджмент інформаційної безпеки: Практичний посібник. К.: IT-Expert, 2023. 352 с.

2. Антонюк В. В., Жора В. В. Система управління інформаційною безпекою в банківському секторі України: актуальні проблеми та шляхи їх вирішення. Кібербезпека: освіта, наука, техніка. 2023. № 1(17). С. 6-21.

3. Архипов О. Є., Козюра В. Д. Управління ризиками в системах захисту інформації: монографія. К.: ДУІКТ, 2023. 278 с.

4. Бакалінський О. В., Маслянко П. П. Створення та впровадження системи менеджменту інформаційної безпеки на підприємстві. Інформаційна безпека людини, суспільства, держави. 2023. № 2(33). С. 113-122.

5. Бурячок В. Л., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект: підручник. К.: ДУТ, 2023. 320 с.

6. Войтко С. В., Морозов В. П. Аналіз регуляторних вимог до систем захисту інформації в умовах цифрової трансформації. Економіка і управління. 2023. № 2. С. 119-125.

7. Гаврилова Л. В. Методи оцінювання ефективності системи менеджменту інформаційної безпеки підприємства. Безпека інформації. 2024. Том 30, № 1. С. 67-75.

8. Гнатюк С. О., Сидоренко В. М. Стандартизація у сфері інформаційної безпеки: міжнародний досвід та українські реалії. Захист інформації. 2023. Том 25, № 3. С. 123-134.

9. Горбенко І. Д., Потій О. В. Методологія оцінювання стану кібербезпеки інформаційно-телекомунікаційних систем. Радіотехніка. 2024. Вип. 206. С. 7-16.

10. Грайворонський М. В., Новіков О. М. Безпека інформаційно-комунікаційних систем. К.: Основа, 2023. 436 с.

11. Дудикевич В. Б., Микитин Г. В. Захист інформації в інформаційних системах: навчальний посібник. Львів: НУ "Львівська політехніка", 2023. 312 с.

12. Євсеєв С. П., Король О. Г. Методи та моделі оцінки ризиків інформаційної безпеки. Системи обробки інформації. 2024. № 1(168). С. 88-97.

13. Єрохін А. Л., Ляшенко О. С. Технологічні аспекти забезпечення кібербезпеки підприємств. Сучасні інформаційні системи. 2024. Т. 8, № 1. С. 74-81.

14. Зінько С. М., Джурабаєв Д. Х. Моніторинг та аудит інформаційної безпеки. Інформаційні технології і засоби навчання. 2023. Т. 94, № 2. С. 238-251.

15. Зубок М. І. Інформаційна безпека суб'єктів підприємництва: навч. посіб. К.: КНЕУ, 2023. 226 с.

16. Корченко О. Г., Бурячок В. Л., Гнатюк С. О. Кібернетична безпека держави: характеристика сучасних викликів, загроз та ризиків. Інформаційна безпека. 2023. № 3(31). С. 5-14.

17. Кучернюк П. В. Технології управління інцидентами інформаційної безпеки. Безпека інформації. 2023. Т. 29, № 2. С. 149-158.

18. Легомінова С. В., Мужанова Т. М. Регуляторні аспекти інформаційної безпеки: міжнародний досвід. Економіка. Менеджмент. Бізнес. 2023. № 2(36). С. 76-85.

19. Лужецький В. А., Кожухівський А. Д., Войтович О. П. Основи інформаційної безпеки: навчальний посібник. Вінниця: ВНТУ, 2023. 316 с.

20. Марущак А. І. Правове забезпечення інформаційної безпеки в Україні: монографія. К.: Юрінком Інтер, 2023. 290 с.

21. Мельник С. В., Васильєв Ю. В. Автоматизовані системи управління ризиками інформаційної безпеки. Кібербезпека: освіта, наука, техніка. 2023. № 2(18). С. 85-94.

22. Мохор В. В., Богданов О. М. Методологія побудови системи управління інформаційною безпекою на базі стандартів ISO/IEC 27000. Реєстрація, зберігання і обробка даних. 2023. Том 25, № 3. С. 56-67.

23. Новіков О. М., Тимошенко А. О. Стан кібербезпеки України: проблеми та перспективи. Інформаційні технології та безпека. 2023. Вип. 11. С. 133-142.

24. Носов В. В., Манжай А. В. Організаційно-правове забезпечення інформаційної безпеки: навч. посіб. Х.: ХНУВС, 2023. 276 с.

25. Петренко А. І., Квасніков В. П. Управління інформаційними ризиками на підприємстві: методи та інструменти. Вісник інженерної академії України. 2023. № 2. С. 273-280.

26. Потій О. В., Мялковський Д. В. Методи оцінки стану інформаційної безпеки в інформаційно-телекомунікаційних системах. Системи управління, навігації та зв'язку. 2023. Вип. 2(68). С. 120-126.

27. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII (зі змінами). Відомості Верховної Ради України. 1992. № 48. Ст. 650.

28. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР (зі змінами). Відомості Верховної Ради України. 1994. № 31. Ст. 286.

29. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII (зі змінами). Відомості Верховної Ради України. 2017. № 45. Ст. 403.

30. Руденко О. В., Скітер І. С. Методи визначення відповідності системи менеджменту інформаційної безпеки міжнародним стандартам. Вчені записки ТНУ ім. В.І. Вернадського. Серія: Технічні науки. 2024. Том 35(74), № 1. С. 204-210.

31. Савченко В. А., Матов О. Я. Аудит та оцінка ефективності системи захисту інформації. Сучасний захист інформації. 2023. № 2(46). С. 76-84.

32. Стрельбіцький М. А., Ткачук Н. А. Управління знаннями в системі інформаційної безпеки підприємства. Економіка та держава. 2024. № 2. С. 68-73.

33. Толюпа С. В., Демченко І. В. Проблеми інформаційної безпеки сучасного суспільства. Телекомунікаційні та інформаційні технології. 2023. № 2(79). С. 4-12.

34. Хорошко В. О., Хохлачова Ю. Є. Управління інцидентами інформаційної безпеки. Захист інформації. 2023. Том 25, № 4. С. 192-200.

35. Чекурін В. Ф., Буджак Я. С. Функціональна стійкість інформаційних систем: методологія аналізу та забезпечення. Відбір і обробка інформації. 2023. Вип. 50(126). С. 13-20.

36. Чунарьова А. В., Чунарьов А. В. Приватність та захист персональних даних у контексті кіберзагроз. Інформаційні технології та безпека. 2023. Вип. 11. С. 50-58.

37. Шелест М. Є., Яковів І. Б. Оцінка уразливостей та управління ризиками інформаційної безпеки. Сучасний захист інформації. 2023. № 1(45). С. 21-29.

38. Юдін О. К., Бучик С. С. Державні інформаційні ресурси: нормативно-правовий аналіз та методологія побудови. К.: НАУ, 2023. 284 с.

39. Яремчук Ю. Є., Карпінець В. В. Криптографічні методи захисту інформації в інформаційно-телекомунікаційних системах. Вінниця: ТОВ "Твори", 2023. 326 с.

40. ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT). [Чинний від 2016-01-01]. Вид. офіц. К.: ДП "УкрНДНЦ", 2016. 22 с.

41. ДСТУ ISO/IEC 27002:2015. Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT). [Чинний від 2016-01-01]. Вид. офіц. К.: ДП "УкрНДНЦ", 2016. 72 с.

42. ДСТУ ISO/IEC 27005:2019. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2018, IDT). [Чинний від 2019-12-01]. Вид. офіц. К.: ДП "УкрНДНЦ", 2019. 54 с.

43. COBIT 2019 Framework: Introduction and Methodology. ISACA, 2018. 94 p.

44. Cybersecurity Framework Version 1.1. NIST, 2018. URL: https://www.nist.gov/cyberframework/framework

45. Fruhlinger J. The 15 biggest data breaches of the 21st century. CSO Online. 2022. URL: https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

46. Hassija V., Chamola V., Saxena V., Jain D., Goyal P., Sikdar B. A survey on IoT security: application areas, security threats, and solution architectures. IEEE Access. 2023. Vol. 11. pp. 12843-12875.

47. IBM Security. Cost of a Data Breach Report 2024. IBM Corporation. 2024. 86 p.

48. ISO/IEC 27035-1:2023. Information security, cybersecurity and privacy protection — Information security incident management — Part 1: Principles and process. ISO/IEC, 2023. 36 p.

49. NIST Special Publication 800-53 Revision 5. Security and Privacy Controls for Information Systems and Organizations. NIST, 2020. 492 p.

50. Payment Card Industry (PCI) Data Security Standard: Requirements and Security Assessment Procedures. PCI Security Standards Council, 2022. 88 p.

51. Savola R. M. Towards a taxonomy of information security metrics. Proceedings of the 2nd International Conference on Risk and Security of Internet and Systems. 2023. pp. 154-161.

52. Shah T. H., Bardi M. A., Farooq A. M. Impacts of COVID-19 on Cybersecurity. 10th International Conference on Software Engineering Research, Management and Applications (SERA). 2023. pp. 113-117.

53. Solms R., Niekerk J. From information security to cyber security. Computers & Security. 2023. Vol. 122. pp. 193-202.

54. Валіна О. М. Політична етика : навч.-метод. посіб. Запоріжжя : ЗНУ, 2017. 102 с.

55. Аванесова Н. Е., Марченко О. В. Стратегічне управління підприємством та сучасним містом: теоретико-методичні засади : монографія. Харків : Щедра садиба плюс, 2015. 196 с.

56. Аніловська Г. Я., Марушко Н. С., Стоколоса Т. М. Інформаційні системи і технології у фінансах : навч. посіб. Львів : Магнолія 2006, 2015. 312 с.

57. Бікулов Д. Т, Чкан А. С., Олійник О. М., Маркова С. В. Менеджмент : навч. посіб. Запоріжжя : ЗНУ, 2017. 360 с.

58. Про освіту : Закон України від 05.09.2017 р. № 2145-VIII. Голос України. 2017. 27 верес. (№ 178-179). С. 10–22.

59. ДСТУ ISO/IEC 27002:2015. Інформаційні технології. Методи захисту. Звід правил щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT). [Чинний від 2017-01-01]. Вид. офіц.. К. : ДП «УкрНДНЦ», 2016. 149с.

60. Коломоєць Т. О. Адміністративна деліктологія та адміністративна деліктність. Адміністративне право України : підручник / за заг. ред. Т. О. Коломоєць. Київ, 2009. С. 195–197.

61. Антонович М. Жертви геноцидів першої половини ХХ століття: порівняльно-правовий аналіз. Голодомор 1932-1933 років: втрати української нації : матеріали міжнар. наук.-практ. конф., м. Київ, 4 жовт. 2016 р. Київ, 2017. С. 133–136.

62. Біленчук П., Обіход Т. Небезпеки ядерної злочинності: аналіз вітчизняного і міжнародного законодавства. Юридичний вісник України. 2017. 20-26 жовт. (№ 42). С. 14–15.