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 В УМОВАХ ФУНКЦІОНУВАННЯ SOC”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека та захист інформації
освітньо-професійної програми Управління інформаційною та кібернетичною безпекою

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

_____ Владислав ДОБРИДНИК
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБД-42

Владислав ДОБРИДНИК
Ім’я, Прізвище

Керівник: Тетяна КАПЕЛЮШНА
д.е.н, доцент Ім’я, Прізвище
Рецензент: Галина ГАЙДУР
д.т.н, професор Ім’я, Прізвище

Київ 2026

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра Управління кібербезпекою та захистом інформації
Ступінь вищої освіти бакалавр
Спеціальність 125 Кібербезпека та захист інформації
Освітньо-професійна програма Управління інформаційною та кібернетичною безпекою

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

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Добриднику Владиславу Олександровичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи: “Методи забезпечення відповідності системи менеджменту інформаційної безпеки регуляторним вимогам в умовах функціонування SOC”
керівник кваліфікаційної роботи Тетяна КАПЕЛЮШНА, д.е.н., доцент
(Ім’я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від “20“ лютого 2026 р. № 51

2. Строк подання кваліфікаційної роботи “12” травня 2026 р

3. Вихідні дані до кваліфікаційної роботи: *міжнародні стандарти ISO/IEC 27001:2022, ISO/IEC 27002:2022, PCI DSS v4.0, NIST SP 800-61 Rev.3, NIST CSF 2.0; нормативні документи НБУ (Постанова №95 від 28.09.2017); Закон України «Про основні засади забезпечення кібербезпеки України» №2163-VIII від 05.10.2017; наукові публікації у сфері інформаційної безпеки та Security Operations Center; відкриті аналітичні звіти провідних компаній галузі (Gartner, Ponemon Institute, IBM X-Force, CrowdStrike); документація провідних SIEM/SOAR/EDR платформ; рекомендації MITRE ATT&CK для фінансового сектору.*

4. Перелік питань, які потрібно розробити:
1. Проаналізувати регуляторне середовище у сфері інформаційної безпеки та визначити ключові вимоги до СМІБ.
2. Проаналізувати архітектуру, функції та інструментальні засоби Security Operations Center як операційного середовища забезпечення інформаційної безпеки.
3. Виявити взаємозв’язки між процесами SOC та вимогами регуляторів до СМІБ, провести gap-аналіз існуючих підходів до забезпечення відповідності.
4. Порівняти сучасні методи забезпечення відповідності СМІБ регуляторним вимогам у контексті функціонування SOC.
5. Вдосконалити узагальнену методику інтеграції процесів SOC у систему забезпечення відповідності СМІБ та сформувати практичні рекомендації щодо її впровадження.

5. Перелік ілюстративного матеріалу: *презентація Power Point*

6. Дата видачі завдання “05” березня 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2026	
2.	Збір та аналіз літератури.	30.03.2026	
3.	Ознайомлення із теоретичними основими захисту інформаційного середовища підприємства підприємства та вимогами СМІБ	08.04.2026	
4.	Аналітичне дослідження інструментарію захисту інформаційного середовища та ролі SOC у забезпеченні вимог СМІБ	15.04.2026	
5.	Розробка методики забезпечення відповідності СМІБ та інтеграція із SOC	22.04.2026	
6.	Формулювання висновків за результатами проведеного дослідження.	29.04.2026	
7.	Оформлення роботи.	06.05.2026	
8.	Оформлення презентації.	11.05.2026	
9.	Отримання рецензії на роботу.	01.06.2026	
10.	Захист в ЕК.	15.06.2026	

Здобувач вищої освіти _____ Владислав ДОБРИДНИК
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Тетяна КАПЕЛЮШНА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

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

Направляється здобувач Добридник В. О. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека та захист інформації
(код, найменування спеціальності)
Освітньо-професійної програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Методи забезпечення відповідності системи менеджменту інформаційної безпеки регуляторним вимогам в умовах функціонування SOC "
Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач ДОБРИДНИК Владислав продемонстрував глибоке розуміння теоретичних основ захисту інформаційного середовища підприємства, детально проаналізувавши нормативні вимоги до функціонування SOC та СМІБ. Опрацьований теоретичний матеріал свідчить про високий рівень фахової підготовки автора та його здатність комплексно оцінювати методи забезпечення відповідності регуляторним вимогам.

Особливої уваги заслуговує аналітична частина дослідження, в якій автор не лише здійснив ґрунтовний огляд сучасного інструментарію кіберзахисту, але й провів якісний Gap-аналіз існуючих підходів до інтеграції СМІБ та SOC. Здобувачеві вдалося чітко ідентифікувати розриви між закоментованими регуляторними вимогами та реальними операційними процесами моніторингу.

Практичну цінність та безперечний елемент новизни становить розроблена здобувачем авторська методика SOCE (Security Operations as Compliance Evidence). Запропонований алгоритм перетворення операційних процесів SOC на доказову базу для аудиту СМІБ, разом із адаптованими рекомендаціями для банківського сектору та оцінкою доцільності впровадження.

З огляду на вищезазначене, вважаю, що кваліфікаційна дозволяє оцінити кваліфікаційну роботу здобувача ДОБРИДНИКА Владислава на оцінку "відмінно" та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Тетяна КАПЕЛЮШНА
«12» травня 2026 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Добридник В.О. допускається до захисту даної роботи в екзаменаційній комісії.

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

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

Здобувача вищої освіти Добридника Владислава Олександровича
На тему: «Методи забезпечення відповідності системи менеджменту інформаційної безпеки регуляторним вимогам в умовах функціонування SOC»

Актуальність. Тема кваліфікаційної роботи є актуальною в умовах сучасного регуляторного середовища банківського сектору України. Банківські установи одночасно підпадають під дію Постанови НБУ №95, міжнародного стандарту ISO/IEC 27001:2022, стандарту PCI DSS v4.0 та GDPR, що формує складний комплаєнс-ландшафт, систематизований методичний підхід до управління яким у вітчизняній науковій літературі практично відсутній. Посилення регуляторного тиску з боку НБУ та зростання кількості кіберінцидентів у фінансовому секторі підтверджують практичну значущість обраної теми.

Позитивні сторони. Кваліфікаційна робота відзначається логічно структурованим та послідовним викладом матеріалу. У першому розділі ретельно досліджено регуляторне середовище банківського сектору: систематизовано вимоги всіх чотирьох регуляторів із зазначенням конкретних строків, санкцій та механізмів перевірки відповідності, що виходить за межі формального переліку нормативних вимог і демонструє глибоке розуміння практики регуляторних відносин. Другий розділ містить детальний аналіз трирівневої архітектури SOC та інструментального стека з прив'язкою до конкретних контролів СМІБ, а проведений gap-аналіз дозволив системно виявити шість типових розривів у банківській практиці та визначити механізми їх усунення.

Позитивні сторони.

1. Представляє наукову цінність третій розділ, у якому розроблено авторська методика SOCE, що принципово відрізняється від наявних методологій SANS Institute та рекомендацій Gartner, наявністю формалізованого двостороннього зв'язку між контролями СМІБ та процесами SOC.
2. Практичну цінність становить диференційований підхід до впровадження для трьох профілів банків та розроблена система з 11 вимірюваних KPI відповідності СМІБ.

Недоліки. Робота матиме більшу практичну цінність за умови доповнення результатами апробації запропонованої методики або пілотного впровадження у банку.

Висновок. Кваліфікаційна робота Добридника Владислава Олександровича є самостійним та завершеним дослідженням, що відповідає вимогам до кваліфікаційних робіт освітнього ступеня бакалавра зі спеціальності 125 «Кібербезпека та захист інформації».

Рецензент: завідувач кафедри
Систем та технологій кібербезпеки,
д.т.н, професор

_____
підпис

Галина ГАЙДУР
Ім’я, Прізвище

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню та розробці методичного підходу до забезпечення відповідності системи менеджменту інформаційної безпеки регуляторним вимогам шляхом інтеграції процесів та інструментів Security Operations Center як засобу безперервного моніторингу та формування доказової бази відповідності.

Метою роботи є розробки та обґрунтування методики забезпечення відповідності системи менеджменту інформаційної безпеки (СМІБ) регуляторним вимогам за рахунок інтеграції з операційними процесами SOC (на прикладі банківських установ).

Об'єктом дослідження методи, підходи та інструментальні засоби забезпечення відповідності СМІБ регуляторним вимогам в умовах безперервного функціонування центру операцій з кібербезпеки SOC

Предметом дослідження є методи та механізми забезпечення відповідності системи менеджменту інформаційної безпеки регуляторним вимогам із використанням процесів і технологій Security Operations Center.

Методи дослідження. У роботі використано системний аналіз, порівняльний аналіз, методи узагальнення та класифікації, gap-аналіз, а також процесний підхід PDCA для дослідження структури СМІБ та взаємодії її процесів із SOC.

Галузь застосування. Розроблені підходи можуть бути застосовані підприємствами банківського сектору, а також організаціями інших галузей з підвищеними вимогами до інформаційної безпеки для підвищення рівня відповідності регуляторним вимогам, автоматизації комплаєнсу та удосконалення процесів внутрішнього аудиту.

Кваліфікаційна робота містить вступ, три розділи, висновки, список використаних джерел (42 найменування) та додатки. Загальний обсяг роботи – 88 сторінок, з яких 4 сторінки займає список використаних джерел. Робота містить

6 рисунків, 11 таблиць (у т.ч. 3 у додатках).

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

Ключові слова: СИСТЕМА МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, SECURITY OPERATIONS CENTER, ВІДПОВІДНІСТЬ РЕГУЛЯТОРНИМ ВИМОГАМ, БЕЗПЕРЕРВНИЙ КОМПЛАЄНС, SOCE, SIEM, SOAR.

ABSTRACT

The qualification work is devoted to the development of a methodological approach to ensuring the compliance of an Information Security Management System (ISMS) with regulatory requirements through the integration of Security Operations Center (SOC) processes and tools as a mechanism for continuous monitoring and compliance evidence generation.

The purpose of the study is to develop a five-stage SOCE (Security Operations as Compliance Evidence) methodology that systematically transforms routine SOC operational activities into verified compliance evidence, eliminating the need for parallel compliance processes.

The object of the study is the Information Security Management System of an organization operating within a Security Operations Center environment.

The subject of the study is the methods and mechanisms for ensuring ISMS compliance with regulatory requirements using SOC processes and technologies.

Research methods. The following methods were applied: systematic analysis, comparative analysis, generalization and classification, gap analysis, and the PDCA process approach for examining ISMS structure and its interaction with SOC.

As a result, the work: analyzed the regulatory environment of the Ukrainian banking sector (NBU Resolution No. 95, ISO/IEC 27001:2022, PCI DSS v4.0, GDPR); examined the three-tier SOC architecture and its correspondence to ISMS controls; identified six systemic compliance gaps typical of banking practice; developed the original SOCE methodology comprising five interrelated stages (compliance control mapping, evidence automation, continuous compliance monitoring, structured evidence provision, and continuous improvement loop); and formulated practical recommendations for implementation across three bank profiles.

Field of application. The developed approaches can be applied by banking sector organizations and other regulated industries to improve ISMS compliance levels, automate compliance evidence collection, and enhance internal audit processes.

The qualification work consists of an introduction, three chapters containing 6

figures and 11 tables, conclusions, and a list of references containing 42 items. The total volume of the work is 88 pages.

Keywords: INFORMATION SECURITY MANAGEMENT SYSTEM, SECURITY OPERATIONS CENTER, REGULATORY COMPLIANCE, ISO/IEC 27001, PCI DSS, CONTINUOUS COMPLIANCE, SOCE, SIEM, SOAR.

ЗМІСТ

ВСТУП

В умовах розвитку цифрового суспільства інформаційні технології стали невід'ємною складовою функціонування підприємств, установ та організацій практично в усіх галузях економіки. Автоматизація бізнес-процесів, використання хмарних технологій, розвиток електронного документообігу, дистанційних сервісів та цифрових платформ сприяють підвищенню ефективності діяльності організацій, однак одночасно створюють нові виклики у сфері інформаційної безпеки. Інформація, інформаційні ресурси та цифрові сервіси перетворилися на стратегічно важливі активи, від рівня захищеності яких залежить стабільність функціонування сучасних підприємств.

Особливого значення питання захисту інформаційного середовища набувають для організацій, діяльність яких пов'язана з обробкою великих обсягів конфіденційної інформації, персональних даних або забезпеченням безперервності критичних сервісів. До таких сфер належать банківський сектор, державні установи, телекомунікаційні компанії, IT-підприємства, промислові підприємства, об'єкти критичної інфраструктури, медичні установи та сфера електронної комерції. У процесі цифрової трансформації зазначені організації активно використовують автоматизовані інформаційні системи, мережеву інфраструктуру, веб-технології та хмарні сервіси, що суттєво розширює поверхню потенційних кіберзагроз.

Інформаційне середовище підприємства характеризується високим рівнем інтеграції інформаційних систем, постійним обміном даними між внутрішніми та зовнішніми компонентами інфраструктури, використанням віддаленого доступу та сервісів цифрової взаємодії. За таких умов організації стикаються зі значною кількістю кіберзагроз, серед яких найбільш поширеними є фішингові атаки, програми-вимагачі, компрометація облікових записів, витік конфіденційної інформації, атаки на веб-додатки, експлуатація вразливостей програмного забезпечення та атаки на хмарні середовища. Реалізація таких

загроз може призвести до фінансових втрат, порушення безперервності бізнес-процесів, репутаційних ризиків та невиконання регуляторних вимог.

У зв’язку з постійним зростанням кількості кіберінцидентів та ускладненням методів проведення атак особливої актуальності набуває необхідність впровадження комплексного підходу до управління інформаційною безпекою. Одним із найбільш поширених міжнародних підходів до організації процесів захисту інформації є система менеджменту інформаційної безпеки (СМІБ), побудована відповідно до вимог стандартів серії ISO/IEC 27000. СМІБ забезпечує систематизований підхід до управління ризиками інформаційної безпеки, формування політик безпеки, контролю доступу, управління інцидентами та забезпечення безперервного вдосконалення процесів захисту інформації.

Додатковим фактором актуалізації проблематики забезпечення інформаційної безпеки є посилення регуляторних вимог у сфері кіберзахисту та захисту персональних даних. Організації різних галузей повинні забезпечувати відповідність міжнародним стандартам, галузевим нормативам та вимогам державного регулювання. Для фінансового сектору такими вимогами є нормативні документи Національного банку України та стандарт PCI DSS, для підприємств, що працюють із персональними даними, – вимоги GDPR та законодавства України у сфері захисту персональних даних. Виконання зазначених вимог передбачає не лише впровадження технічних засобів захисту, але й забезпечення постійного моніторингу, аудиту та підтвердження ефективності функціонування системи інформаційної безпеки.

Важливу роль у забезпеченні безперервного моніторингу інформаційного середовища відіграють Security Operations Center (SOC). SOC являє собою спеціалізований центр моніторингу та реагування на події інформаційної безпеки, який забезпечує централізований збір та аналіз журналів подій, виявлення аномальної активності, реагування на інциденти, управління вразливостями та підтримку процесів забезпечення відповідності регуляторним вимогам. Використання SOC дозволяє організаціям перейти від реактивної

моделі захисту до проактивного підходу, орієнтованого на безперервний контроль інформаційного середовища та раннє виявлення кіберзагроз.

Особливого значення інтеграція процесів SOC та СМІБ набуває для банківського сектору, оскільки банки є одними з найбільш цифровізованих і регульованих організацій. Банківські установи обробляють великі обсяги фінансової та персональної інформації, забезпечують виконання електронних платежів у режимі реального часу та повинні підтримувати високий рівень доступності сервісів. Саме тому банки активно впроваджують сучасні засоби моніторингу подій безпеки, системи управління інцидентами, SIEM-платформи та механізми автоматизації реагування на кіберзагрози.

Питанням забезпечення інформаційної безпеки, розвитку систем менеджменту інформаційної безпеки, функціонування Security Operations Center та управління кіберризиками присвячено значну кількість наукових праць вітчизняних і зарубіжних дослідників, а також міжнародних стандартів і рекомендацій у сфері кібербезпеки. Незважаючи на це, питання інтеграції процесів SOC у систему забезпечення відповідності СМІБ регуляторним вимогам потребує подальшого дослідження, особливо в контексті практичного застосування у банківському секторі.

Таким чином, актуальність теми кваліфікаційної роботи зумовлена необхідністю розроблення сучасних підходів до забезпечення відповідності систем менеджменту інформаційної безпеки регуляторним вимогам шляхом інтеграції процесів та технологій Security Operations Center як механізму безперервного моніторингу, аналізу та підтвердження ефективності функціонування засобів захисту інформації.

Метою роботи є розроблення методичного підходу до забезпечення відповідності системи менеджменту інформаційної безпеки регуляторним вимогам шляхом інтеграції процесів та інструментів Security Operations Center як засобу безперервного моніторингу та доказової бази відповідності.

Для досягнення поставленої мети необхідно вирішити такі завдання:

- дослідити регуляторне середовище у сфері інформаційної безпеки та визначити вимоги до систем менеджменту інформаційної безпеки;
- проаналізувати архітектуру, функції та інструментальні засоби Security Operations Center як операційного середовища забезпечення інформаційної безпеки;
- виявити взаємозв'язки між процесами SOC та вимогами регуляторів до СМІБ, а також здійснити gap-аналіз існуючих підходів до забезпечення відповідності;
- порівняти сучасні методи забезпечення відповідності СМІБ регуляторним вимогам у контексті функціонування SOC;
- розробити узагальнену методику інтеграції процесів SOC у систему забезпечення відповідності СМІБ та сформувати практичні рекомендації щодо її застосування на прикладі підприємств банківського сектору.

Об'єктом дослідження є система менеджменту інформаційної безпеки організації, що функціонує в умовах Security Operations Center.

Предметом дослідження є методи та механізми забезпечення відповідності системи менеджменту інформаційної безпеки регуляторним вимогам із використанням процесів і технологій Security Operations Center.

Методи дослідження. Для досягнення поставленої мети у роботі використано комплекс загальнонаукових та спеціальних методів дослідження, зокрема: системний аналіз – для дослідження структури інформаційного середовища та процесів забезпечення інформаційної безпеки; порівняльний аналіз – для оцінювання сучасних підходів до побудови SOC та забезпечення відповідності СМІБ регуляторним вимогам; методи узагальнення та класифікації – для систематизації регуляторних вимог і засобів захисту інформації; gap-аналіз – для виявлення невідповідностей між існуючими підходами до забезпечення відповідності та вимогами інформаційної безпеки; процесний підхід PDCA – для аналізу функціонування СМІБ та взаємодії її процесів із Security Operations Center.

Наукова новизна одержаних результатів полягає в удосконаленні методичного підходу до забезпечення відповідності системи менеджменту інформаційної

безпеки регуляторним вимогам шляхом інтеграції процесів та інструментів Security Operations Center як механізму безперервного моніторингу, централізованого контролю подій безпеки та формування доказової бази відповідності.

Практичне значення одержаних результатів полягає у можливості використання запропонованих підходів підприємствами різних галузей для підвищення рівня відповідності вимогам інформаційної безпеки, автоматизації процесів моніторингу та реагування на інциденти, а також удосконалення процесів внутрішнього аудиту та управління кіберризиками. Найбільш доцільним застосування запропонованих рекомендацій є для підприємств банківського сектору, які функціонують в умовах підвищених вимог до інформаційної безпеки та кіберзахисту.

Структура роботи. Кваліфікаційна робота складається зі вступу, трьох розділів, висновків та списку використаних джерел. У першому розділі розглянуто теоретичні основи захисту інформаційного середовища підприємства та функціонування системи менеджменту інформаційної безпеки. У другому розділі проведено аналіз сучасних засобів і практик захисту інформаційного середовища та досліджено особливості функціонування Security Operations Center. У третьому розділі сформовано практичні рекомендації щодо забезпечення відповідності СМІБ регуляторним вимогам шляхом інтеграції процесів SOC у систему інформаційної безпеки підприємства на прикладі банківського сектору.

Розділ 1. ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА ПІДПРИЄМСТВА

1.1 Поняття та складові інформаційного середовища підприємства

В умовах розвитку цифрової економіки інформація стала одним із ресурсів функціонування підприємств, установ та організацій. Використання інформаційно-комунікаційних технологій забезпечує автоматизацію бізнес-процесів, підтримку управлінської діяльності, взаємодію із клієнтами, зберігання та обробку великих обсягів даних. Практично всі сфери діяльності – банківський сектор, телекомунікації, електронна комерція, промисловість, державне управління, логістика, медицина та ІТ-галузь – функціонують в умовах постійного використання цифрових технологій та інформаційних систем [1].

У процесі цифрової трансформації підприємства формують складне інформаційне середовище, яке об’єднує інформаційні ресурси, програмне забезпечення, апаратно-технічні засоби, мережеву інфраструктуру, персонал та організаційні процеси. Ефективність функціонування такого середовища безпосередньо впливає на стабільність діяльності організації, конкурентоспроможність та рівень захищеності інформаційних активів [2].

У науковій літературі інформаційне середовище підприємства визначається як сукупність інформаційних ресурсів, технічних засобів, програмного забезпечення, телекомунікаційних систем, інформаційних процесів та організаційних механізмів, які забезпечують створення, обробку, передачу, зберігання та захист інформації в межах діяльності організації [3]. Інформаційне середовище є основою цифрового функціонування сучасного підприємства та забезпечує підтримку управлінських, виробничих і комунікаційних процесів.

Особливого значення інформаційне середовище набуває для організацій, діяльність яких пов’язана з обробкою значних обсягів конфіденційної інформації або забезпеченням безперервності критичних сервісів. До таких організацій належать банки, телекомунікаційні компанії, державні установи, медичні заклади,

підприємства енергетичного сектору та об’єкти критичної інфраструктури. Для даних організацій порушення функціонування інформаційного середовища може призвести до фінансових втрат, витоку даних, зупинки бізнес-процесів або порушення регуляторних вимог [4].

Основними складовими інформаційного середовища підприємства є:

- інформаційні ресурси;
- інформаційні системи;
- програмне забезпечення;
- апаратно-технічна інфраструктура;
- телекомунікаційні мережі;
- персонал організації;
- організаційні процеси;
- засоби забезпечення інформаційної безпеки.

Інформаційні ресурси є базовою складовою інформаційного середовища та включають структуровані й неструктуровані дані, електронні документи, бази даних, цифрові архіви, фінансову інформацію, персональні дані клієнтів, журнали подій безпеки та інші інформаційні активи підприємства [5]. У різних галузях характер інформаційних ресурсів може відрізнятися. Наприклад, у медичних установах критичними є медичні записи пацієнтів, у промисловості – технологічна документація та дані виробничих процесів, а у банківському секторі – фінансові транзакції та персональні дані клієнтів.

Наступною складовою є інформаційні системи, які забезпечують автоматизацію бізнес-процесів та підтримку діяльності організації. До таких систем належать ERP-системи, CRM-платформи, системи електронного документообігу, бухгалтерські системи, корпоративні веб-портали, хмарні сервіси та спеціалізовані прикладні системи [6]. У банківському секторі важливу роль відіграють автоматизовані банківські системи, системи дистанційного банківського обслуговування та платіжні платформи.

Ефективність функціонування інформаційного середовища значною мірою залежить від програмного забезпечення, яке використовується організацією.

Програмне забезпечення включає операційні системи, системи управління базами даних, серверні платформи, прикладні програми, аналітичні системи та засоби кіберзахисту. Вразливості програмного забезпечення залишаються однією з найбільш поширених причин реалізації кіберзагроз, що обумовлює необхідність постійного оновлення програмних компонентів та контролю безпечності конфігурацій [7].

Апаратно-технічна інфраструктура інформаційного середовища включає серверне обладнання, робочі станції, мобільні пристрої, системи зберігання даних, мережеве обладнання та дата-центри. Організації активно використовують технології віртуалізації та хмарних обчислень, що дозволяє забезпечити масштабованість та гнучкість IT-інфраструктури [8]. Водночас використання хмарних сервісів створює нові виклики у сфері інформаційної безпеки, пов’язані із захистом даних, управлінням доступом та контролем хмарних середовищ.

Важливою складовою інформаційного середовища є телекомунікаційна інфраструктура, яка забезпечує передачу інформації між компонентами системи. До телекомунікаційної інфраструктури належать локальні та глобальні мережі, VPN-з’єднання, бездротові мережі, маршрутизатори, комутатори та засоби захисту мережевого трафіку [9]. Значна частина атак спрямована саме на мережеву інфраструктуру підприємств, тому захист каналів передачі даних є одним із ключових завдань забезпечення інформаційної безпеки.

Одним із найбільш чутливих до кіберзагроз серед складових інформаційного середовища є персонал організації. Незважаючи на розвиток технологічних засобів захисту, людський фактор залишається однією з основних причин порушення інформаційної безпеки [10]. Помилки користувачів, використання слабких паролів, порушення політик безпеки або застосування методів соціальної інженерії можуть призвести до компрометації інформаційних ресурсів. Саме тому підприємства й надалі впроваджують програми підвищення обізнаності персоналу у сфері кібербезпеки та механізми контролю доступу.

Організаційні процеси забезпечують управління функціонуванням інформаційного середовища та реалізацію заходів інформаційної безпеки. До таких

процесів належать управління ризиками, резервне копіювання, аудит інформаційних систем, реагування на інциденти, управління доступом, управління змінами та забезпечення безперервності діяльності [11]. Саме в межах організаційних процесів формується система менеджменту інформаційної безпеки.

Система менеджменту інформаційної безпеки (СМІБ) є одним із механізмів забезпечення захисту інформаційного середовища підприємства. Відповідно до ISO/IEC 27001:2022 СМІБ являє собою сукупність політик, процедур, процесів та ресурсів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації. Основною особливістю СМІБ є використання ризик-орієнтованого підходу, який передбачає ідентифікацію загроз, оцінювання ризиків та впровадження відповідних заходів контролю [12].

Системи менеджменту інформаційної безпеки функціонують на основі процесного підходу та циклу PDCA (Plan-Do-Check-Act), який забезпечує безперервне вдосконалення процесів інформаційної безпеки [12]. На етапі Plan визначаються цілі та політики безпеки, на етапі Do реалізуються механізми захисту, етап Check передбачає моніторинг та аудит ефективності заходів безпеки, а етап Act забезпечує вдосконалення процесів управління інформаційною безпекою.

Важливу роль у забезпеченні ефективного функціонування інформаційного середовища відіграють Security Operations Center (SOC). SOC являє собою спеціалізований центр моніторингу подій інформаційної безпеки, який забезпечує централізований збір та аналіз журналів подій, виявлення кіберзагроз, реагування на інциденти та підтримку процесів забезпечення відповідності регуляторним вимогам [13]. Використання SOC дозволяє організаціям реалізувати проактивний підхід до забезпечення інформаційної безпеки та забезпечити безперервний контроль інформаційного середовища.

Особливо активно SOC впроваджуються у високоризикових галузях, зокрема у банківському секторі, телекомунікаціях та на об’єктах критичної інфраструктури. Для банківських установ використання SOC є необхідним через значну кількість кіберзагроз, високі вимоги до доступності сервісів та необхідність

забезпечення відповідності нормативним вимогам Національного банку України, PCI DSS та міжнародним стандартам інформаційної безпеки [14].

Однією з головних проблем сучасного інформаційного середовища є постійне зростання кількості кіберзагроз. Найбільш поширеними загрозами залишаються фішинг, програми-вимагачі, компрометація облікових записів, атаки на веб-додатки, витік персональних даних та експлуатація вразливостей програмного забезпечення [15]. Складність сучасних атак постійно зростає, що вимагає використання комплексних механізмів моніторингу, аналізу та реагування на інциденти.

Таким чином, інформаційне середовище підприємства є складною багаторівневою системою, яка включає інформаційні ресурси, технічну інфраструктуру, програмне забезпечення, мережеві засоби, персонал та організаційні процеси. В умовах цифровізації та зростання кількості кіберзагроз забезпечення захисту інформаційного середовища стає одним із ключових завдань сучасних організацій незалежно від сфери діяльності. Важливу роль у реалізації процесів захисту інформаційного середовища відіграють системи менеджменту інформаційної безпеки та Security Operations Center як механізми безперервного моніторингу, аналізу та реагування на кіберзагрози.

1.2 Нормативні вимоги до SOC та СМІБ

Банківський сектор України функціонує в умовах складного нормативно-правового середовища, що формується перетином вимог національного регулятора, міжнародних стандартів та галузевих кодексів. Для розроблення ефективного методичного підходу до інтеграції SOC у систему забезпечення відповідності СМІБ необхідно детально проаналізувати кожен регуляторний документ: не лише перелік формальних вимог, але й механізм підтвердження відповідності, практику регуляторних перевірок та санкції за порушення [14].

Постанова Правління НБУ №95 від 28.09.2017 «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки та кіберзахисту в банківській системі України» є основоположним регуляторним документом для банківського сектору у сфері кіберзахисту [32]. Документ структурований за шістьма розділами відповідно до функцій кібербезпеки фреймворку NIST CSF: Ідентифікація (Розділ III), Захист (Розділ IV), Виявлення (Розділ V), Реагування (Розділ VI) та Відновлення. Така структура дозволяє банкам безпосередньо зіставляти вимоги НБУ з міжнародними стандартами та кращими практиками [20].

Найбільш операційно значущою для SOC є вимога щодо звітування про кіберінциденти, закріплена у Розділі VI. Банки зобов'язані повідомляти НБУ про суттєві кіберінциденти не пізніше ніж через 72 години після їх виявлення. Суттєвим вважається інцидент, що призвів до: переривання надання банківських послуг більш ніж на чотири години; несанкціонованого доступу до критичної інформації; або компрометації платіжної інфраструктури. Критично важливим є те, що 72-годинний відлік розпочинається з моменту виявлення – тобто з часової мітки, яку фіксує SIEM при генерації першого підтвердженого алерту. Саме тому SOC є єдиним підрозділом банку, здатним забезпечити документально підтверджену відповідність цій вимозі [32].

Важливим практичним нюансом Постанови №95 є принципова відмінність між формальним та фактичним виконанням вимог. Постанова не встановлює конкретних технічних вимог до інструментів моніторингу, надаючи банкам свободу у виборі технологій. Проте при перевірці НБУ інспектори оцінюють фактичну спроможність банку виявляти та реагувати на інциденти через практичне тестування, а не лише шляхом перевірки наявності нормативних документів і процедур. Банки, що мають функціонуючий SOC із задокументованими процесами та вимірюваними метриками, демонструють суттєво вищий результат при регуляторних перевірках порівняно з банками, де кіберзахист реалізований переважно на папері.

Міжнародний стандарт ISO/IEC 27001:2022 є основою для побудови СМІБ та її міжнародної сертифікації [12]. Версія 2022 суттєво відрізняється від попередньої редакції 2013 року: перехід від 114 контролів у 14 доменах до 93 контролів у чотирьох тематичних групах, введення 11 нових контролів, серед яких особливого значення набувають A.5.7 («Threat Intelligence»), A.5.23 («ІБ при використанні хмарних сервісів»), A.8.16 («Моніторинг діяльності») та A.6.8 («Звітування про події ІБ») – усі вони безпосередньо кореспондують з функціями SOC. Відповідність цим контролям SOC забезпечує через повсякденну операційну діяльність, перетворюючи рутинні процеси моніторингу на автоматично генеровані докази для аудиторів.

Процес сертифікації за ISO/IEC 27001 передбачає дві стадії проведення зовнішнього аудиту акредитованим органом з сертифікації [33]. Stage 1 аудит (документаційний) оцінює повноту документації СМІБ: Декларацію застосовності (Statement of Applicability), Звіт про оцінку ризиків, реєстр активів, процедури управління інцидентами. Stage 2 аудит (операційний) є значно складнішим: аудитор перевіряє фактичне функціонування СМІБ через інтерв'ю з персоналом та перевірку реальних журналів і записів за останні 90–180 днів. Типові запити аудиторів у Stage 2 включають: хронологію останніх десяти інцидентів із доказами реагування у SOAR; звіти Log Source Coverage за останній квартал; результати сканування вразливостей та підтвердження їх усунення; протоколи Management Review. Усі ці артефакти є природним продуктом повсякденної операційної діяльності SOC, що знімає потребу у спеціальній підготовці документів «під аудит».

Ключовим практичним нюансом є те, що аудитори ISO/IEC 27001:2022 оцінюють не лише наявність доказів, але й їхню несуперечливість та повноту [33]. Якщо журнали SIEM фіксують підозрілу подію, а у системі SOAR відповідного тікету немає – це свідчить про те, що процес моніторингу є формальним і не функціонує на практиці. Аналогічно, рівень False Positive Rate вище 50% вказує на неналежне налаштування правил кореляції, що ставить під сумнів ефективність усього процесу моніторингу. Такі невідповідності можуть призвести до видачі

major nonconformity – критичної невідповідності, що унеможливлює отримання або підтвердження сертифіката до її усунення.

Стандарт PCI DSS (Payment Card Industry Data Security Standard) версії 4.0, що набрав чинності у квітні 2024 року, встановлює обов'язкові вимоги для всіх банків-емітентів та еквайрів [17]. Версія 4.0 принципово відрізняється від попередньої (3.2.1) введенням концепції «Customized Approach» – можливості використання альтернативних технічних засобів для досягнення цілей безпеки, за умови їх обґрунтування через формальну оцінку ризиків. Це суттєво розширює роль SOC, оскільки саме він надає технічну базу для оцінки ризиків, необхідної при застосуванні кастомізованих підходів (вимога 12.3.2). Вимога 10 PCI DSS v4.0 є найбільш безпосередньо пов'язаною з функціями SIEM: вимагає автоматичного журналювання дій привілейованих користувачів (10.2.1), захисту журналів від несанкціонованої зміни через WORM-механізм (10.3), оперативного аналізу журналів для виявлення аномалій (10.6) та зберігання журналів не менше 12 місяців з оперативним доступом до даних за останні три місяці (10.7). Постанова НБУ №95 у цьому контексті встановлює суворіший строк зберігання – щонайменше три роки для записів про кіберінциденти.

Загальний регламент про захист даних (GDPR) застосовується до банків, що обробляють персональні дані громадян ЄС [18]. Стаття 32 GDPR вимагає від банків технічних та організаційних заходів захисту ПД, що відповідають рівню ризику, зокрема: псевдонімізацію та шифрування; забезпечення безперервної конфіденційності, цілісності та доступності систем; здатність своєчасно відновити доступ до ПД після інциденту; регулярне тестування ефективності технічних заходів. Стаття 33 GDPR встановлює вимогу повідомляти наглядовий орган про порушення безпеки ПД протягом 72 годин після виявлення. Відповідно до Guidelines 9/2022 Комітету Ради Європи з питань захисту даних (EDPB) [40], «виявленням» вважається момент, коли банк отримав достатньо інформації для підтвердження факту порушення. SOC через SOAR фіксує обидва моменти – часову мітку першого алерту та часову мітку підтвердження після розслідування, – що є критичним для доведення дотримання строків перед наглядовим органом.

Закон України «Про основні засади забезпечення кібербезпеки України» №2163-VIII від 05.10.2017 [34] визначає правові та організаційні засади кіберзахисту об'єктів критичної інфраструктури. Для банків, класифікованих як такі об’єкти, закон встановлює додаткові вимоги: взаємодія з CERT-UA через структурований обмін TI-фідами та звітуванням про інциденти; проведення обов'язкових аудитів кіберзахисту; негайне оповіщення про кіберінциденти на критичній інфраструктурі. Практичним способом виконання цих вимог є інтеграція SOC з CERT-UA через API-з’єднання для отримання актуальних IoC та автоматичного сповіщення при виявленні загроз, пов'язаних з атаками на об’єкти КІ. У табл. 1.1 систематизовано матрицю відповідності із зіставленням ключових вимог, строків виконання, санкцій та інструментів SOC.

Таблиця 1.1

Матриця відповідності СМІБ банку нормативним вимогам

Регулятор / Стандарт	**Ключові вимоги до SOC та СМІБ**	**Строки виконання**	**Санкції за невиконання**	**Інструмент SOC**
НБУ Постанова №95 (2017)	Безперервний моніторинг кіберзагроз (Розд. V); звітування про суттєві кіберінциденти до НБУ; формування реєстру кіберінцидентів; призначення відповідальної особи за кіберзахист	72 год. з моменту виявлення суттєвого інциденту; щорічна звітність про стан кіберзахисту	Заходи впливу НБУ: попередження, штраф, тимчасова адміністрація; відкликання ліцензії у разі систематичних порушень	SOAR (авто-тікет з таймером 72h); SIEM (реєстр інцидентів); звіт за шаблоном НБУ
ISO/IEC 27001:2022	Оцінка ризиків (п. 6.1.2); впровадження 93 контролів Додатку A; безперервний моніторинг (п. 9.1); огляд з боку керівництва (п. 9.3); постійне вдосконалення (п. 10.1)	Безперервно; Stage 1/Stage 2 при сертифікації; щорічні наглядові аудити; ресертифікація кожні 3 роки	Відмова у сертифікації; major/minor nonconformity; призупинення або відкликання сертифіката	SIEM compliance-дашборд; SOAR (chain of custody); GRC-платформа; Management Review звіт

Продовження таблиці 1.1

PCI DSS v4.0 (квітень 2024)	Захист даних платіжних карток у CDE; журналювання всього доступу (вимога 10); щоквартальне сканування (вимога 11.3); тест на проникнення (вимога 11.4); управління вразливостями (вимога 6); Customized Approach (вимога 12.3.2)	Безперервно (журналювання); щоквартально (сканування); щорічно (pentest); retention ≥ 12 міс.	Втрата статусу PCI-compliant; штраф Visa/Mastercard від $5 тис. до $100 тис./місяць; заборона приймати картки	SIEM (immutable logs, WORM-сховище); Tenable/Qualys (VM-сканування); SOAR (remediation tracking)
GDPR / Закон України «Про захист ПД»	Технічні та організаційні заходи захисту ПД (ст. 32); повідомлення наглядового органу при порушенні (ст. 33); DPIA (ст. 35); privacy by design (ст. 25)	72 год. після підтвердження порушення (ст. 33); без затримки для повідомлення суб'єктів (ст. 34)	Штраф до 4% глобального річного обороту або 20 млн EUR; репутаційні збитки; судові позови суб'єктів даних	SOAR + DLP (автоматична ескалація при витоку ПД); автотаймер GDPR-72h; auto-draft звіту для ДПА
Закон України «Про основні засади кібербезпеки» №2163-VIII	Класифікація об'єктів критичної інфраструктури; обов'язковий аудит кіберзахисту; взаємодія з CERT-UA; негайне звітування при КІ-інцидентах	За вимогою регулятора; негайно для критичних КІ-інцидентів з оповіщенням CERT-UA	Адміністративна відповідальність за порушення вимог щодо КІ; кримінальна відповідальність	SOAR-інтеграція з CERT-UA API; TI-фіди від CERT-UA; координаційні плейбуки для КІ-інцидентів

Сучасні організації функціонують в умовах постійного розвитку цифрових технологій, інтеграції інформаційних систем та збільшення обсягів інформаційних потоків. Незалежно від галузі діяльності – промисловості, банківського сектору, ІТ-індустрії, електронної комерції, телекомунікацій чи державного управління – підприємства використовують складні інформаційні інфраструктури, які об’єднують різноманітні апаратні, програмні та мережеві компоненти. У таких умовах особливого значення набуває формування єдиного інформаційного середовища, що забезпечує взаємодію всіх елементів організації та підтримку її бізнес-процесів [2].

Єдине інформаційне середовище організації являє собою інтегровану сукупність інформаційних систем, інформаційних ресурсів, програмного забезпечення, технічної інфраструктури, мережевих сервісів та організаційних процесів, які функціонують як цілісна система для забезпечення ефективної діяльності підприємства [3]. Основною особливістю такого середовища є взаємозалежність його компонентів, коли порушення функціонування одного елемента може впливати на роботу інших складових інформаційної інфраструктури.

Формування єдиного інформаційного середовища забезпечує централізацію обробки інформації, автоматизацію бізнес-процесів, підвищення швидкості обміну даними та ефективність управління організацією. Водночас інтеграція інформаційних систем та сервісів супроводжується зростанням складності управління інформаційною безпекою, оскільки збільшення кількості взаємопов’язаних компонентів створює додаткові ризики та потенційні точки компрометації [1].

У структурі єдиного інформаційного середовища організації можна виділити декілька основних рівнів:

- рівень користувачів;
- прикладний рівень;
- рівень даних;
- мережевий рівень;
- інфраструктурний рівень;
- хмарний рівень;
- рівень засобів інформаційної безпеки.

Рівень користувачів включає персонал організації, зовнішніх користувачів, клієнтів та партнерів, які взаємодіють з інформаційними системами підприємства. Саме користувачі є джерелом формування значної частини інформаційних потоків та одночасно залишаються одним із найбільш вразливих елементів системи безпеки [10]. У сучасних організаціях використовується велика кількість механізмів контролю доступу, багатофакторної автентифікації та систем управління ідентифікацією (IAM), спрямованих на мінімізацію ризиків, пов’язаних із людським фактором.

Прикладний рівень об’єднує програмні системи та сервіси, які забезпечують автоматизацію бізнес-процесів організації. До таких систем належать ERP-платформи, CRM-системи, системи електронного документообігу, веб-додатки, корпоративні портали, аналітичні системи та хмарні сервіси [6]. Для різних галузей характерне використання спеціалізованих прикладних систем. Наприклад, у банківському секторі використовуються автоматизовані банківські системи та платіжні сервіси, у промисловості – системи автоматизованого управління виробництвом, а у сфері електронної комерції – платформи онлайн-продажу та системи обробки платежів.

Рівень даних є однією з найбільш критичних складових інформаційного середовища, оскільки саме дані становлять основну цінність для організації. На цьому рівні функціонують системи управління базами даних, сховища даних, системи резервного копіювання та архівування інформації [11]. Захист даних є ключовим завданням інформаційної безпеки, особливо для організацій, що працюють із персональними даними, фінансовою інформацією або конфіденційною комерційною інформацією.

Мережевий рівень забезпечує передачу інформації між компонентами інформаційного середовища. До нього належать локальні мережі, глобальні мережеві з’єднання, VPN-інфраструктура, бездротові мережі, маршрутизатори, комутатори та мережеві шлюзи [9]. Саме мережевий рівень є одним із головних об’єктів атак кіберзлочинців, тому організації активно використовують міжмережеві екрани, системи виявлення вторгнень, системи сегментації мережі та засоби шифрування трафіку.

Інфраструктурний рівень включає серверне обладнання, дата-центри, віртуалізовані середовища, системи зберігання даних та робочі станції користувачів [16]. У сучасних організаціях значного поширення набули технології віртуалізації, які дозволяють ефективно використовувати обчислювальні ресурси та забезпечувати масштабованість IT-інфраструктури. Водночас централізація ресурсів потребує додаткових заходів забезпечення безпеки та резервування.

Важливим компонентом сучасного інформаційного середовища є хмарний рівень. Хмарні технології забезпечують організаціям можливість використання віддалених обчислювальних ресурсів, платформ та програмного забезпечення без необхідності створення власної фізичної інфраструктури [8]. Використання моделей SaaS, PaaS та IaaS дозволяє підвищити гнучкість бізнес-процесів та оптимізувати витрати на IT-інфраструктуру. Проте використання хмарних сервісів створює нові виклики у сфері інформаційної безпеки, пов'язані із захистом даних, контролем доступу та управлінням хмарними конфігураціями.

Окреме місце у структурі єдиного інформаційного середовища займають засоби інформаційної безпеки, які забезпечують захист усіх компонентів інфраструктури. До таких засобів належать міжмережеві екрани (Firewall), системи виявлення та запобігання вторгненням (IDS/IPS), антивірусні рішення, системи DLP, SIEM-платформи, EDR/XDR-рішення, системи управління доступом та засоби криптографічного захисту інформації.

У сучасних умовах ефективне функціонування єдиного інформаційного середовища неможливе без використання системи менеджменту інформаційної безпеки (СМІБ). СМІБ забезпечує інтеграцію організаційних, технічних та процедурних заходів захисту інформації у межах єдиної керованої системи. Основним завданням СМІБ є забезпечення конфіденційності, цілісності та доступності інформації шляхом використання ризик-орієнтованого підходу до управління інформаційною безпекою.

Однією з ключових особливостей СМІБ є використання процесного підходу, який дозволяє інтегрувати заходи інформаційної безпеки у всі бізнес-процеси організації. Відповідно до вимог ISO/IEC 27001:2022 СМІБ повинна функціонувати на основі циклу PDCA (Plan-Do-Check-Act), який забезпечує безперервне вдосконалення системи управління інформаційною безпекою [12].

На етапі Plan організація визначає цілі інформаційної безпеки, оцінює ризики та формує політики безпеки. Етап Do передбачає впровадження технічних та організаційних механізмів захисту інформації. На етапі Check здійснюється

моніторинг ефективності заходів безпеки, аудит інформаційних систем та оцінювання відповідності вимогам стандартів і нормативних документів. Етап Act забезпечує вдосконалення процесів захисту інформації на основі результатів моніторингу та аудиту [17].

У сучасних організаціях важливу роль у забезпеченні ефективного функціонування СМІБ та контролю єдиного інформаційного середовища відіграє Security Operations Center (SOC). SOC забезпечує централізований моніторинг подій безпеки, аналіз журналів подій, виявлення кіберзагроз та реагування на інциденти [13]. Використання SOC дозволяє інтегрувати різнорідні засоби захисту інформації в єдину систему моніторингу та забезпечити постійний контроль стану інформаційного середовища.

Особливого значення функціонування SOC набуває для організацій із розгалуженою цифровою інфраструктурою та високими вимогами до інформаційної безпеки. Найбільш активно SOC впроваджуються у банківському секторі, телекомунікаціях, IT-компаніях, державних установах та на об’єктах критичної інфраструктури [4]. Для банківських установ SOC є важливим елементом забезпечення відповідності вимогам Національного банку України, міжнародних стандартів ISO/IEC 27001 та PCI DSS.

Однією з сучасних концепцій побудови єдиного інформаційного середовища є Zero Trust Architecture. Концепція Zero Trust базується на принципі «ніколи не довіряй – завжди перевіряй» та передбачає постійну перевірку автентичності користувачів, пристроїв і сервісів незалежно від їх розташування у мережі [18]. Реалізація Zero Trust Architecture передбачає використання багатофакторної автентифікації, сегментації мережі, контролю доступу та безперервного моніторингу подій безпеки.

Ще однією важливою концепцією є Defense in Depth – багаторівневий підхід до забезпечення інформаційної безпеки, який передбачає використання декількох незалежних рівнів захисту [19]. У межах цієї концепції організації використовують поєднання технічних, організаційних та процедурних механізмів безпеки, що дозволяє знизити ризик успішної реалізації кіберзагроз.

Таким чином, єдине інформаційне середовище сучасної організації являє собою складну багаторівневу систему, яка об’єднує користувачів, інформаційні системи, дані, мережеву інфраструктуру, хмарні сервіси та засоби інформаційної безпеки. Ефективне функціонування такого середовища потребує інтеграції технічних і організаційних механізмів захисту, використання систем менеджменту інформаційної безпеки та забезпечення безперервного моніторингу подій безпеки. Важливу роль у реалізації цих процесів відіграють Security Operations Center, які забезпечують централізований контроль інформаційного середовища та підтримку процесів управління інформаційною безпекою.

1.3 Методи захисту інформаційного середовища та підходи до забезпечення відповідності СМІБ регуляторним вимогам

В умовах розвитку цифрових технологій та постійного зростання кількості кіберзагроз традиційні підходи до забезпечення інформаційної безпеки вже не забезпечують достатнього рівня захисту інформаційного середовища організацій. Тривалий час більшість підприємств використовували переважно реактивні механізми захисту, орієнтовані на реагування після виникнення інциденту інформаційної безпеки. Однак у зв’язку зі збільшенням складності кібератак, автоматизацією діяльності кіберзлочинців та використанням прихованих механізмів компрометації інформаційних систем виникла необхідність переходу до проактивних моделей забезпечення інформаційної безпеки [4].

Організації функціонують в умовах високої залежності від цифрових сервісів, інформаційних систем та мережевої інфраструктури. Банківський сектор, IT-компанії, державні установи, промислові підприємства, телекомунікаційні оператори, медичні заклади та підприємства електронної комерції використовують великі обсяги інформаційних ресурсів і забезпечують безперервне функціонування цифрових сервісів. За таких умов порушення інформаційної безпеки

може призвести до фінансових втрат, витоку конфіденційної інформації, репутаційних ризиків, порушення виробничих процесів або невиконання регуляторних вимог [15].

Проактивний підхід до захисту інформаційного середовища передбачає не лише реагування на вже реалізовані інциденти, але й постійний моніторинг інформаційної інфраструктури, прогнозування потенційних загроз, виявлення аномальної активності та запобігання реалізації кіберзагроз [20]. Основною метою проактивного захисту є мінімізація часу виявлення атак, скорочення часу реагування на інциденти та забезпечення безперервності функціонування організації.

На відміну від реактивної моделі забезпечення інформаційної безпеки, яка орієнтована переважно на ліквідацію наслідків інцидентів, проактивний підхід базується на постійному аналізі подій безпеки, оцінюванні ризиків та виявленні потенційних ознак компрометації інформаційного середовища [21]. Реалізація такого підходу потребує використання сучасних технологій моніторингу, аналізу та автоматизації процесів реагування на кіберзагрози.

До основних проактивних засобів захисту інформаційного середовища належать:

- системи Security Information and Event Management (SIEM);
- Endpoint Detection and Response (EDR);
- Extended Detection and Response (XDR);
- Security Orchestration, Automation and Response (SOAR);
- системи Threat Intelligence;
- Threat Hunting;
- системи управління вразливостями;
- системи аналізу поведінки користувачів (UEBA);
- засоби моніторингу мережевої активності.

Одним із ключових елементів сучасного проактивного захисту є Security Operations Center (SOC). SOC являє собою спеціалізований центр моніторингу та реагування на події інформаційної безпеки, який забезпечує централізований ко-

нтроль стану інформаційного середовища організації [13]. Основними функціями SOC є збір та аналіз журналів подій, виявлення кіберзагроз, реагування на інциденти, управління вразливостями, проведення Threat Hunting та підтримка процесів забезпечення відповідності регуляторним вимогам.

У сучасних організаціях SOC виконує роль операційного ядра системи забезпечення інформаційної безпеки. Використання SOC дозволяє інтегрувати різнорідні засоби захисту інформації у єдину систему моніторингу та забезпечити безперервний контроль інформаційного середовища [22]. Найбільш активно SOC впроваджуються у банківському секторі, телекомунікаційних компаніях, IT-організаціях, державних структурах та на об’єктах критичної інфраструктури.

Особливого значення використання SOC набуває у банківському секторі, оскільки банки є одними з найбільш цифровізованих та регульованих організацій. Банківські установи обробляють великі обсяги фінансової та персональної інформації, забезпечують функціонування платіжних сервісів та дистанційного банківського обслуговування, що робить їх одними з основних цілей кібератак [14]. Саме тому банки активно впроваджують сучасні системи моніторингу подій безпеки, автоматизації реагування та аналізу кіберзагроз.

Одним із ключових технологічних компонентів SOC є SIEM-система (Security Information and Event Management). SIEM забезпечує централізований збір, зберігання та аналіз журналів подій із різних компонентів інформаційного середовища [8]. Джерелами даних для SIEM можуть бути сервери, мережеве обладнання, міжмережеві екрани, системи управління доступом, прикладні сервіси, хмарні платформи та кінцеві пристрої користувачів.

Використання SIEM-систем дозволяє організації:

- здійснювати централізований моніторинг подій безпеки;
- автоматизувати виявлення інцидентів;
- забезпечувати журналювання та аудит подій;
- формувати доказову базу відповідності регуляторним вимогам;
- скорочувати час реагування на кіберінциденти;
- забезпечувати кореляцію подій безпеки з різних джерел.

Для організацій із високими вимогами до інформаційної безпеки централізоване журналювання подій є важливим елементом забезпечення відповідності міжнародним стандартам та нормативним вимогам. Особливо це актуально для банківського сектору, де необхідно забезпечувати відповідність вимогам Національного банку України, ISO/IEC 27001 та PCI DSS [24].

Важливу роль у сучасному проактивному захисті відіграють системи Endpoint Detection and Response (EDR). EDR-рішення забезпечують моніторинг активності кінцевих пристроїв, аналіз поведінки процесів, виявлення шкідливого програмного забезпечення та реагування на інциденти безпеки [25]. На відміну від традиційних антивірусних рішень, EDR використовує поведінковий аналіз та механізми виявлення аномалій, що дозволяє ефективніше виявляти складні сучасні атаки.

Подальшим розвитком EDR-технологій стали системи Extended Detection and Response (XDR), які забезпечують інтеграцію даних із різних джерел інформаційного середовища: кінцевих пристроїв, серверів, мережевої інфраструктури, електронної пошти та хмарних сервісів [26]. Використання XDR дозволяє організації отримати цілісне уявлення про події інформаційної безпеки та підвищити ефективність виявлення складних багатовекторних атак.

Суттєву роль у функціонуванні сучасних SOC відіграють платформи Security Orchestration, Automation and Response (SOAR). SOAR-системи забезпечують автоматизацію процесів реагування на інциденти, оркестрацію взаємодії між засобами захисту та виконання типових сценаріїв реагування без участі оператора [27].

Використання SOAR дозволяє:

- автоматизувати обробку інцидентів;
- скоротити час реагування на загрози;
- стандартизувати процеси реагування;
- знизити навантаження на аналітиків SOC;
- підвищити ефективність функціонування систем моніторингу.

Одним із ключових напрямів розвитку сучасного проактивного кіберзахисту є використання Threat Intelligence. Threat Intelligence являє собою процес збору, аналізу та використання інформації про актуальні кіберзагрози, індикатори компрометації, тактики та методи проведення атак. Використання Threat Intelligence дозволяє організаціям адаптувати механізми захисту до актуального ландшафту кіберзагроз та підвищити ефективність виявлення атак.

У межах діяльності SOC інформація Threat Intelligence використовується для оновлення правил кореляції SIEM-систем, виявлення індикаторів компрометації та підтримки процесів Threat Hunting. Threat Hunting являє собою процес активного пошуку прихованих загроз та аномальної активності в інформаційному середовищі організації [29]. На відміну від традиційного моніторингу Threat Hunting передбачає проактивний аналіз поведінки користувачів, мережевої активності та системних подій із метою виявлення складних або невідомих атак.

Важливим елементом проактивного захисту є процес управління вразливостями (Vulnerability Management). Управління вразливостями включає виявлення, оцінювання, пріоритизацію та усунення вразливостей програмного забезпечення та інформаційних систем [30]. Регулярне проведення сканування вразливостей та контроль безпечності конфігурацій дозволяють знизити ризик успішної реалізації кіберзагроз.

Для підвищення ефективності виявлення аномальної активності сучасні організації використовують системи User and Entity Behavior Analytics (UEBA). UEBA-рішення забезпечують аналіз поведінки користувачів та пристроїв із використанням алгоритмів машинного навчання та дозволяють виявляти нетипову активність, яка може свідчити про компрометацію облікових записів або внутрішні загрози [31].

У контексті сучасного кіберзахисту важливе значення має концепція Defense in Depth, яка передбачає використання багаторівневого захисту інформаційного середовища [19]. Реалізація цієї концепції базується на поєднанні технічних, організаційних та процедурних механізмів безпеки на різних рівнях інфо-

рмаційної інфраструктури. Поєднання SIEM, EDR/XDR, SOAR, систем контролю доступу, мережевих засобів захисту та систем моніторингу дозволяє створити комплексну систему кіберзахисту.

Сучасні проактивні засоби захисту тісно пов’язані з процесами системи менеджменту інформаційної безпеки. Відповідно до ISO/IEC 27001:2022 СМІБ повинна забезпечувати постійний моніторинг ризиків, оцінювання ефективності заходів безпеки та безперервне вдосконалення процесів захисту інформації [12]. Саме Security Operations Center та сучасні системи моніторингу забезпечують практичну реалізацію зазначених вимог.

Для організацій, що функціонують в умовах підвищених регуляторних вимог, особливого значення набуває забезпечення постійного контролю інформаційного середовища та документування подій безпеки. У банківському секторі вимоги до моніторингу подій інформаційної безпеки, реагування на інциденти та управління кіберризиками визначаються нормативними документами Національного банку України та міжнародними стандартами інформаційної безпеки.

Ефективне забезпечення захисту інформаційного середовища організації базується не лише на використанні технічних засобів захисту, але й на впровадженні комплексних методів управління інформаційною безпекою. У сучасних умовах найбільш результативними є методи, що поєднують організаційні, технічні та аналітичні підходи до виявлення, попередження та мінімізації кіберзагроз.

Одним із базових методів забезпечення інформаційної безпеки є ризик-орієнтований підхід, який використовується в межах системи менеджменту інформаційної безпеки відповідно до вимог ISO/IEC 27001:2022. Даний метод передбачає ідентифікацію інформаційних активів, аналіз потенційних загроз і вразливостей, оцінювання рівня ризику та впровадження відповідних заходів контролю. Основною перевагою ризик-орієнтованого підходу є можливість пріоритезації ресурсів безпеки та концентрації уваги на найбільш критичних компонентах інформаційного середовища.

Важливим методом забезпечення захисту інформаційного середовища є безперервний моніторинг подій інформаційної безпеки. Даний підхід реалізується за допомогою Security Operations Center (SOC), SIEM-платформ, систем аналізу журналів подій та засобів автоматизованого реагування на інциденти. Метод безперервного моніторингу забезпечує оперативне виявлення аномальної активності, контроль дій користувачів, виявлення спроб несанкціонованого доступу та формування доказової бази для аудиту інформаційної безпеки.

Одним із найбільш ефективних сучасних методів захисту інформаційного середовища є концепція Zero Trust Architecture. Вона базується на принципі «ніколи не довіряй – завжди перевіряй» та передбачає постійну автентифікацію і перевірку користувачів, пристроїв та сервісів незалежно від їх місця розташування у мережі. Реалізація Zero Trust включає використання багатофакторної автентифікації, сегментації мережі, контролю привілейованого доступу та моніторингу поведінки користувачів.

Не менш важливим методом є багаторівневий захист Defense in Depth, який передбачає використання декількох незалежних рівнів захисту інформаційного середовища. У межах цього підходу одночасно застосовуються міжмережеві екрани, системи IDS/IPS, EDR/XDR-рішення, антивірусні системи, DLP-платформи, криптографічний захист та резервне копіювання. Основною перевагою Defense in Depth є підвищення стійкості інформаційної інфраструктури навіть у випадку компрометації окремого механізму захисту.

Окрему роль у системах захисту відіграють методи автоматизації реагування на інциденти інформаційної безпеки. Використання SOAR-платформ дозволяє автоматизувати обробку сповіщень, створення інцидентів, виконання сценаріїв реагування та підготовку звітності для регуляторних органів. Автоматизація значно скорочує час реагування на інциденти та знижує навантаження на аналітиків SOC.

Важливим методом забезпечення безпеки інформаційного середовища є управління вразливостями. Даний метод передбачає регулярне сканування інформаційної інфраструктури, виявлення вразливостей програмного забезпечення,

оцінювання рівня критичності та контроль усунення недоліків безпеки. У організаціях для реалізації цього підходу використовуються платформи Qualys, Nessus, Rapid7 та інші системи vulnerability management.

Також важливим елементом захисту є методи підвищення обізнаності персоналу у сфері інформаційної безпеки. Навіть за наявності сучасних технічних засобів захисту людський фактор залишається однією з основних причин виникнення інцидентів інформаційної безпеки. Саме тому організації впроваджують програми Security Awareness, навчання персоналу, симуляції фішингових атак та політики контролю доступу.

Таким чином, проактивні засоби захисту інформаційного середовища є основою сучасної системи забезпечення інформаційної безпеки організації. Використання SIEM, EDR/XDR, SOAR, Threat Intelligence, Threat Hunting та інших технологій дозволяє забезпечити безперервний моніторинг інформаційного середовища, своєчасне виявлення кіберзагроз та ефективне реагування на інциденти. Центральну роль у реалізації проактивного підходу до забезпечення інформаційної безпеки відіграє Security Operations Center, який виступає операційним середовищем підтримки процесів системи менеджменту інформаційної безпеки та забезпечення відповідності регуляторним вимогам.

Аналіз практики банківського сектору дозволяє виокремити три принципово різних підходи до забезпечення відповідності СМІБ регуляторним вимогам: реактивний, проактивний та безперервний (SOC-based). Кожен підхід відрізняється ступенем зрілості процесів, технологічним забезпеченням та здатністю підтримувати відповідність у динамічному середовищі кіберзагроз. Разом з тим, ефективність будь-якого підходу до відповідності СМІБ нерозривно пов'язана з вибором архітектурних концепцій безпеки, що лежать в основі захисту інформаційного середовища [13].

Реактивний підхід до забезпечення відповідності характеризується мінімальним технологічним забезпеченням та орієнтацією на формальне виконання вимог перед плановими аудитами. Банки, що використовують цей підхід, як правило, готують документацію «під аудит», ручно агрегуючи дані з різних систем.

Оцінка відповідності здійснюється раз на рік або безпосередньо перед регуляторною перевіркою. Ризик регуляторних санкцій при цьому є максимальним, оскільки реальний стан відповідності між аудитами залишається невідомим. Рівень зрілості за моделлю CMMI відповідає першому рівню (Chaotic / Initial) [20].

Проактивний підхід передбачає регулярні планові внутрішні аудити (щоквартально), використання GRC-систем для управління відповідністю та часткову автоматизацію збору доказів. Банки цього рівня мають систематизований реєстр ризиків та контролів, проте оцінка відповідності залишається дискретною: між плановими перевірками можуть накопичуватися невідповідності. Рівень зрілості – 2–3 за CMMI (Managed/Defined).

Безперервний (SOC-based) підхід є найвищим рівнем зрілості управління відповідністю. Він ґрунтується на концепції Continuous Compliance («комплаєнс як код»), де вимоги регуляторів формалізовані у вигляді технічних правил та перевірок, що автоматично виконуються у реальному часі. SOC реалізує цю концепцію через написання SIEM-правил кореляції, що безпосередньо відображають вимоги конкретних контролів СМІБ; налаштування compliance-дашборду з індикацією «зелений/жовтий/червоний» для кожного контролю; а також автоматичну генерацію сповіщень при виявленні «compliance drift» – відхилення від цільового стану відповідності [14]. Порівняльний аналіз трьох підходів наведено у табл. 1.2.

Таблиця 1.2

Порівняльний аналіз підходів до забезпечення відповідності СМІБ

Критерій оцінювання	**Реактивний підхід**	**Проактивний підхід**	**Безперервний (SOC-based) підхід**
Частота оцінки стану відповідності	Раз на рік або лише при аудиті НБУ/ISO	Щоквартально (планові внутрішні аудити)	24/7 у режимі реального часу – безперервний моніторинг
Час виявлення невідповідності (drift)	Місяці – до моменту проведення аудиту	Тижні – між плановими перевірками	Хвилини – автоматичний compliance drift alert при відхиленні від норми
Якість доказової бази	Фрагментована, підготовлена вручну; висока ймовірність неузгодженостей та пропусків	Часткова, напівавтоматична; краща узгодженість, але ручна підготовка звітів	Повна, автоматизована, незмінна (immutable logs); структурований Аудиторський портал

Продовження таблиці 1.2

Вартість регуляторних санкцій (ризик)	Висока: штрафи НБУ, втрата PCI DSS статусу, репутаційні збитки, можливе відкликання ліцензії	Середня: проблеми виявляються до аудиту, але інциденти у міжаудитні periodи можливі	Мінімальна: раннє виявлення, автоматичне усунення до накопичення критичної маси невідповідностей
Технологічне забезпечення	Excel, Word, ручна документація; відсутня інтеграція між засобами захисту	GRC-система, часткова автоматизація звітності; базова інтеграція SIEM	SIEM + SOAR + GRC + EDR + TI + VM; повна оркестрація та автоматизація доказів
Відповідність вимогам НБУ №95	Формальна – мінімальні дії для проходження перевірки	Часткова – плановий комплаєнс без безперервного моніторингу	Повна – включно з автоматичним дотриманням 72-год. строку звітування
Відповідність ISO 27001, п. 9.1	Формальна – відсутнє фактичне вимірювання ефективності	Задовільна – вимірювання проводяться, але нерегулярно	Повна – безперервне вимірювання KPI/KRI та автоматичні Management Review звіти
Рівень зрілості СМІБ (CMMI)	Рівень 1: початковий (Chaotic)	Рівень 2–3: керований / визначений (Managed/Defined)	Рівень 4–5: кількісно керований / оптимізований (Quantitatively Managed/Optimizing)

У контексті вибору підходу до забезпечення відповідності СМІБ особливу роль відіграють дві сучасні архітектурні концепції кіберзахисту – Zero Trust Architecture та Defense in Depth. Їх практичне застосування суттєво впливає на ефективність функціонування SOC та рівень відповідності СМІБ регуляторним вимогам.

Концепція Zero Trust Architecture (ZTA) базується на принципі «ніколи не довіряй – завжди перевіряй» (Never Trust, Always Verify) та передбачає постійну перевірку автентичності та авторизації кожного користувача, пристрою та мережевого запиту незалежно від їх розташування у мережі [18]. Відповідно до NIST SP 800-207, ключовими компонентами Zero Trust є ідентифікація та управління доступом (IAM) на основі багатофакторної автентифікації, мікросегментація мережі для обмеження бокового переміщення зловмисника (lateral movement), а також безперервний моніторинг та верифікація всіх сесій доступу.

З точки зору СМІБ, реалізація Zero Trust безпосередньо підтримується функціями SOC. SIEM-система у рамках ZTA моніторить аномалії автентифікації (наприклад, вхід з нетипового місцезнаходження або в нетиповий час), що є реалізацією контролу A.8.16 («Моніторинг»). UEBA-модуль визначає поведінкові базиси кожного користувача та виявляє відхилення, що свідчать про компрометацію облікового запису. Мікросегментація мережі обмежує зону ураження у разі успішної атаки та відповідає принципу «мінімальних привілеїв» (Least Privilege), закріпленому в контролах A.5.15 та A.5.18 ISO/IEC 27001:2022 [18].

Концепція Defense in Depth (багаторівневий захист, або «ешелонована оборона») передбачає використання декількох незалежних рівнів захисту інформаційного середовища таким чином, що подолання зловмисником одного рівня не призводить до компрометації всієї системи [19]. У банківському контексті Defense in Depth реалізується через поєднання мережевого захисту (NGFW, IDS/IPS, мікросегментація), захисту кінцевих точок (EDR/XDR, антивірус, шифрування дисків), контролю доступу (IAM, PAM, MFA), захисту даних (DLP, шифрування at rest та in transit), а також безперервного моніторингу (SIEM, SOAR) як останнього рівня виявлення.

Взаємозв'язок концепцій ZTA та Defense in Depth з операційними функціями SOC є двостороннім. З одного боку, SOC забезпечує технічну реалізацію цих концепцій через моніторинг їх ефективності та своєчасне виявлення порушень. З іншого боку, самі концепції визначають архітектурну основу, на якій будується SOC. Відповідність СМІБ регуляторним вимогам в умовах ZTA та Defense in Depth суттєво зростає, оскільки кожен рівень захисту генерує власну телеметрію, що збагачує загальну картину подій безпеки в SIEM та підвищує точність виявлення загроз [19].

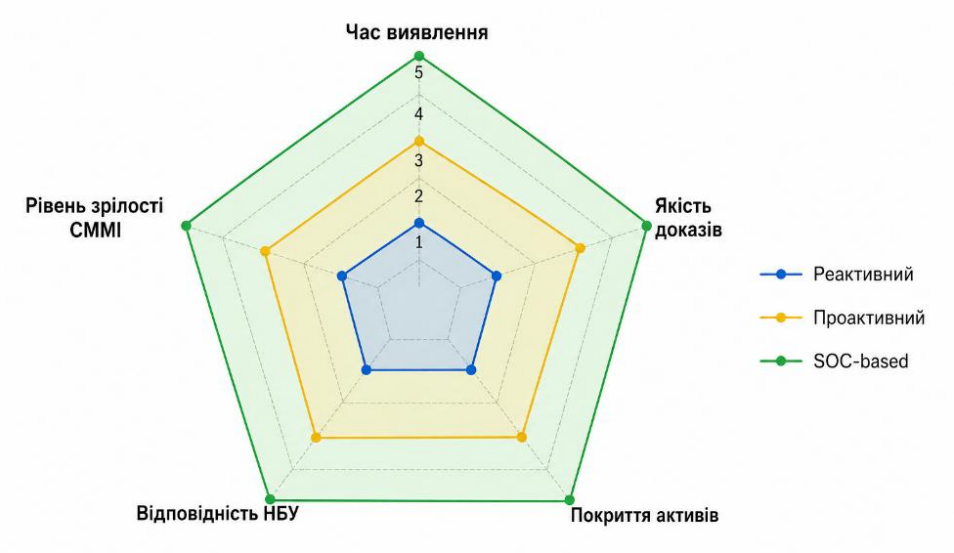

Рис. 1.1. Зіставлення підходів до комплаєнсу СМІБ за критеріями зрілості та ефективності

Висновок до розділу 1

Перший розділ встановив теоретичний фундамент дослідження, визначивши ключові характеристики інформаційного середовища банківської установи та систему регуляторних вимог, у межах яких воно функціонує. Проведений аналіз підтвердив, що сучасний банк діє в умовах складного та багаторівневого нормативного поля, де одночасно діють Постанова НБУ №95, міжнародний стандарт ISO/IEC 27001:2022, стандарт платіжної індустрії PCI DSS v4.0 та GDPR. Кожен із цих регуляторів висуває специфічні, але взаємодоповнюючі вимоги до процесів моніторингу, журналювання, управління інцидентами та формування доказової бази відповідності.

Дослідження нормативних вимог до SOC та СМІБ показало, що жодна з ключових регуляторних вимог – безперервний моніторинг подій безпеки, 72-годинне звітування про кіберінциденти, щоквартальне сканування вразливостей – не може бути системно виконана без функціонуючого Security Operations Center. Таким чином, SOC виступає не лише інструментом технічного захисту, але й операційною платформою, що забезпечує виконання регуляторних обов'язків банку.

Аналіз існуючих методів захисту інформаційного середовища та підходів до забезпечення відповідності СМІБ виявив принципову відмінність між реактивним «аудитним» комплаєнсом та концепцією безперервної відповідності (Continuous Compliance). Реактивний підхід, за якого банк підтверджує відповідність раз на рік, є системно неефективним в умовах динамічного регуляторного середовища. Це зумовлює необхідність розробки методики, що забезпечить постійне підтвердження відповідності на основі операційної діяльності SOC, що й стало предметом подальшого дослідження.

Розділ 2. АНАЛІЗ ІНСТРУМЕНТАРІЮ ЗАХИСТУ ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА ТА РОЛІ SOC У ЗАБЕЗПЕЧЕННІ ВИМОГ СМІБ

2.1 Аналіз засобів захисту інформаційного середовища підприємства

Організації, що функціонують в умовах підвищених регуляторних вимог, зокрема банківський сектор, потребують комплексного підходу до формування системи захисту інформаційного середовища. Аналіз сучасних засобів захисту інформаційного середовища неможливий без розгляду архітектури та операційної моделі Security Operations Center (SOC) як організаційно-технічного ядра, що інтегрує всі компоненти системи безпеки в єдиний керований механізм [13].

Security Operations Center являє собою спеціалізований організаційно-технічний підрозділ, основним призначенням якого є безперервний моніторинг, виявлення, аналіз та координація реагування на інциденти інформаційної безпеки. З точки зору СМІБ відповідно до ISO/IEC 27001:2022 SOC виступає операційним ядром «Check»-фази циклу PDCA. Саме тут відбувається вимірювання ефективності функціонуючих засобів захисту та збір верифікованих доказів відповідності регуляторним вимогам [12].

Архітектурно SOC є трирівневою операційною структурою, де кожен рівень виконує чітко визначені функції, забезпечуючи ефективний розподіл навантаження та спеціалізацію аналітиків. Розуміння цієї структури є ключовим для оцінки здатності SOC забезпечувати вимоги СМІБ щодо управління інцидентами та безперервного моніторингу [22].

Перший рівень — L1 (Triage Analysts) — є першою лінією захисту та виконує роль фільтра між загальним потоком подій і процесом реагування. Аналітики L1 здійснюють цілодобовий моніторинг алертів SIEM-системи, виконують первинну класифікацію кожної події (malware, phishing, brute force, аномалія тощо), збирають базовий контекст — IP-адреси, часові мітки, задіяні хости — та прий-

мають рішення про ескалацію на другий рівень. Аналітики L1 не проводять глибокого розслідування: їхнє завдання полягає у відокремленні реального інциденту від хибного спрацювання. Надмірна кількість хибних спрацювань (False Positive Rate > 30%) є критичним показником, що свідчить про неефективне налаштування правил кореляції SIEM.

Другий рівень — L2 (Incident Responders) — є детективним щаблем SOC. Аналітики L2 отримують ескальовані інциденти і проводять повноцінне розслідування: відновлюють хронологію атаки, визначають вектор компрометації, оцінюють масштаб ураження інфраструктури. Реагування на інцидент включає ізоляцію заражених хостів, блокування шкідливих IP-адрес і доменів, ініціювання скидання скомпрометованих облікових записів, а також взаємодію з власниками систем та IT-підрозділом. На основі проведених розслідувань аналітики L2 здійснюють тюнінг правил детектування у SIEM та оновлюють сигнатури IDS/IPS. Саме аналітики L2 несуть безпосередню відповідальність за дотримання 72-годинного строку повідомлення Національного банку України про суттєві кіберінциденти відповідно до Постанови №95.

Третій рівень — L3 (Threat Hunters / Senior Analysts) — є елітним щаблем операційної зрілості SOC. На відміну від L1 та L2, аналітики третього рівня не чекають спрацювання алерту, а самостійно проводять проактивний пошук прихованих загроз (Threat Hunting): формулюють гіпотезу щодо можливої присутності зловмисника в інфраструктурі, розробляють методику перевірки та виконують пошук за даними телеметрії. До функцій L3 також належать аналіз шкідливого програмного забезпечення (реверс-інжиніринг), розроблення складних кореляційних правил, Sigma- та YARA-правил, які використовуються рівнями L1 та L2. Аналітики L3 визначають пріоритети покриття фреймворку MITRE ATT&CK, беруть участь в оцінці зрілості SOC та формують стратегічні рекомендації щодо розвитку системи захисту [29].

Зазначена структура безпосередньо кореспондує з вимогами ISO/IEC 27001:2022 щодо розподілу обов’язків та відповідальності (п. 5.3), управління ін-

цидентами (контрол A.5.26), збору та збереження доказів (A.5.28) та забезпечення безперервного моніторингу (A.8.16). У табл. 2.1 систематизовано трирівневу операційну структуру SOC у зіставленні з процесами СМІБ та ключовими показниками ефективності.

Таблиця 2.1.

Трирівнева операційна структура SOC та відповідність процесам СМІБ

Рівень SOC	**Ролі та основні функції**	**Процеси СМІБ (ISO/IEC 27001)**	**Показники ефективності (KPI)**
L1 – Triage (Первинний аналітик)	Моніторинг алертів SIEM у режимі 24/7; Первинна класифікація подій; Збір базового контексту (IoC, хости, часові мітки); Ескалація до L2; Ведення журналу звернень	A.8.15 — Ведення журналів; A.8.16 — Моніторинг діяльності; A.5.25 — Оцінка подій безпеки	Час первинної класифікації < 15 хв.; False Positive Rate < 20%; Охоплення моніторингом активів > 95%
L2 – Investigation (Аналітик з реагування)	Глибоке розслідування підтверджених інцидентів; Відновлення хронології атаки; ізоляція хостів та Блокування загроз; тюнінг правил Детектування; підготовка звітів для НБУ	A.5.26 — Реагування на інциденти; A.5.28 — Збір доказів; A.5.27 — Висновки з інцидентів	MTTR (критичні) < 4 год.; Дотримання 72-год. строку для НБУ — 100%; Повнота документування — 100%
L3 – Threat Hunting / Senior Analyst	Проактивний пошук прихованих загроз; Аналіз шкідливого ПЗ (реверс-інжиніринг); Розроблення Sigma/YARA-правил; стратегічний розвиток SOC; Оцінка зрілості та покриття MITRE ATT&CK	A.5.7 — Threat Intelligence; A.8.8 — Управління технічними вразливостями; A.5.29 — Безперервність ІБ	Виявлені приховані загрози на квартал; Нові detection rules ≥ 5/квартал; Покриття TTP MITRE ATT&CK > 60%

Важливим концептуальним аспектом є розмежування між SOC як підрозділом та SOC як набором процесів і технологій. SOC-as-a-function реалізується у трьох організаційних моделях, кожна з яких має суттєві відмінності з точки зору

можливості забезпечити відповідність СМІБ регуляторним вимогам. Вибір моделі є стратегічним рішенням для кожного банку та визначає баланс між рівнем контролю над даними, операційною зрілістю та фінансовими витратами [5].

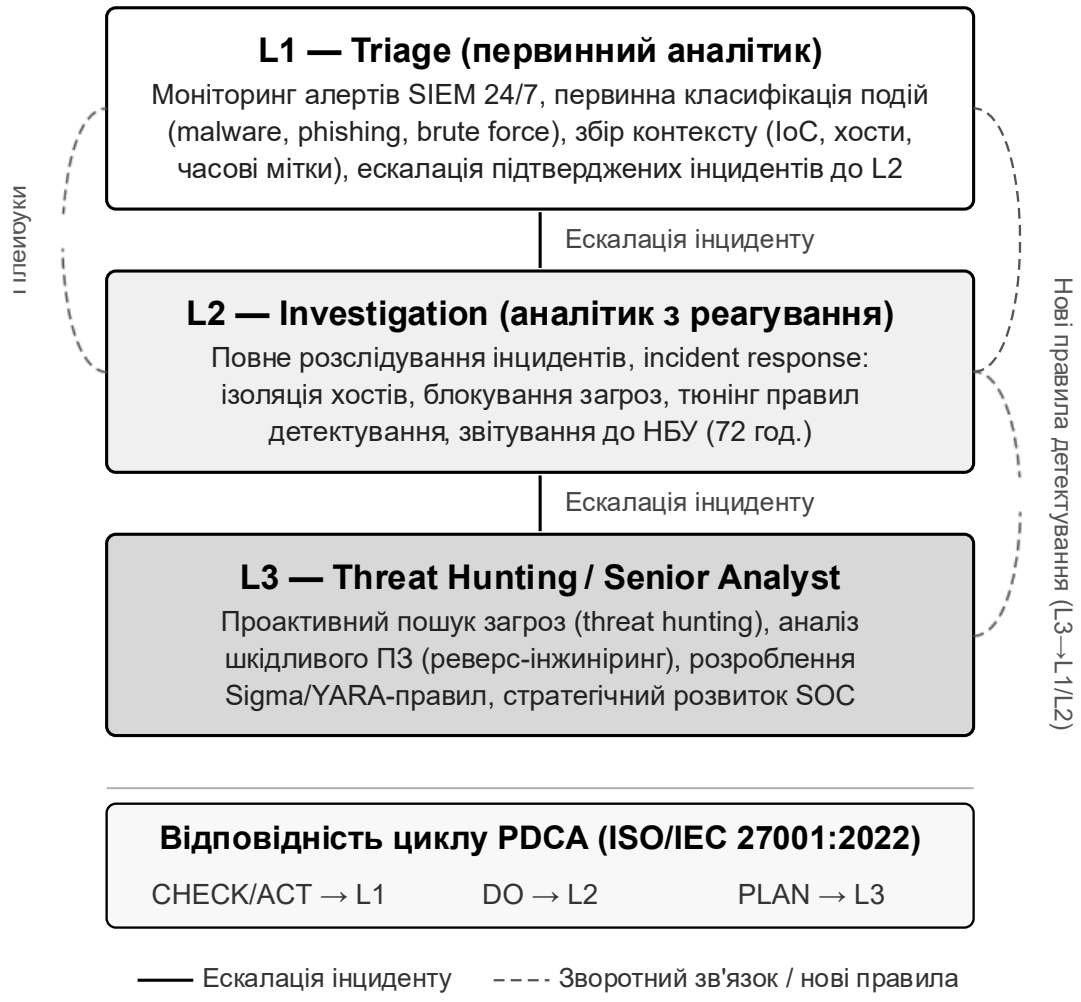

Рис. 2.1. Трирівнева операційна структура SOC (Tier Model) та її взаємодія з циклом PDCA СМІБ

Вибір організаційної моделі побудови SOC є одним із ключових стратегічних рішень у сфері інформаційної безпеки банку, яке безпосередньо впливає на спроможність організації виконувати регуляторні вимоги, забезпечувати відповідність СМІБ та захищати конфіденційні дані клієнтів. Аналіз трьох основних моделей – In-house SOC, MSSP та гібридна модель – дозволяє виявити ключові переваги та недоліки кожного підходу з урахуванням специфіки банківського сектору України [4].

Модель In-house SOC передбачає повне розгортання та управління інфраструктурою, персоналом і процесами безпеки силами самого банку. Команда SOC є штатними співробітниками банку, а всі дані обробляються виключно у внутрішній інфраструктурі. Ця модель забезпечує максимальний контроль над конфіденційністю даних, що є критичною перевагою для банків з огляду на вимоги банківської таємниці відповідно до статті 60 Закону України «Про банки і банківську діяльність», GDPR та Постанови НБУ №95. Відсутність передачі телеметрії та журналів подій зовнішнім сторонам усуває правові ризики, пов'язані з обробкою персональних даних та банківської таємниці.

Однак побудова In-house SOC вимагає значних капітальних та операційних інвестицій. Початкові витрати на ліцензування SIEM-платформи рівня enterprise (IBM QRadar, Splunk Enterprise Security, Microsoft Sentinel) становлять від 200 тисяч до 1 мільйона USD залежно від обсягу телеметрії та набору модулів. Додатково необхідно враховувати витрати на апаратну інфраструктуру, утримання команди кваліфікованих аналітиків (дефіцит якої є гострою проблемою на ринку праці у сфері кібербезпеки) та постійне навчання персоналу. За оцінками Gartner [5], повна вартість власності (TCO) In-house SOC для середнього банку становить від 1,5 до 4 мільйонів USD щорічно.

Модель MSSP (Managed Security Service Provider) передбачає передачу функцій моніторингу та реагування зовнішньому постачальнику послуг безпеки. Для банків ця модель є привабливою насамперед з точки зору швидкості розгортання (від одного до трьох місяців) та можливості отримати зрілі процеси безпеки без тривалого організаційного будівництва. Проте для банківського сектору MSSP-модель несе суттєві регуляторні ризики, пов'язані з передачею даних третій стороні. По-перше, передача журналів подій та телеметрії до зовнішнього MSSP фактично є передачею даних третій стороні, що вимагає ретельного правового аналізу на предмет відповідності вимогам банківської таємниці. По-друге, відповідно до статті 45 GDPR, передача персональних даних до третіх країн допустима лише за наявності рішення про достатній рівень захисту або стандарт-

них договірних положень. Угода про рівень послуг з MSSP повинна містити детальні положення про захист даних (Data Processing Agreement) відповідно до статті 28 GDPR [18].

З точки зору ISO/IEC 27001:2022, залучення MSSP відповідає концепції управління ризиками постачальника (Supplier Relationships, контроли A.5.19–A.5.22). Банк залишається власником ризику, тому угода про рівень послуг має включати зобов'язання MSSP щодо повідомлення про інциденти у строки, що відповідають вимогам НБУ (72 години), а також права банку на проведення аудиту MSSP.

Гібридна модель поєднує елементи In-house та MSSP: банк утримує власну команду аналітиків L2/L3, яка відповідає за критичні розслідування та стратегічний розвиток SOC, а рутинний моніторинг L1 та базовий збір телеметрії делегуються MSSP-провайдеру. Дана модель є оптимальною для більшості банків середнього розміру в Україні з огляду на баланс витрат, рівня контролю та регуляторної відповідності. У гібридній моделі критично важливим є чіткий розподіл обов'язків (RACI-матриця) між внутрішньою командою та MSSP, а також умова збереження всіх інструментів SOC (SIEM, SOAR) у власності банку, що забезпечує повний контроль над даними [6].

У табл. 2.2 наведено розгорнутий порівняльний аналіз трьох моделей побудови SOC з урахуванням специфіки регуляторного середовища банківського сектору України.

Окремої уваги заслуговує питання ефективності основних технологічних засобів захисту, що використовуються у середовищі SOC. Систематизований огляд переваг та недоліків ключових класів інструментів дозволяє оцінити їх роль у формуванні доказової бази відповідності СМІБ.

Системи класу SIEM (Security Information and Event Management) є центральним елементом технологічного стека SOC. Їх головною перевагою є здатність до централізованого збору та кореляції журналів подій з гетерогенної банківської

інфраструктури – від автоматизованих банківських систем (АБС) і систем дистанційного банківського обслуговування (ДБО) до хмарних платформ та мережевого обладнання.

Таблиця 2.2

Порівняльний аналіз моделей побудови SOC для банківського сектору України

Критерій порівняння	In-house SOC (власний)	MSSP (зовнішній)	Гібридна модель
Контроль над даними та конфіденційністю	Повний – усі дані в інфраструктурі банку; Максимально відповідає банківській таємниці (ст. 60 ЗУ «Про банки і банківську діяльність»)	Обмежений – дані передаються зовнішньому провайдеру; Потребує детального DPA згідно ст. 28 GDPR	Частковий – критичні та чутливі дані залишаються в банку; Некритичні потоки – у MSSP
Початкові витрати (TCO)	Дуже високі: ліцензії SIEM enterprise-рівня (IBM QRadar, Splunk ES) – 200 тис. – 1 млн USD; Утримання команди; TCO 1,5–4 млн USD/рік (Gartner)	Відносно низькі – SLA-модель оплати без капітальних інвестицій; Ризик «vendor lock-in»	Середні – поєднання капітальних інвестицій у власну інфраструктуру L2/L3 та операційних витрат на MSSP L1
Швидкість розгортання	12–24 місяці: підбір персоналу, впровадження технологій, розробка процесів	1–3 місяці: MSSP використовує готову інфраструктуру та процеси	3–9 місяців: компроміс між зрілістю MSSP та розвитком власної L2/L3 команди
Відповідність банківській таємниці (ст. 60 ЗУ)	Повна – дані не залишають інфраструктуру банку	Умовна – вимагає ретельного правового аналізу SLA та DPA; Регуляторний ризик	Висока – при умові збереження журналів критичних систем (АБС, ДБО) всередині банку
Дотримання вимог НБУ №95 (72 год.)	Повна – пряма відповідальність власної команди SOC	Залежить від SLA з MSSP; Ризик затримки ескалації	Повна – внутрішня L2-команда контролює процес звітування до НБУ
Зрілість процесів на старті	Низька – процеси будуються з нуля; Ризик значного часу на становлення	Висока – MSSP використовує зрілі процеси та накопичений досвід	Середня – L1 процеси успадковані від MSSP; L2/L3 розвиваються
Кастомізація під специфіку банку	Максимальна – правила SIEM та плейбуки налаштовуються під конкретні системи (АБС, ДБО, процесинг)	Обмежена – MSSP використовує стандартні сценарії для фінансового сектору	Висока – L2/L3 кастомізують критичні сценарії; L1 використовує стандартні правила MSSP

Продовження таблиці 2.2

Оптимальний профіль банку	Великі системоутворюючі банки з активами > 50 млрд грн та розвиненим IT-підрозділом	Малі банки або банки на початковому етапі розвитку СМІБ з обмеженими ресурсами ІБ	Банки середнього розміру (активи 5–50 млрд грн); Оптимальний баланс витрат та контролю

Саме це робить SIEM незамінним інструментом для виконання контролю A.8.15 («Ведення журналів») та A.8.16 («Моніторинг») у версії ISO/IEC 27001:2022 [7]. Водночас SIEM-системи мають суттєвий недолік – складність налаштування правил кореляції та значна кількість хибних спрацювань (false positives) при неякісному «тюнінгу». Ненавчена SIEM може генерувати тисячі алертів на добу, що призводить до «alert fatigue» у аналітиків L1 та ризику пропустити справжні інциденти.

Системи EDR/XDR забезпечують захист кінцевих точок, проте їх ефективність в банківському середовищі обмежується наявністю застарілих операційних систем та спеціалізованих банківських терміналів, що не підтримують встановлення агентів. Для таких систем необхідним доповненням є мережевий моніторинг (Network Detection and Response, NDR). Платформи SOAR вирішують проблему швидкості реагування через автоматизацію, проте їх впровадження потребує значних початкових інвестицій у розробку плейбуків та інтеграцію з існуючими системами банку [27].

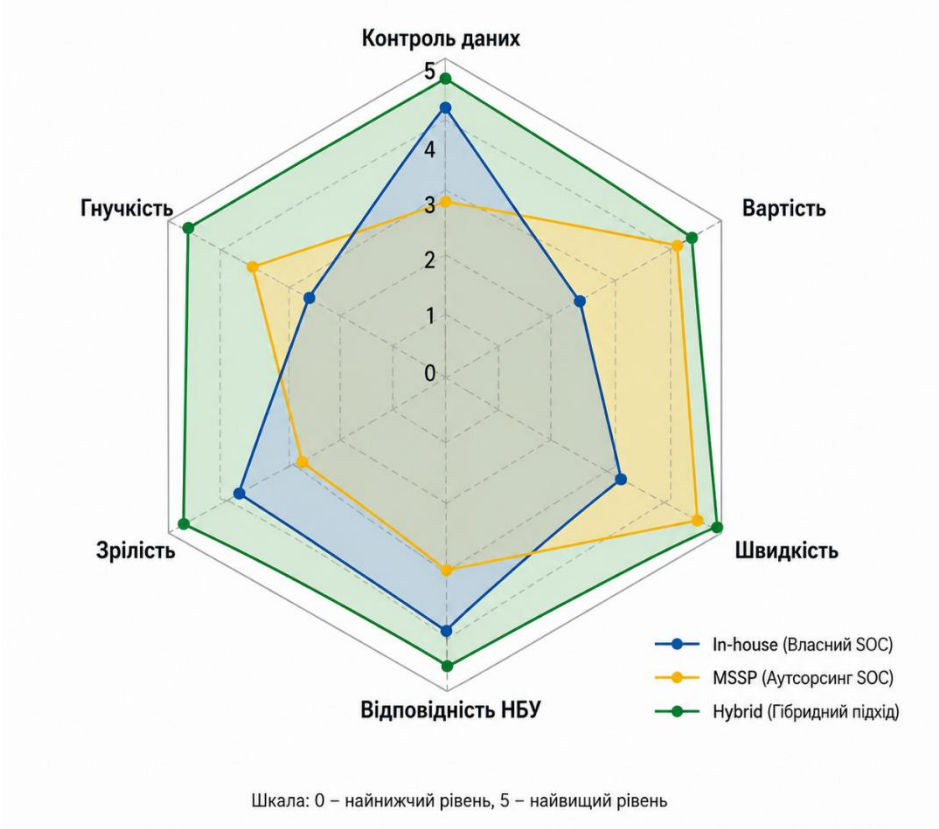

Рис. 2.2. Порівняльна діаграма ефективності моделей SOC за ключовими параметрами

2.2 Аналіз інструментальних засобів SOC: конкретні рішення та їх відповідність вимогам СМІБ

Технологічний стек SOC визначається набором взаємопов'язаних платформ і систем, кожна з яких виконує специфічні функції в загальній архітектурі забезпечення безпеки. У контексті СМІБ ці інструменти є не лише засобами захисту, але й джерелами доказів виконання контролів ISO/IEC 27001:2022, вимог НБУ та PCI DSS [8]. Нижче наведено детальний аналіз ключових технологічних компонентів SOC із зазначенням конкретних рішень, що найчастіше використовуються у банківському середовищі.

Серед провідних SIEM-рішень, що використовуються у фінансовому секторі, виокремлюють кілька платформ. IBM QRadar SIEM є одним із найпоширеніших рішень у великих банках та фінансових установах завдяки вбудованим use

cases для фінансової галузі, потужному модулю UEBA та здатності обробляти десятки мільярдів подій на добу. Splunk Enterprise Security – лідер ринку за гнучкістю та можливостями кастомізації; широко застосовується у банках з розвиненою аналітичною культурою завдяки власній мові запитів SPL та інтеграції з хмарними платформами. Microsoft Sentinel є хмарною SIEM-платформою, що забезпечує нативну інтеграцію з екосистемою Microsoft (Active Directory, Azure AD, Microsoft 365), що є актуальним для банків з переважно Windows-інфраструктурою; модель оплати «pay-per-GB» знижує вхідний поріг для банків середнього розміру. ArcSight Enterprise Security Manager (Micro Focus) традиційно використовується у великих фінансових установах із складною гетерогенною інфраструктурою, що функціонує роками без суттєвих архітектурних змін [23].

Для виконання вимог PCI DSS (вимога 10.5 – захист журналів аудиту від несанкціонованої зміни) SIEM повинна реалізовувати механізм незмінності журналів (log immutability) через запис у захищене сховище з WORM-семантикою (Write Once, Read Many). Вимога PCI DSS 10.7 вимагає зберігання журналів аудиту не менше 12 місяців, з оперативним доступом до даних за останні три місяці. Відповідно до Постанови НБУ №95, банки зобов'язані забезпечити зберігання записів про кіберінциденти протягом не менш ніж трьох років [24].

Системи класу EDR/XDR є обов'язковим компонентом SOC для захисту кінцевих точок банківської інфраструктури. CrowdStrike Falcon є найпоширенішим EDR-рішенням у глобальному фінансовому секторі завдяки хмарній архітектурі, що не впливає на продуктивність банківських систем, та вбудованому Threat Graph для кореляції загроз у реальному часі. Microsoft Defender for Endpoint широко використовується у банках з переважно Windows-інфраструктурою через нативну інтеграцію з Active Directory та групові політики безпеки. SentinelOne Singularity вирізняється вбудованим ШІ для автономного реагування без участі аналітика та здатністю відновлювати зашифровані програмами-здирниками файли (Rollback function) – критична функція для банків, де атаки ransomware можуть зупинити надання послуг [25].

SOAR-платформи кардинально підвищують ефективність роботи SOC через автоматизацію повторюваних задач реагування. Palo Alto Networks XSOAR (раніше Demisto) є лідером ринку з найбільшою бібліотекою готових інтеграцій та плейбуків для фінансової галузі, включаючи плейбуки для автоматичного звітування до регуляторів. Splunk SOAR забезпечує нативну інтеграцію з Splunk SIEM та єдиний робочий простір аналітика. Ключовою перевагою SOAR з точки зору СМІБ є автоматичне документування кожного кроку реагування з часовою міткою, що формує повний «ланцюжок доказів» (chain of custody) для аудиторів [27].

Окремої уваги заслуговують платформи Threat Intelligence, що забезпечують SOC структурованими даними про актуальні кіберзагрози. Recorded Future є провідною комерційною TI-платформою з глибокою аналітикою фінансового сектору, що дозволяє прогнозувати майбутні атаки на основі аналізу тенденцій у dark web та хакерських форумах. FS-ISAC (Financial Services Information Sharing and Analysis Center) є галузевою організацією, що надає специфічну розвідку про загрози виключно для фінансового сектору та є рекомендованим ресурсом відповідно до кращих практик НБУ. Використання TI безпосередньо пов'язане з контролем A.5.7 («Threat Intelligence») ISO/IEC 27001:2022, що є новим контролем, введеним у версії 2022 року [28].

Узагальнений огляд усього спектра інструментальних засобів SOC із систематизацією за класами рішень, контролями СМІБ та формами доказів відповідності наведено у табл. 2.3(Додатки).

Наведені в таблиці інструментальні засоби функціонують не ізольовано, а у взаємопов'язаній архітектурі, де кожен компонент виконує чітко визначену роль у циклі забезпечення відповідності. Архітектуру технологічного стека SOC та потоки даних між його ключовими підсистемами — SIEM, SOAR, TI та VM — і зовнішніми регуляторами проілюстровано на рис. 2.3.

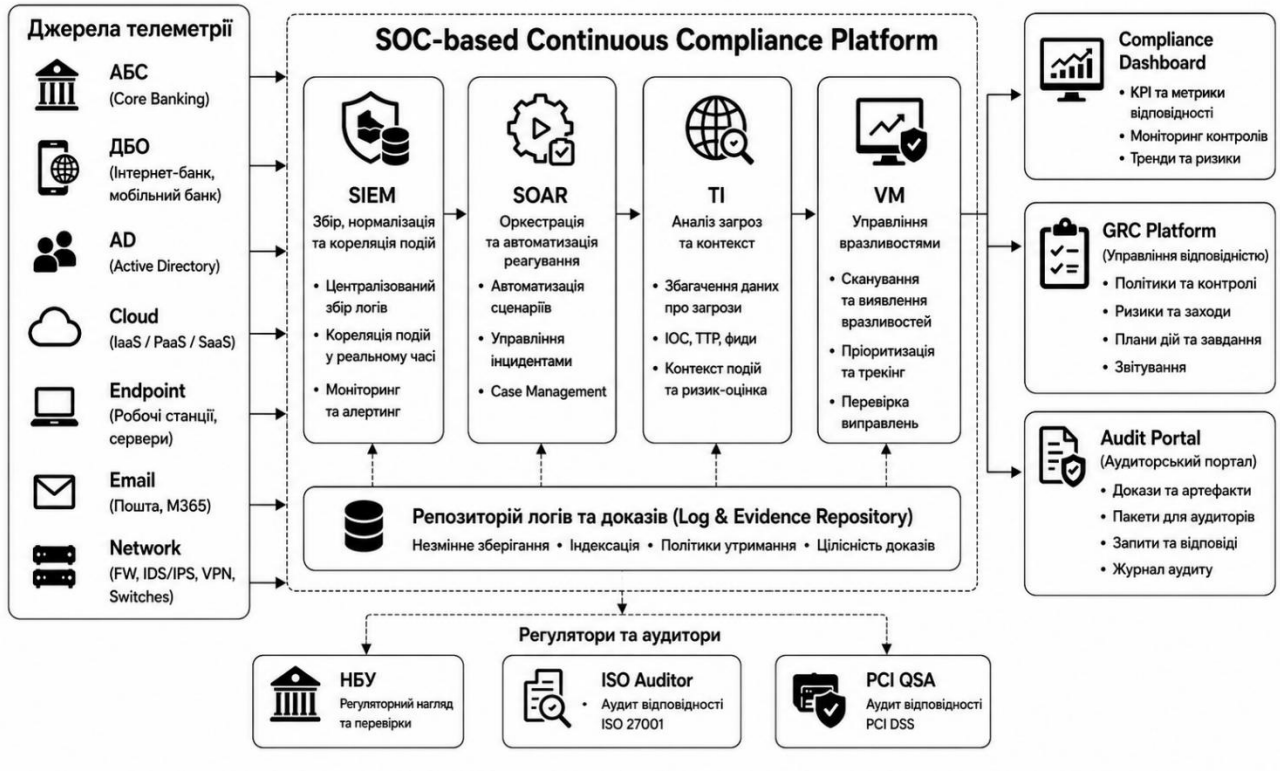

Рис. 2.3. Архітектура технологічного стека SOC та потоки даних між компонентами

2.3 Gap-аналіз підходів до відповідності СМІБ та роль SOC у подоланні виявлених розривів

Для оцінювання рівня відповідності системи менеджменту інформаційної безпеки регуляторним вимогам у роботі використано метод gap-аналізу. Вибір саме цього методу обумовлений його широким застосуванням у міжнародній практиці аудиту інформаційної безпеки, сертифікації ISO/IEC 27001 та оцінювання відповідності вимогам PCI DSS і нормативним документам НБУ. Gap-аналіз дозволяє виявити розриви між поточним станом процесів інформаційної безпеки організації та цільовими вимогами регуляторів або міжнародних стандартів.

Основною метою застосування gap-аналізу є визначення рівня зрілості процесів СМІБ, виявлення відсутніх або недостатньо реалізованих механізмів контролю, а також формування рекомендацій щодо усунення виявлених невідповідностей. Особливу увагу приділено процесам моніторингу, управління інцидентами, журналювання подій, реагування на кіберзагрози та формування доказової бази відповідності.

У межах дослідження gap-аналіз проводився шляхом порівняння:

- вимог ISO/IEC 27001:2022;
- вимог PCI DSS v4.0;
- положень НБУ №95;
- функціональних можливостей SOC;
- фактичного рівня реалізації процесів моніторингу та реагування.

Для виявлення розривів використовувався метод експертного порівняльного оцінювання, який базується на зіставленні вимог регуляторних документів із наявними процесами та інструментами забезпечення інформаційної безпеки. Кожен контроль або вимога оцінювалися за рівнем реалізації у межах організації.

У роботі застосовано шкалу оцінювання рівня відповідності:

- 0 – контроль відсутній;
- 1 – контроль реалізований частково;
- 2 – контроль реалізований повністю;
- 3 – контроль автоматизований та інтегрований у процеси SOC.

Основними показниками, які використовувалися під час gap-аналізу, є:

- рівень автоматизації моніторингу подій безпеки;
- наявність централізованого журналювання;
- швидкість виявлення інцидентів (MTTD);
- швидкість реагування на інциденти (MTTR);
- рівень покриття інформаційних активів моніторингом;
- наявність механізмів управління вразливостями;
- рівень інтеграції SIEM/SOAR-платформ;
- можливість формування доказової бази для аудиту.

Розриви визначалися як невідповідності між регуляторними вимогами та фактичним рівнем реалізації процесів інформаційної безпеки. Наприклад, відсутність централізованого збору журналів подій або автоматизованого реагування на інциденти розглядалася як критичний розрив, оскільки такі механізми є обов’язковими для виконання вимог ISO/IEC 27001, PCI DSS та нормативних документів НБУ.

Результати gap-аналізу показали, що найбільші розриви спостерігаються у таких напрямах:

- автоматизація реагування на інциденти;
- централізований моніторинг подій безпеки;
- управління журналами подій;
- інтеграція процесів SOC із СМІБ;
- контроль відповідності у режимі continuous compliance.

Використання Security Operations Center дозволяє суттєво скоротити виявлені розриви шляхом впровадження безперервного моніторингу, централізованого аналізу подій безпеки, автоматизованого реагування на інциденти та формування доказової бази відповідності регуляторним вимогам.

Gap-аналіз між поточним станом відповідності СМІБ та цільовим станом, що відповідає вимогам регуляторів, є обов'язковою процедурою в рамках пункту 6.1 ISO/IEC 27001. Проведений аналіз практики банківського сектору дозволив систематизувати ключові розриви, що типово виявляються у банках при впровадженні або сертифікаційному аудиті СМІБ, та визначити механізми SOC для їх усунення [32].

Першим та найбільш поширеним розривом є відсутність безперервного моніторингу подій безпеки. У більшості банків перевірка стану інформаційної безпеки здійснюється переважно «на момент аудиту», тоді як між аудитами інциденти не фіксуються систематично та не розслідуються. Наслідком є ситуація, коли банк формально відповідає вимогам під час перевірки, але фактично не контролює стан захищеності між аудитами. Це прямо суперечить вимогам НБУ №95

(Розділ VI) щодо оперативного виявлення та звітування про кіберінциденти, а також вимогам ISO/IEC 27001:2022 щодо безперервного моніторингу (A.8.16).

Другим системним розривом є ручне та фрагментоване формування доказів відповідності. Підготовка пакету документів до аудиту в більшості банків займає від двох до чотирьох тижнів і супроводжується значним ризиком людських помилок та неузгодженостей між різними системами. Аудитори ISO/IEC 27001 неодноразово фіксували ситуації, коли журнали SIEM свідчили про наявність підозрілих подій, що були проігноровані без документованого обґрунтування – і такі випадки ставали підставою для відмови у сертифікації.

Третім розривом є реактивне управління вразливостями. Значна частина банків усуває вразливості лише після їх реальної експлуатації або за результатами планових аудитів, тоді як стандарт PCI DSS v4.0 (вимога 11.3) вимагає проведення щоквартального автентифікованого сканування зовнішньої та внутрішньої інфраструктури, а також позапланового сканування після кожної суттєвої зміни в інфраструктурі. Відсутність задокументованих результатів сканування є підставою для втрати PCI DSS статусу та штрафних санкцій платіжних систем [17].

Четвертим розривом є фрагментованість доказової бази та відсутність кросплатформної кореляції подій. Навіть банки, що мають формально функціонуючі журнали подій в окремих системах (АБС, NGFW, Active Directory), часто не здатні відтворити повний ланцюг конкретного інциденту через відсутність інтеграції між цими системами. Аудитори ISO/IEC 27001 при Stage 2 аудиті вимагають саме цієї здатності – продемонструвати наскрізне відстеження інциденту від першої аномальної події до повного усунення наслідків.

П'ятим розривом є відсутність вимірюваних метрик ефективності засобів захисту. Більшість банків не можуть виміряти фактичну ефективність впроваджених засобів захисту та надати аудитору конкретні числові докази зниження ризиків. Відповідно до пункту 9.1 ISO/IEC 27001:2022 («Моніторинг, вимірювання, аналіз та оцінювання»), відсутність вимірювань є підставою для major nonconformity – критичної невідповідності, що унеможливлює отримання або

підтвердження сертифікату. Детальний аналіз усіх виявлених розривів та відповідних механізмів SOC для їх усунення наведено у табл. 2.4.

Таблиця 2.4.

Gap-аналіз відповідності СМІБ та механізми SOC для усунення виявлених розривів

Виявлений розрив (Gap)	**Прояв у банківській практиці**	**Ризик регуляторної невідповідності**	**Механізм SOC для усунення**	**Покриття контролем СМІБ**
Відсутність безперервного моніторингу подій безпеки	Перевірка стану ІБ здійснюється лише «на момент аудиту»;	НБУ №95, Розд. VI: невиконання вимоги оперативного звітування;	SIEM 24/7 збирає та корелює події з усієї інфраструктури; усі інциденти автоматично документуються з часовою міткою	ISO A.8.16 (Моніторинг); НБУ №95 Розд. V, VI
	Інциденти між аудитами не фіксуються і не розслідуються	Штрафні санкції або відкликання ліцензії		
Ручне формування доказів відповідності	Пакет документів до аудиту готується вручну 2–4 тижні; висока ймовірність неузгодженостей та людських помилок	ISO 27001: аудитор відхиляє доказову базу через суперечності;	SOAR автоматично документує кожен крок реагування; GRC-інтеграція формує структурований, пов'язаний пакет доказів	ISO A.5.28, 9.1; ISO 10.1 (вдосконалення)
		Відмова у сертифікації або major nonconformity		
Реактивне управління вразливостями (після інциденту)	Критичні вразливості в АБС/ДБО відомі місяцями;	PCI DSS вимога 11.3: невиконання вимоги щоквартального сканування;	Безперервне сканування VM + автоматична CVSS-пріоритизація через SOAR + контроль строків усунення (MTTR tracking)	ISO A.8.8;
	Банк не має ресурсів для планового сканування і пріоритизації	Втрата PCI-compliant статусу та штраф платіжних систем		PCI DSS 11.3, 11.4

Продовження таблиці 2.4

Фрагментована та неузгоджена доказова база	Аудитор не може відстежити повний ланцюг інциденту;	ISO 27001: відсутність доказів операційного виконання контролів A.5.26, A.8.16;	SIEM корелює події з усіх джерел в єдиному просторі; XDR надає цілісну картину інциденту від початкового вектору до ліквідації	ISO A.8.15, A.8.16;
	Журнали АБС, NGFW та Active Directory не корельовані між собою	Відмова у сертифікації або critical finding		A.5.26, A.5.28
Відсутність вимірюваних KPI та KRI відповідності	Банк не може виміряти, чи знизився ризик після впровадження нових засобів захисту;	ISO 27001, п. 9.1: відсутність вимірювань – підстава для major nonconformity;	Compliance-дашборди SOC відображають KPI у реальному часі; автоматичні щомісячні Management Review звіти для CISO та керівництва	ISO 9.1 (вимірювання), 9.3 (огляд керівництва)
	Відсутні метрики для огляду з боку керівництва	Неможливо продемонструвати ефективність СМІБ		
Слабка інтеграція процесів ІБ та бізнес-процесів банку	Нові банківські продукти (мобільний банкінг, відкритий API) впроваджуються без оцінки ризиків ІБ та без підключення до SIEM	ISO 27001, п. 6.1.2: нові активи не відображені в реєстрі ризиків;	SOC-дані про загрози інтегруються у процес управління ризиками; нові активи автоматично реєструються в CMDB та підключаються до SIEM	ISO 6.1.2; A.8.9 (управління конфігурацією); A.8.32 (управління змінами)
		НБУ: ризики нових продуктів не контролюються		

Системний аналіз виявлених розривів засвідчує, що більшість із них мають спільну першопричину – реактивний та фрагментований підхід до управління відповідністю СМІБ. SOC як операційна платформа вирішує ці розриви не шляхом створення паралельних compliance-процесів, а через інтеграцію вимог відповідності безпосередньо в операційну діяльність команди безпеки. Замість додаткового навантаження на персонал банку, SOC-based підхід перетворює рутинні операційні активності – моніторинг алертів, реагування на інциденти, сканування вразливостей – на автоматично генеровані верифіковані докази відповідності [13].

Висновок до розділу 2

Другий розділ здійснив комплексний аналіз засобів захисту інформаційного середовища банківської установи, зосередившись на Security Operations Center як організаційно-технічному ядрі, що інтегрує всі компоненти системи безпеки. Дослідження трирівневої операційної моделі SOC (L1–L3) підтвердило її безпосередню відповідність вимогам ISO/IEC 27001:2022 щодо розподілу обов'язків, управління інцидентами та безперервного моніторингу. Порівняльний аналіз трьох моделей побудови SOC – In-house, MSSP та гібридної – встановив, що гібридна модель є оптимальною для більшості банків середнього розміру в Україні з огляду на баланс контролю над конфіденційністю даних, відповідності банківській таємниці та операційних витрат.

Аналіз інструментальних засобів SOC виявив, що конкретні технологічні рішення – SIEM (IBM QRadar, Splunk ES, Microsoft Sentinel), EDR/XDR (CrowdStrike Falcon, SentinelOne), SOAR (Palo Alto XSOAR, Splunk SOAR) та платформи Threat Intelligence – виконують не лише захисну функцію, але й є первинними джерелами доказів виконання контролів СМІБ. Ця подвійна роль інструментів SOC є концептуальною основою для розробки методики SOC-based compliance: кожен алерт SIEM, тікет SOAR та звіт VM є потенційним верифікованим доказом відповідності регуляторним вимогам.

Проведений gap-аналіз виявив шість системних розривів, що типово притаманні банківській практиці: відсутність безперервного моніторингу, ручне формування доказів відповідності, реактивне управління вразливостями, фрагментована доказова база, відсутність вимірюваних метрик ефективності та слабка інтеграція процесів ІБ з бізнес-процесами банку. Встановлено, що спільною першопричиною усіх шести розривів є реактивний, фрагментований підхід до управління відповідністю. Для кожного розриву визначено конкретний механізм SOC для усунення, що сформувало вимоги до методики, розробленої у третьому розділі.

Розділ 3. РОЗРОБКА МЕТОДИКИ SOCE(SECURITY OPERATIONS AS COMPLIANCE EVIDENCE) ЗАБЕЗПЕЧЕННЯ ВІДПОВІДНОСТІ СМІБ ТА ІНТЕГРАЦІЯ ІЗ SOC

3.1 Розробка методики SOCE (Security Operations as Compliance Evidence) для забезпечення відповідності СМІБ та її інтеграція у SOC

На підставі аналізу регуляторного середовища, gap-аналізу та порівняльного дослідження підходів до комплаєнсу запропоновано удосконалити методику інтеграції процесів SOC у систему забезпечення відповідності СМІБ банку за допомогою розширення етапу Check циклу PDCA на два етапи. Методика ґрунтується на принципі «Security Operations as Compliance Evidence» (SOCE) – операційна діяльність SOC систематично й автоматично перетворюється на верифіковані докази виконання регуляторних вимог, не створюючи паралельних compliance-процесів та не збільшуючи навантаження на персонал банку [35].

В основі методики лежить цикл PDCA (Plan-Do-Check-Act) стандарту ISO/IEC 27001:2022 та концепція Continuous Compliance, що базується на принципі «compliance as code» – регуляторні вимоги формалізуються у вигляді технічних правил і автоматизованих перевірок (SIEM use cases, SOAR-плейбуки, VM-scheduled scans), що виконуються безперервно в режимі реального часу [14]. Це докорінно відрізняє запропонований підхід від традиційного «аудитного» комплаєнсу, де відповідність підтверджується раз на рік та фактично втрачає актуальність одразу після завершення перевірки. Практичне значення переходу до Continuous Compliance підтверджується дослідженням Ponemon Institute [36], згідно з яким організації з безперервним моніторингом відповідності скорочують вартість кіберінцидентів у середньому на 75 млн грн порівняно з організаціями, що покладаються на реактивний підхід.

Пропонована методика складається з п'яти взаємопов'язаних етапів, що формують замкнений цикл безперервного вдосконалення. Детальний опис усіх етапів наведено у табл. 3.1, а матриця зіставлення контролів СМІБ з процесами SOC – у табл. 3.2 (Додатки).

Перший етап – Картографування (Compliance Control Mapping) – реалізує фазу «Plan» циклу PDCA та є стратегічною основою усієї методики. На цьому етапі формується детальна матриця відповідності між операційними процесами SOC, конкретними інструментами та кожним контролем СМІБ. Для кожного контролю визначається: який процес SOC генерує докази його виконання; який інструмент є джерелом; в якому форматі та з якою частотою докази є необхідними для аудитора. Вихідним результатом є «Реєстр контролів SOC-СМІБ» – структурований документ у GRC-системі або захищеній таблиці, що виступає єдиним джерелом правди про стан відповідності [35].

Практичним нюансом першого етапу є необхідність обов'язкової участі обох сторін – технічної команди SOC та compliance-команди. Технічна команда знає фактичні можливості інструментів (що реально генерує SIEM, якого формату є звіти SOAR), тоді як compliance-команда розуміє інтерпретацію вимог конкретними аудиторами та типові запити при перевірках НБУ або ISO [33]. Без цієї двосторонньої взаємодії Реєстр ризикує залишитися формальним документом, що не відображає реального стану справ.

Другий етап – Автоматизований збір доказів (Evidence Automation) – є технічним ядром методики та реалізує фазу «Do». Для кожного контролю у SIEM налаштовуються scheduled reports та compliance use cases, що автоматично агрегують докази виконання. У SOAR розробляються плейбуки реагування з обов'язковим compliance-кроком, що документує виконаний контроль. Технічна реалізація включає: налаштування автотаймера НБУ-72h та GDPR-72h у SOAR з автоматичним формуванням чернетки звіту до регулятора; налаштування WORM-захисту журналів для виконання PCI DSS 10.3; інтеграцію систем управління вразливостями з SOAR для автоматичного відкриття remediation tasks з дедлайном відповідно до CVSS-оцінки. Для GRC-інтеграції налаштовується API-з'єднання

між SIEM/SOAR та GRC-платформою банку. Якщо банк не має спеціалізованої GRC-системи, мінімально прийнятним рішенням є автоматичний щотижневий експорт compliance-звітів у форматі PDF до захищеного сховища з незмінним журналом доступу, що може бути реалізовано засобами Microsoft Power Automate без значних інвестицій у ліцензування [30].

Третій етап – Безперервний моніторинг відповідності (Continuous Compliance Monitoring) – реалізує фазу «Check» в операційному вимірі. SOC здійснює безперервний моніторинг не лише кіберзагроз, але й стану відповідності СМІБ через спеціалізований compliance-дашборд у реальному часі, що відображає: відсоток активів банку, охоплених SIEM-моніторингом (Log Source Coverage); кількість відкритих вразливостей за рівнями критичності; динаміку MTTD та MTTR порівняно з цільовими SLA; відсоток плейбуків SOAR, виконаних без відхилень; наявність прострочених remediation tasks. Критично важливою функцією є автоматичне виявлення «compliance drift»: якщо новий сервер або банківська система введена в промислову експлуатацію без підключення до SIEM, система автоматично виявляє «нерозпізнаний актив» (unmanaged asset) через порівняння CMDB зі списком активних джерел журналів та генерує тікет у SOAR для усунення [14].

Четвертий етап – Аудиторська взаємодія (Structured Evidence Provision) – реалізує другу частину фази «Check» та формалізує процедуру надання доказів аудиторам. Замість традиційної ручної підготовки документів протягом двох-чотирьох тижнів аудитори отримують структурований доступ до стандартизованих звітів через «Аудиторський портал» – захищений розділ у GRC-системі з RBAC-контролем та журналюванням доступу. Ключовою перевагою підходу є скорочення витрат на підготовку до аудиту з двох-чотирьох тижнів до одного-двох днів. За даними ServiceNow та Ponemon Institute [39], організації з автоматизованим збором доказів скорочують витрати на підготовку до аудиту СМІБ у середньому на 60–70%.

П'ятий етап – Безперервне вдосконалення (Continuous Improvement Loop) – реалізує фазу «Act» та замикає цикл PDCA. Кожне audit finding автоматично перетворюється на remediation task у SOAR з призначеним власником, дедлайном та пріоритетом. Після підтвердження усунення SOAR автоматично генерує «Звіт про закрите finding» з доказами вжитих заходів та оновленим статусом у Реєстрі – прямий доказ виконання вимоги пункту 10.1 ISO/IEC 27001 щодо постійного вдосконалення СМІБ. Зведений опис усіх п'яти етапів методики наведено у табл. 3.1.

Таблиця 3.1

Методика інтеграції SOC у систему забезпечення відповідності СМІБ банку

№	Назва етапу	Ключові дії та нюанси реалізації	Артефакт (вихід)	Відповідальний	PDCA
1	**Картографування (Compliance Control Mapping)**	Зіставлення кожного контролю СМІБ з процесом SOC та інструментом;	Реєстр контролів SOC-СМІБ (GRC або захищена таблиця);	CISO + SOC Lead + Compliance Officer	Plan
		Визначення формату і частоти доказів;	Матриця відповідності (SOC процес → контроль → регулятор);		
		Формування Реєстру;			
		Двостороння взаємодія технічної та compliance-команд. Критерій: ≥ 80% контролів СМІБ покрито відображеннями на SOC-процеси	Затверджений CISO		
2	**Автоматизований збір доказів (Evidence Automation)**	Налаштування SIEM compliance use cases та scheduled reports для кожного контролю;	Compliance use cases у SIEM;	SOC Engineer + SIEM Admin + SOAR Developer	Do
		SOAR-плейбуки з обов'язковим compliance-кроком;			
		API-інтеграція з GRC;	Бібліотека SOAR-плейбуків;		
		WORM-захист журналів;	API-інтеграція з GRC;		
		Автотаймер НБУ-72h та GDPR-72h у SOAR;	WORM-конфігурація сховища;		
		Auto-draft звітів до регуляторів	Документація налаштувань		

Продовження таблиці 3.1

3	**Безперервний моніторинг відповідності (Continuous Compliance Dashboard)**	24/7 моніторинг compliance-метрик (Log Source Coverage, MTTD, MTTR, FPR, MTTR вразливостей); автоматичне виявлення compliance drift (нові активи без SIEM; прострочені remediation tasks; перевищення SLA); щотижневий PDF-звіт; щомісячний Management Review звіт	Compliance-дашборд (real-time); Автоматичні drift-сповіщення; Щотижневий звіт; Management Review report з KPI-динамікою	SOC Analyst L2 + Compliance Analyst	Check (1)
4	**Аудиторська взаємодія (Structured Evidence Provision)**	Аудиторський портал (захищений розділ GRC або веб-застосунок): доступ аудитора (ISO, PCI QSA, НБУ) до SIEM-звітів, SOAR-тікетів, VM-звітів, Management Review протоколів – за обраний аудитором період. Підготовка пакету доказів: ≤ 2 дні. Журналювання доступу аудитора (RBAC)	Аудиторський портал; структурований Evidence Package (SIEM звіти + SOAR тікети + VM звіти + Management Review протоколи)	Compliance Officer + SOC Lead	Check (2)
5	**Безперервне вдосконалення (Continuous Improvement Loop)**	Автоматичне відкриття remediation task у SOAR для кожного audit finding; призначення власника, дедлайну, пріоритету; ескалація при простроченні; auto-генерація «Звіту про закрите finding» як доказ ISO 10.1; аналіз патернів для вдосконалення SIEM-правил та плейбуків	Remediation tasks у SOAR; звіти про закриті findings; оновлені плейбуки та SIEM-правила; актуалізований Реєстр контролів	CISO + SOC Lead + Compliance Officer	Act

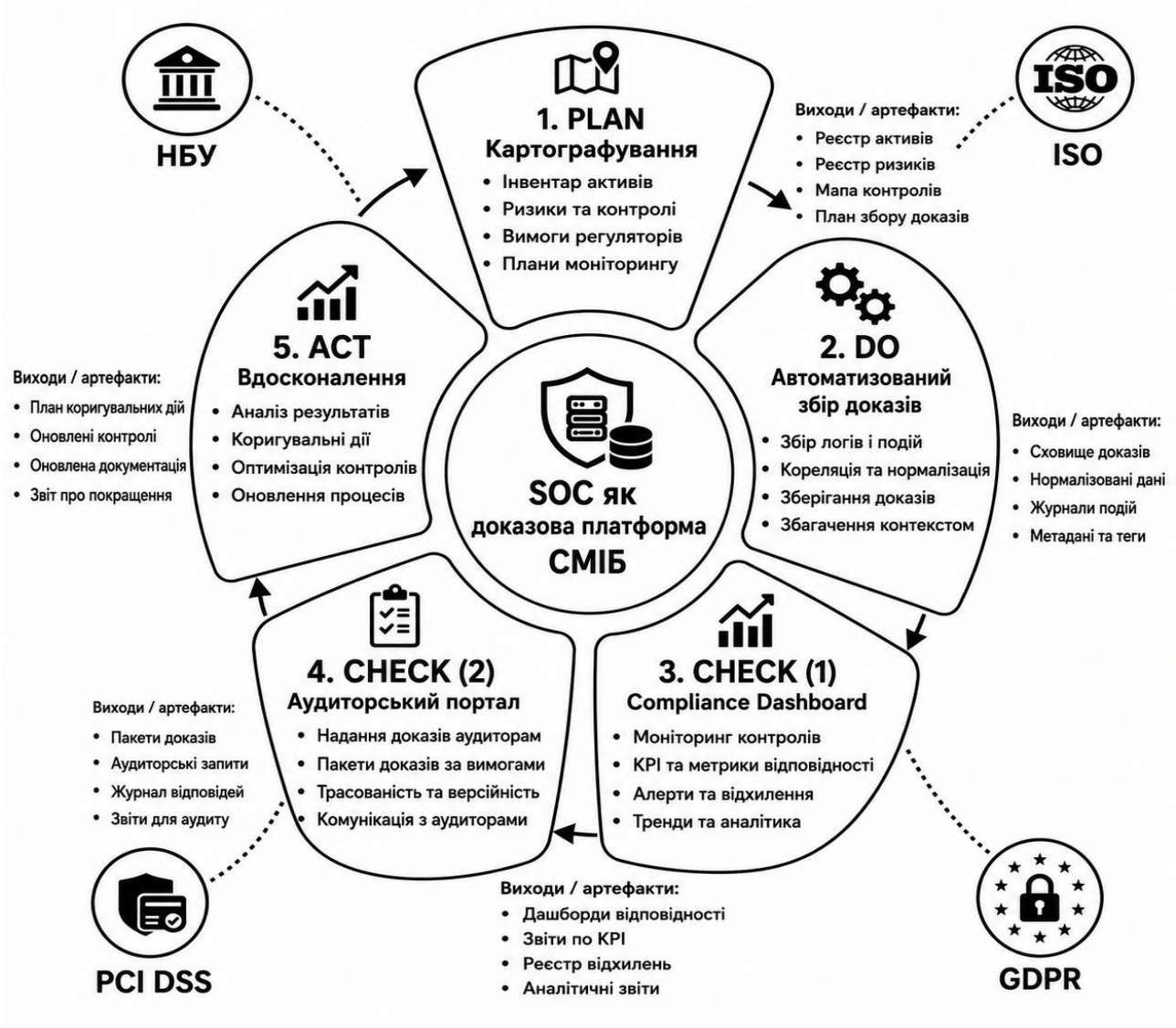

Рис. 3.1. Методика інтеграції SOC у систему забезпечення відповідності СМІБ банку (PDCA-цикл)

Практична цінність методики полягає у її масштабованості. Для великих системоутворюючих банків з In-house SOC методика реалізується повністю через власну GRC-платформу та зрілу команду. Для банків середнього розміру з гібридним SOC пріоритетними є Етапи 1–2 (картографування та автоматизація доказів). Для менших банків з MSSP-моделлю методика адаптується у спрощеному варіанті: Реєстр контролів ведеться у форматі захищеної таблиці, а звіти MSSP інтегруються у документаційну базу через структурований шаблон. Рекомендований горизонт повного впровадження – від 12 до 24 місяців залежно від вихідної зрілості SOC та СМІБ [35].

Для обґрунтування наукової новизни запропонованої методики SOCE необхідно систематично порівняти її з найбільш поширеними підходами до забезпечення відповідності СМІБ: методологією SANS Institute та рекомендаціями Gartner у сфері SOC-based compliance.

Методологія SANS Institute (зокрема, курси SEC511 та SEC555) пропонує підхід до побудови SOC з акцентом на технічних компетенціях аналітиків, налаштуванні правил кореляції SIEM та розробці use cases для виявлення загроз [22]. Ключовою відмінністю підходу SANS є орієнтація насамперед на ефективність виявлення загроз (threat detection effectiveness), тоді як питання формування доказової бази відповідності СМІБ розглядається як вторинне. SANS пропонує окремі use cases для compliance-аудиту, однак не формує цілісного циклу інтеграції операційних процесів SOC у систему підтвердження відповідності. Фактично, compliance у методології SANS є побічним продуктом операційної діяльності SOC, а не системно організованим процесом.

Рекомендації Gartner у сфері Security Operations (зокрема, документи «Market Guide for Security Operations Center» та «Hype Cycle for Security Operations») акцентують на автоматизації SOC, впровадженні SOAR-платформ та розвитку аналітичних можливостей [22]. Gartner рекомендує розглядати compliance як один з use cases SOC, проте не пропонує структурованої методики зіставлення конкретних контролів СМІБ з операційними процесами SOC. Підхід Gartner є описовим (descriptive) та орієнтований на визначення ринкових тенденцій, тоді як SOCE є prescriptive – тобто надає покроковий алгоритм впровадження.

Методика SOCE відрізняється від зазначених підходів за трьома ключовими ознаками. По-перше, SOCE формалізує двосторонній зв'язок між контролями СМІБ та операційними процесами SOC через структурований «Реєстр контролів SOC-СМІБ», якого немає ні в SANS, ні в рекомендаціях Gartner. По-друге, SOCE враховує специфіку регуляторного середовища банківського сектору України (Постанова НБУ №95, PCI DSS v4.0, GDPR), тоді як SANS та Gartner пропонують універсальні підходи без прив'язки до конкретних юрисдикцій. По-третє,

SOCE включає явний механізм автоматизації доказів відповідності через SOAR-плейбуки з compliance-кроком, що перетворює кожну операцію реагування на задокументований доказ виконання контролю СМІБ – цього елементу немає у жодній з розглянутих методологій.

Таким чином, методика SOCE не є альтернативою підходам SANS або Gartner, а є їх розвитком і конкретизацією стосовно задачі забезпечення відповідності СМІБ у банківському секторі. SOCE систематизує найкращі практики галузі у вигляді покрокової методики, адаптованої до регуляторних вимог НБУ, ISO/IEC 27001:2022 та PCI DSS v4.0.

3.2 Рекомендації щодо інтеграції із SOC методики SOCE(Security Operations as Compliance Evidence) в банківських установах та оцінка доцільності впровадження

На основі розробленої методики, аналізу регуляторного середовища та дослідження кращих практик галузі сформульовано структуровані практичні рекомендації для банків щодо побудови SOC-based Continuous Compliance. Рекомендації організовані за трьома рівнями управління – стратегічним, тактичним та операційним – і враховують специфіку банківського сектору України [35].

На стратегічному рівні першочерговим завданням є формальне закріплення у внутрішній нормативній базі банку ролі SOC як платформи збору доказів відповідності СМІБ. Рекомендується внести зміни до «Положення про інформаційну безпеку» та «Положення про SOC», де SOC визначається як «Технологічна платформа безперервного моніторингу та збору доказів відповідності СМІБ банку». У посадових інструкціях аналітиків L2/L3 рекомендується явно зазначити обов'язок документування дій із прив'язкою до конкретних контролів СМІБ. Рекомендується виділити окрему роль «Compliance Analyst» у структурі SOC (або призначити відповідального аналітика L2, що суміщає функції моніторингу та підтримки compliance-активностей), що забезпечить інституційну відповідальність за актуальність Реєстру контролів.

Стратегічно важливим є впровадження концепції «Security by Design» при розробці нових банківських продуктів та послуг. Відповідно до контролю A.8.25 ISO/IEC 27001:2022 («Безпечний життєвий цикл розробки»), кожен новий проєкт – запуск нового каналу ДБО, відкриття Open Banking API, перехід на хмарну платформу – повинен проходити обов'язкову оцінку ризиків ІБ за участю SOC до виходу в продуктивне середовище. Новий актив має автоматично реєструватися у CMDB та підключатися до SIEM-моніторингу одночасно з початком промислової експлуатації. Цей підхід реалізує принцип «privacy by design» статті 25 GDPR та вимоги PCI DSS 12.3.4 щодо оцінки нових технологій [17].

Стратегічним орієнтиром для визначення цільового рівня зрілості SOC є модель CISA Zero Trust Maturity Model v2.0 [35], яка визначає п'ять рівнів зрілості для кожного стовпа Zero Trust (Identity, Devices, Networks, Applications & Workloads, Data). Для банківського сектору рекомендується досягати рівня «Advanced» за стовпами Identity та Devices (моніторинг привілейованого доступу та стану кінцевих точок) протягом першого року впровадження SOC-based compliance, та рівня «Optimal» за стовпом Data (класифікація та захист усіх категорій банківських даних) – протягом другого-третього року.

На тактичному рівні ключовим завданням є формування «Бібліотеки плейбуків SOC» – набору стандартизованих плейбуків SOAR для типових інцидентів банківського сектору. Кожен плейбук повинен містити явне посилання на контролі СМІБ та регуляторні вимоги, виконання яких він забезпечує, що перетворює кожне реагування на інцидент на автоматично задокументований доказ відповідності. Детальний опис рекомендованої бібліотеки плейбуків із прив'язкою до MITRE ATT&CK тактик та регуляторних вимог наведено у табл. 3.2 [38].

Таблиця 3.2

Рекомендована бібліотека плейбуків SOC для банківського сектору (SOAR Playbook Library)

Тип інциденту (банківська специфіка)	**Автоматичні кроки плейбука SOAR**	**Контролі СМІБ (ISO 27001:2022)**	**Регуляторна вимога**	**SLA реагування**
BEC – компрометація корпоративної пошти	1. Блокування облікового запису в AD; 2. Відкликання OAuth-токенів; 3. Збір email headers; 4. Перевірка вихідних переказів за 48 год.; 5. Оцінка витоку ПД → автотаймер GDPR-72h; 6. Сповіщення керівника ІБ та фінансового директора; 7. Збір forensic-артефактів поштового сервера	A.5.26, A.5.28; A.8.15 (журнали пошти); A.5.18 (доступ); A.8.7 (шкідливе ПЗ)	GDPR ст. 33 (витік ПД);	P1: MTTI < 30 хв.;
			НБУ №95 (фінансові операції);	MTTR < 4 год.;
			PCI DSS 12.10	GDPR-звіт < 72 год.
Атака на ДБО / мобільний банкінг	1. Тимчасове блокування підозрілої клієнтської сесії; 2. Збір транзакційних логів API; 3. Fingerprint пристрою (IP, User-Agent, геолокація, device ID); 4. Сповіщення фрод-відділу; 5. Моніторинг суміжних рахунків; 6. Блокування підозрілих IP у WAF; 7. Звіт до НБУ при підтвердженні компрометації	A.5.26; A.8.16 (моніторинг транзакцій); A.5.14 (передача інформації); A.5.28	НБУ №95 (компрометація платіжної інфраструктури);	P1: MTTI < 15 хв.;
			PCI DSS 12.10;	MTTR < 2 год.;
			Закон «Про платіжні послуги»	НБУ-звіт < 72 год.
Ransomware / програма-здирник	1. Негайна мережева ізоляція скомпрометованих хостів (EDR auto-containment); 2. Зупинка підозрілих процесів; 3. Memory dump для криміналістики; 4. Ідентифікація initial access vector; 5. Сповіщення BCP-команди; 6. Перевірка цілісності резервних копій; 7. Ретроспективний пошук у SIEM за IoC; 8. Звіт до НБУ (переривання > 4 год.)	A.5.26, A.5.28; A.8.13 (резервні копії); A.5.29 (безперервність ІБ); A.8.7	НБУ №95 (переривання сервісів > 4 год.);	P1: MTTI < 15 хв.;
			PCI DSS 12.10;	ізоляція < 30 хв.;
			Закон №2163-VIII (об'єкти КІ)	НБУ-звіт < 72 год.

Продовження таблиці 3.2

Компрометація привілейованого облікового запису	1. Примусове скидання пароля (PAM-інтеграція); 2. Відкликання всіх активних сесій; 3. Аудит дій за останні 7 днів (AD audit log); 4. Перевірка змін у критичних системах (АБС, NGFW, AD); 5. Ескалація до L3; 6. Сповіщення CISO; 7. Ініціювання Threat Hunting за аналогічними IoC	A.5.18 (права доступу); A.8.16 (моніторинг); A.5.26; A.8.2 (привілейований доступ)	НБУ №95 Розд. IV (контроль привілейованого доступу);	P1: MTTI < 30 хв.;
				скидання пароля < 1 год.;
			PCI DSS 8.6 (MFA для адміністраторів)	розслідування < 4 год.
Виявлення шкідливого ПЗ / APT-індикатор	1. Ізоляція хосту (EDR containment); 2. IoC-збагачення через TI-платформу (Recorded Future/MISP); 3. Retrohunt по SIEM за IoC за 30 днів; 4. Memory dump + file quarantine; 5. Перевірка суміжних хостів на той самий IoC; 6. Оновлення NGFW/EDR-блокувальних правил; 7. Документування TTP за MITRE ATT&CK	A.8.7 (захист від шкідливого ПЗ); A.5.7 (TI); A.5.26; A.5.28	НБУ №95;	P1: MTTI < 30 хв.;
			PCI DSS 5.3 (антивірусний контроль);	ізоляція < 1 год.;
			кращі практики CERT-UA	retrohunt < 4 год.
Витік персональних даних (Data Breach)	1. DLP-алерт: ідентифікація типу та обсягу витоку ПД; 2. Блокування каналу витоку (email/USB/cloud upload); 3. Forensic-збір доказів із SHA-256 хешом; 4. Юридична оцінка: чи підпадає під ст. 33 GDPR; 5. Автотаймер GDPR-72h → auto-draft звіту для ДПА; 6. Оцінка необхідності повідомлення суб'єктів (ст. 34)	A.5.12 (класифікація); A.8.12 (запобігання витоку); A.5.26, A.5.28	GDPR ст. 33, 34;	P1: MTTI < 1 год.;
			Закон України «Про захист ПД»;	GDPR-оцінка < 4 год.;
			НБУ №95 (витік клієнтських даних)	звіт ДПА < 72 год.

На тактичному рівні рекомендується також впровадити процедуру «Щоквартального огляду Реєстру контролів SOC-СМІБ». Реєстр потребує обов’язкового перегляду при кожній зміні інфраструктури, після кожного значного інциденту (для актуалізації покриття та виявлення прогалин) та при виході нових версій регуляторних документів. Відповідальним за актуальність Реєстру є Compliance Analyst при технічній підтримці керівника SOC та з формальним затвердженням CISO.

Окремою тактичною рекомендацією є впровадження регулярних спільних навчань (table-top exercises) команди SOC та compliance-підрозділу з відпрацювання сценаріїв реагування на типові для банківського сектору інциденти. Згідно з дослідженням Ponemon Institute [36], організації, що проводять регулярні кіберучення, скорочують середній час реагування на реальні інциденти на 30–45% порівняно з організаціями без такої практики. Сценарії навчань повинні включати не лише технічні аспекти реагування, але й відпрацювання процедур звітування до НБУ та ДПА в умовах стресу та часових обмежень – оскільки саме дотримання строків звітування є одним із найбільш ризикових аспектів регуляторної відповідності банків. Документація проведених навчань є доказом виконання контролів A.6.3 (навчання та підготовка) та A.5.26 (готовність до реагування) ISO/IEC 27001:2022.

На операційному рівні ключовим інструментом управління є система KPI відповідності СМІБ, що забезпечує вимірювані метрики для оцінки ефективності функціонування SOC у контексті регуляторних вимог. Система KPI, наведена у табл. 3.5, розроблена на основі вимог ISO/IEC 27001:2022 (п. 9.1), Постанови НБУ №95, PCI DSS v4.0, NIST SP 800-61 Rev.3 [37] та EDPB Guidelines 9/2022 [40].

Таблиця 3.3

Система KPI для SOC-based відповідності СМІБ банку

KPI / SLA показник	**P1 Критичний**	**P2 Високий**	**Тренд**	**Регуляторне обґрунтування**	**Джерело вимірювання в SOC**
MTTD – середній час виявлення загрози	< 1 год.	< 4 год.	↓	НБУ №95 (оперативне виявлення) PCI DSS 10.6 (щоденний аналіз журналів) NIST SP 800-61 Rev.3	SIEM: дельта між часом першої аномальної події та генерацією підтвердженого алерту
MTTI – час до початку розслідування	< 30 хв.	< 2 год.	↓	ISO A.5.26 (оцінка та реагування) NIST SP 800-61 Rev.3 (рекомендований час тріажу)	SOAR: час між відкриттям тікету та першою дією L2-аналітика
MTTR – час стримування загрози (Containment)	< 4 год.	< 24 год.	↓	НБУ №95 (переривання сервісів < 4 год.) ISO A.5.26; NIST SP 800-61 Rev.3	SOAR: час завершення кроку «Containment» у плейбуку

Продовження таблиці 3.3

Дотримання 72-год. строку звітування (НБУ / ДПА)	100%	–	→ 100%	НБУ №95 п. 6.9 (72 год. з моменту виявлення) GDPR ст. 33 (72 год. після підтвердження) EDPB Guidelines 9/2022	SOAR: автотаймер + відсоток вчасно надісланих звітів / загальна кількість суттєвих інцидентів
Покриття активів SIEM-моніторингом (Log Source Coverage)	> 98%	–	↑ до 100%	ISO A.8.15, A.8.16 PCI DSS 10.2 (журналювання всіх компонентів у CDE)	SIEM: щоденний звіт (активні log sources / загальна кількість активів у CMDB)
MTTR вразливостей – критичних / важливих	≤ 14 днів	≤ 30 днів	↓	PCI DSS 11.3 (між скануваннями); ISO A.8.8; NIST CSF 2.0 (Respond function)	VM Scanner → SOAR remediation task: дата виявлення → дата підтвердженого закриття
False Positive Rate (FPR) алертів SIEM	< 15%	< 25%	↓	Операційна ефективність SOC ISO 9.1 (вимірювання ефективності засобів захисту) Ponemon 2024	SIEM: відношення алертів, закритих як FP, до загальної кількості алертів за місяць
Частка автоматизованих доказів відповідності СМІБ	> 80%	–	↑	ISO 9.1 (вимірювання) мета методики SOCE – automation of compliance evidence	GRC: відсоток контролів, для яких докази генеруються автоматично без ручного втручання
Retention журналів аудиту (повнота зберігання)	≥ 36 міс.	–	→	НБУ №95 (KI-записи ≥ 3 роки); PCI DSS 10.7 (≥ 12 міс., оперативний доступ до 3 міс.)	SIEM: щомісячна перевірка retention policy; звіт про обсяг збережених журналів
Закриття audit findings у встановлений строк	> 90%	–	↑ до 100%	ISO 10.1 (постійне вдосконалення); Внутрішні SLA за результатами аудиту	SOAR: відсоток remediation tasks, закритих до дедлайну / загальна кількість findings
Охоплення Threat Hunting (тактики MITRE ATT&CK)	> 60% тактик	–	↑	ISO A.5.7 (Threat Intelligence) кращі практики MITRE ATT&CK для Financial Services	L3 Threat Hunting звіт: покриті тактики / загальна кількість актуальних ATT&CK-тактик для FS

Практичне впровадження системи KPI потребує налаштування автоматизованого збору метрик з операційних систем SOC без ручного втручання. SIEM на-

дає метрики MTTD, Log Source Coverage та FPR; SOAR – MTTI, MTTR, своєчасність звітування та закриття audit findings; система VM – MTTR вразливостей та охоплення сканування; GRC-платформа – частку автоматизованих доказів. Усі метрики автоматично включаються до щомісячного Management Review звіту для CISO та керівництва банку, що безпосередньо виконує вимогу пункту 9.3 ISO/IEC 27001:2022 щодо огляду з боку керівництва.

Додатковою операційною рекомендацією є впровадження щомісячних «Compliance Review» зустрічей за участю керівника SOC, CISO та Compliance Officer. Порядок денний таких зустрічей має включати: огляд compliance-дашборду та динаміки KPI; аналіз нових або змінених регуляторних вимог; перегляд відкритих audit findings та статусу їх усунення; оцінку нових ризиків, виявлених SOC протягом місяця; планування Threat Hunting активностей на наступний місяць [12]. Протоколи цих зустрічей є прямим доказом виконання вимоги пункту 9.3 ISO/IEC 27001:2022, оскільки демонструють системний огляд стану СМІБ уповноваженим керівництвом.

Реалізація запропонованих рекомендацій потребує поетапного підходу. На першому етапі (0–6 місяців) рекомендується сфокусуватися на Етапах 1–2 методики: формуванні Реєстру контролів, налаштуванні базових compliance use cases у SIEM та впровадженні автотаймера НБУ/GDPR у SOAR. На другому етапі (6–12 місяців) – розгортання compliance-дашборду та формування бібліотеки плейбуків. На третьому етапі (12–24 місяці) – повний перехід до Continuous Compliance з автоматизованим Аудиторським порталом та впровадженням системи KPI. Такий горизонт планування узгоджується з дворічним циклом між первинною сертифікацією та першим наглядовим аудитом ISO/IEC 27001, що дозволяє банку досягти повної зрілості SOC-based compliance до моменту першої ресертифікації [33].

Практичне застосування рекомендацій суттєво варіюється залежно від категорії банку. В українському банківському секторі доцільно виокремити три профілі: малі банки (активи до 50 млрд грн, чисельність IT-персоналу 10–30 осіб), банки середнього розміру (активи 100–300 млрд грн, IT-підрозділ 30–150

осіб) та великі системоутворюючі банки (активи понад 400 млрд грн). Різниця у доступному бюджеті на кібербезпеку (КБ) між цими категоріями є принциповою і визначає склад технологічного стека SOC, модель його побудови та горизонт досягнення цільового рівня відповідності. У табл 3.4 систематизовано ключові параметри впровадження для кожної категорії.

Для малих банків ключовим обмеженням є не лише бюджет, але й дефіцит кваліфікованого ІБ-персоналу. В умовах, коли функції інформаційної безпеки суміщає один-два штатних спеціалісти, застосування повного стека методики SOCE є недоцільним. Натомість першочерговими заходами є: укладення договору з MSSP-провайдером, що має досвід роботи з банківським сектором і пропонує SLA з гарантованим 72-годинним циклом звітування до НБУ; впровадження Microsoft Sentinel як найбільш доступного хмарного SIEM з моделлю оплати за об'єм даних; автоматизація базового реєстру контролів SOC-СМІБ у форматі захищеної таблиці з автоматичним PDF-звітом через Microsoft Power Automate. Загальні витрати на мінімально необхідний стек для малого банку не перевищують 8–15 млн грн на рік, що цілком вкладається у бюджетний діапазон 4–22,5 млн грн, зберігаючи резерв для операційних та кадрових витрат.

Для банків середнього розміру гібридна модель SOC є оптимальною як з точки зору регуляторної відповідності, так і з позиції витрат. Власна L2/L3-команда (3–8 аналітиків) забезпечує контроль над критичними розслідуваннями та зберігання всіх даних в інфраструктурі банку, що є вимогою банківської таємниці (ст. 60 ЗУ «Про банки»). При цьому делегування L1-моніторингу MSSP суттєво знижує операційне навантаження на власну команду. Методика SOCE для цієї категорії банків рекомендується до повного впровадження за 18–24 місяці, з пріоритизацією Етапів 1–3 у першій половині проєкту. Особливу увагу слід приділити API-інтеграції між SIEM, SOAR та GRC-платформою, оскільки саме автоматизація формування доказів (Етап 2) дає найбільший регуляторний ефект при помірних інвестиціях – скорочення витрат на підготовку до аудиту оцінюється у 60–70% [39].

Великі системоутворюючі банки, що перебувають під посиленим наглядом НБУ та зобов'язані проходити регулярні інспекційні перевірки, мають умови для повноцінного впровадження методики SOCE в усіх п’яти етапах. Власний In-house SOC з командою 15–40+ аналітиків, enterprise-рівень SIEM та SOAR, а також спеціалізована GRC-платформа формують зрілу операційну основу для Continuous Compliance. Ключовою рекомендацією для цієї категорії є запровадження окремої ролі «Head of SOC Compliance» – старшого аналітика (рівень L3), що несе персональну відповідальність за актуальність Реєстру контролів SOC-СМІБ, координацію з compliance-підрозділом та підготовку щоквартальних звітів для Наглядової ради банку. Досягнення рівня зрілості CMMI-4 за системою KPI (табл. 3.3) є реалістичним горизонтом для великого банку протягом 12–18 місяців від початку проєкту за умови виділення бюджету не менше 130млн–4,5 млрд грн на рік на функцію КБ.

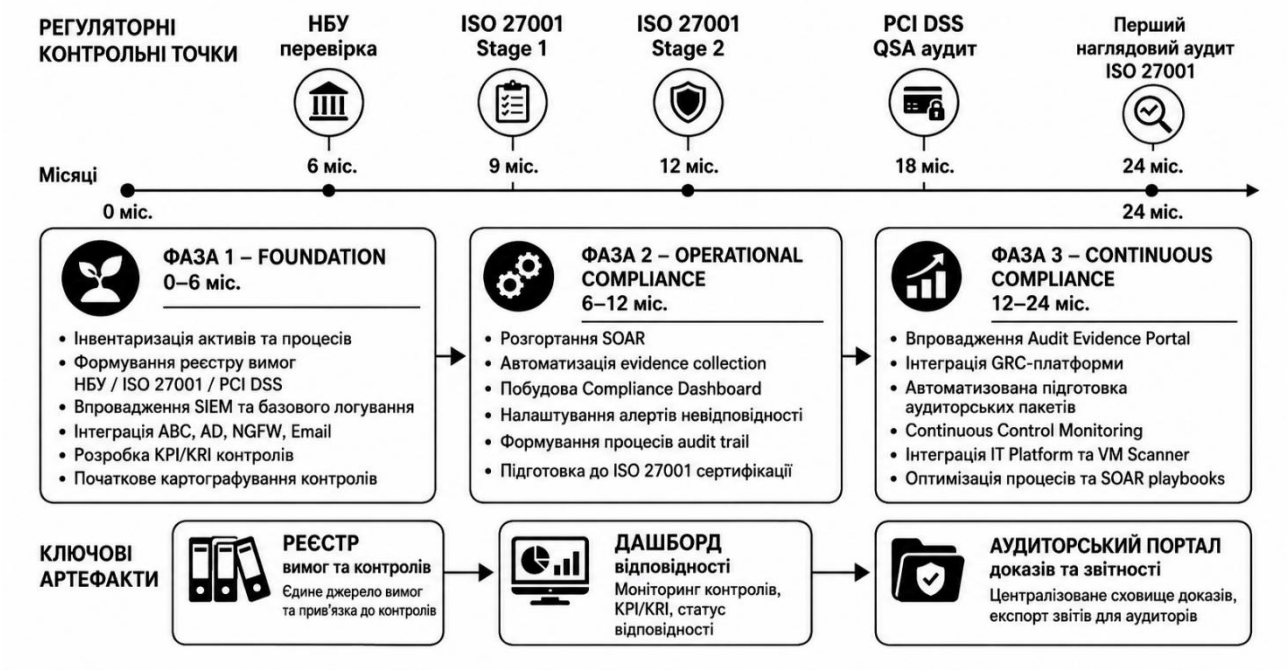

Рис. 3.4. Дорожня карта впровадження SOC-based Continuous Compliance у банку

Висновок до розділу 3

Третій розділ реалізував практичну мету дослідження – розробку та обґрунтування методики SOCE (Security Operations as Compliance Evidence), що забезпечує інтеграцію процесів SOC у систему підтвердження відповідності СМІБ на принципі «compliance as code». Методика охоплює: (1) картографування контролів СМІБ на процеси SOC через «Реєстр контролів SOC-СМІБ»; (2) автоматизований збір доказів через SIEM compliance use cases та SOAR-плейбуки з compliance-кроком; (3) безперервний моніторинг відповідності через compliance-дашборд із функцією виявлення «compliance drift»; (4) структуровану аудиторську взаємодію через спеціалізований аудиторський портал; (5) цикл безперервного вдосконалення на основі автоматичних remediation tasks для кожного audit finding. Порівняльний аналіз з методологіями SANS Institute та рекомендаціями Gartner підтвердив наукову новизну SOCE: жодна з розглянутих методологій не формалізує двосторонній зв'язок між контролями СМІБ і процесами SOC та не забезпечує автоматичної генерації compliance-доказів через SOAR-плейбуки.

Сформульовані практичні рекомендації структуровано на трьох рівнях – стратегічному, тактичному та операційному – з урахуванням трьох профілів банків за обсягом активів. Ключовим операційним інструментом є система KPI відповідності СМІБ, що включає 11 вимірюваних показників, кожен із яких прив'язаний до конкретних регуляторних вимог та автоматично вимірюється засобами SOC. Особливу практичну цінність становить диференційований підхід до впровадження: для малих банків методика адаптується до мінімального стека вартістю від 8,9 до 15,5 млн грн на рік, тоді як великі системоутворюючі банки реалізують SOCE у повному обсязі з GRC-автоматизацією протягом 12–18 місяців.

Теоретична модель прогнозованих результатів впровадження, розроблена на основі галузевих даних Ponemon Institute та IBM X-Force, підтверджує вагому економічну обґрунтованість методики: скорочення MTTD на 95–99%, частка автоматизованих доказів відповідності понад 80% та економія витрат на підготовку до аудиту у розмірі 60–70%. Це підтверджує, що SOC-based підхід до управління

відповідністю СМІБ є не лише технічно реалізованим, але й фінансово ефективним для банківського сектору України.

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи досягнуто поставленої мети — розроблено методичний підхід до забезпечення відповідності системи менеджменту інформаційної безпеки регуляторним вимогам шляхом інтеграції процесів та інструментів Security Operations Center як засобу безперервного моніторингу та формування доказової бази відповідності. Сформульовано такі основні висновки.

1. Дослідження регуляторного середовища підтвердило, що банківський сектор функціонує в умовах одночасної дії кількох нормативних вимог: Постанови НБУ №95, ISO/IEC 27001:2022, PCI DSS v4.0 та GDPR. Ключовими операційно значущими вимогами, що потребують підтримки SOC, є: безперервний моніторинг подій безпеки (A.8.16 ISO/IEC 27001), 72-годинне звітування про кіберінциденти (НБУ №95, Розд. VI; GDPR ст. 33), щоквартальне сканування вразливостей (PCI DSS вимога 11.3) та управління журналами аудиту з ретенцією не менш ніж 12 місяців (PCI DSS вимога 10.7) і не менш ніж 36 місяців (НБУ №95). Встановлено, що жодна з цих вимог не може бути системно виконана без функціонуючого SOC.

2. Аналіз архітектури SOC показав, що трирівнева операційна структура (L1–L3) безпосередньо кореспондує з вимогами СМІБ щодо розподілу обов'язків (п. 5.3 ISO/IEC 27001), управління інцидентами (A.5.26), збору доказів (A.5.28) та безперервного моніторингу (A.8.16). Порівняльний аналіз трьох моделей побудови SOC (In-house, MSSP, гібридна) встановив, що гібридна модель є оптимальною для більшості банків середнього розміру з огляду на баланс контролю над конфіденційністю даних, відповідності банківській таємниці (ст. 60 ЗУ «Про банки і банківську діяльність») та операційних витрат. Аналіз інструментального стека SOC (SIEM, EDR/XDR, SOAR, TI, VM) підтвердив їх подвійну роль: кожен інструмент виступає одночасно засобом захисту та первинним джерелом доказів виконання контролів СМІБ.

3. Gap-аналіз виявив шість системних розривів у практиці забезпечення відповідності СМІБ: відсутність безперервного моніторингу; ручне та фрагментоване формування доказів відповідності; реактивне управління вразливостями; фрагментована та неузгоджена доказова база; відсутність вимірюваних метрик ефективності; слабка інтеграція процесів ІБ та бізнес-процесів банку. Встановлено, що спільною першопричиною усіх розривів є реактивний підхід до управління відповідністю. Для кожного розриву визначено конкретний механізм SOC для усунення через інтеграцію SIEM, SOAR, VM та compliance-дашбордів.

4. Порівняльний аналіз трьох підходів до забезпечення відповідності (реактивного, проактивного та безперервного) підтвердив принципову перевагу SOC-based підходу: час виявлення невідповідності скорочується з місяців до хвилин, рівень зрілості СМІБ підвищується від CMMI-1 до CMMI-4–5. Аналіз архітектурних концепцій Zero Trust та Defense in Depth підтвердив їх синергію з операційними функціями SOC.

5. Розроблено авторську методику SOCE (Security Operations as Compliance Evidence), що забезпечує інтеграцію процесів SOC у систему підтвердження відповідності СМІБ на основі принципу «compliance as code». Методика включає: (1) картографування контролів СМІБ на процеси SOC через «Реєстр контролів SOC-СМІБ»; (2) автоматизований збір доказів через SIEM compliance use cases та SOAR-плейбуки з compliance-кроком; (3) безперервний моніторинг відповідності з функцією автоматичного виявлення «compliance drift»; (4) структуровану аудиторську взаємодію через захищений аудиторський портал, що скорочує підготовку до аудиту з 2–4 тижнів до 1–2 днів; (5) цикл безперервного вдосконалення на основі автоматичних remediation tasks для кожного audit finding. Порівняльний аналіз з методологіями SANS Institute та рекомендаціями Gartner підтвердив наукову новизну SOCE: жодна з розглянутих методологій не формалізує двосторонній зв'язок між контролями СМІБ та процесами SOC і не реалізує автоматизацію доказів через SOAR-плейбуки з compliance-кроком, адаптовані до регуляторного середовища банківського сектору України.

Теоретична модель прогнозованих результатів впровадження, розроблена на основі галузевих даних Ponemon Institute та IBM X-Force, підтверджує скорочення MTTD на 95–99%, частку автоматизованих доказів понад 80% та економію витрат на підготовку до аудиту у розмірі 60–70%. Рекомендований горизонт повного впровадження — 12–24 місяці, з диференційованим підходом для малих (бюджет КБ 4,5–22,5 млн грн/рік), середніх (20–90 млн грн/рік) та великих (100–1000+ млн грн/рік) банків.

Результати дослідження підтверджують, що інтеграція процесів SOC у систему забезпечення відповідності СМІБ є не лише технічно реалізованою, але й економічно обґрунтованою стратегією. Використання SOC як платформи доказової бази відповідності перетворює рутинні операційні активності — моніторинг алертів, реагування на інциденти, сканування вразливостей — на автоматично генеровані верифіковані докази для аудиторів. Запропоновані підходи можуть бути застосовані підприємствами банківського сектору для підвищення рівня відповідності, автоматизації комплаєнсу та удосконалення процесів внутрішнього аудиту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Laudon K. C., Laudon J. P. Management Information Systems: Managing the Digital Firm. 15th ed. Pearson, 2020. 669 p.
2. Turban E., Pollard C., Wood G. Information Technology for Management. 12th ed.
3. Stair R., Reynolds G. Principles of Information Systems. 13th ed. Cengage Learning, 2019. 704 p.
4. ENISA Threat Landscape 2023. European Union Agency for Cybersecurity. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
5. Stallings W. Effective Cybersecurity: A Guide to Using Best Practices and Standards. Addison-Wesley Professional, 2018. 336 p.
6. O'Brien J., Marakas G. Management Information Systems. 11th ed. McGraw-Hill Education, 2019. 592 p.
7. OWASP Foundation. OWASP Top 10: The Ten Most Critical Web Application Security Risks. 2021. URL: https://owasp.org/www-project-top-ten/
8. NIST Special Publication 800-145. The NIST Definition of Cloud Computing. National Institute of Standards and Technology, 2011.
9. Cisco. 2023 Global Networking Trends Report. URL: https://www.cisco.com/c/dam/global/en_ca/solutions/enterprise-networks/xa-09-2023-networking-report.pdf
10. Hadnagy C. Social Engineering: The Science of Human Hacking. 2nd ed. Wiley, 2018. 304 p.
11. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls. International Organization for Standardization, 2022.
12. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements. International Organization for Standardization, 2022.
13. IBM. What is a Security Operations Center (SOC)? URL: https://www.ibm.com/think/topics/security-operations-center

14. Постанова Правління Національного банку України №95 від 28.09.2017 «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки та кіберзахисту в банківській системі України».
15. IBM X-Force Threat Intelligence Index 2025. IBM Security. URL: https://www.ibm.com/reports/threat-intelligence
16. VMware. What is Virtual Infrastructure? URL: https://www.vmware.com/topics/virtual-infrastructure
17. Palo Alto Networks. What is Cybersecurity? URL: https://www.paloaltonetworks.com/cyberpedia/cyber-security
18. NIST Special Publication 800-207. Zero Trust Architecture. National Institute of Standards and Technology, 2020.
19. Microsoft Security. Defense in Depth Strategy. URL: https://learn.microsoft.com/en-us/security/compass/defense-in-depth
20. NIST Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology, 2024.
21. CISA. Cybersecurity Best Practices. URL: https://www.cisa.gov/topics/cybersecurity-best-practices
22. Gartner. Security Operations Center Modernization Trends. 2023.
23. Splunk. What is SIEM (Security Information and Event Management)? 2023. URL: https://www.splunk.com/en_us/blog/learn/siem-security-information-event-management.html
24. PCI Security Standards Council. PCI DSS v4.0. 2022. URL: https://www.pcisecuritystandards.org/
25. CrowdStrike. What is Endpoint Detection and Response (EDR)? 2023. URL: https://www.crowdstrike.com/en-us/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/
26. Palo Alto Networks. What is XDR? Extended Detection and Response. 2023. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-extended-detection-response-XDR

27. Gartner. Market Guide for Security Orchestration, Automation and Response Solutions. 2023.
28. Mandiant. Threat Intelligence Explained. 2023. URL: https://cloud.google.com/security/products/mandiant-threat-intelligence
29. Microsoft Security. What is Threat Hunting? 2023. URL: https://www.microsoft.com/en-us/security/business/security-101/what-is-cyber-threat-hunting
30. NIST Special Publication 800-40 Rev. 4. Guide to Enterprise Patch Management Planning. National Institute of Standards and Technology, 2022.
31. IBM Security. User and Entity Behavior Analytics (UEBA). 2023. URL: https://www.ibm.com/think/topics/ueba
32. Постанова Правління Національного банку України №95 від 28.09.2017 «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки та кіберзахисту в банківській системі України». URL: https://zakon.rada.gov.ua/laws/show/v0095500-17
33. [International Accreditation Forum. ISO/IEC 27001 Certification Process Guidance. IAF, 2023. URL: https://www.iaf.nu/articles/IAF_Documents/90
34. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII. Відомості Верховної Ради, 2017, № 45, ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19
35. CISA. Zero Trust Maturity Model v2.0. Washington, D.C.: CISA, 2023. 64 p. URL: https://www.cisa.gov/zero-trust-maturity-model
36. Ponemon Institute. Cost of a Data Breach Report 2024. IBM Security, 2024. 108 p. URL: https://www.ibm.com/reports/data-breach
37. NIST Special Publication 800-61 Revision 3. Incident Response Recommendations and Considerations for Cybersecurity Risk Management. NIST, 2024. URL: https://doi.org/10.6028/NIST.SP.800-61r3
38. MITRE ATT&CK for Enterprise. Financial Services Sector. MITRE Corporation, 2024. URL: https://attack.mitre.org/

39. ServiceNow / Ponemon Institute. The Economics of Security Operations Centers: What Is the True Cost for Organizations? 2023. URL: https://www.servicenow.com/lpayr/ponemon-soc-report.html
40. European Data Protection Board. Guidelines 9/2022 on Personal Data Breach Notification under GDPR. Brussels: EDPB, 2023. URL: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines
41. SANS Institute. Security Operations Center Curriculum: SEC511 (Continuous Monitoring and Security Operations), SEC555 (SIEM with Tactical Analytics). URL: https://www.sans.org/cyber-security-courses/
42. Gartner. Market Guide for Security Operations Center. Gartner, Inc., 2023. URL: https://www.gartner.com/en/information-technology/insights/security-operations-center

ДОДАТКИ

ДОДАТОК А

Таблиця 2.3

Провідні інструментальні засоби SOC та їх відповідність вимогам СМІБ і регуляторів

Клас засобу	Провідні рішення (банківський сектор)	Ключові функції та особливості	Контролі ISO/IEC 27001:2022 та вимоги PCI DSS v4.0	Форми доказів для СМІБ
SIEM	IBM QRadar SIEM	Централізований збір, нормалізація, кореляція подій; виявлення аномалій; зберігання журналів з WORM-захистом; compliance-дашборди	ISO: A.8.15, A.8.16, A.8.17 (моніторинг, журналювання); PCI DSS: вимоги 10.2–10.7 (log management, retention ≥ 12 міс.)	Журнали кореляції; звіти Log Source Coverage; звіти про виявлені інциденти; архів подій з незмінністю (immutable logs)
	Splunk Enterprise Security			
	Microsoft Sentinel			
	ELK Stack (open source)			
EDR/XDR	CrowdStrike Falcon	Безперервний моніторинг кінцевих точок; поведінковий аналіз процесів; автономне реагування (ізоляція хосту, припинення процесів); збір forensic-артефактів	ISO: A.8.7 (захист від шкідливого ПЗ), A.8.8 (вразливості), A.5.26 (реагування); PCI DSS: вимога 5.3 (антивірусний захист)	Звіти виявлення загроз; forensic artifacts (memory dumps, process trees); timeline інциденту від початкового вектору до ліквідації
	Microsoft Defender for Endpoint			
	SentinelOne Singularity			
	Palo Alto Cortex XDR			
SOAR	Palo Alto XSOAR	Автоматизація плейбуків реагування; оркестрація між засобами захисту; управління тікетами інцидентів; авто-документування кроків реагування	ISO: A.5.26 (реагування на інциденти), A.5.27 (навчання на інцидентах); A.5.28 (збір доказів); вимоги НБУ №95 (72-год. звітування)	Хронологія кожного інциденту; плейбуки з відміткою часу; автотаймер для звітів до НБУ/ДПА; «ланцюжок доказів» (chain of custody)
	Splunk SOAR			
	Microsoft Sentinel Automation			
	IBM Resilient			
Threat Intelligence (TI)	Recorded Future	Структуровані дані про кіберзагрози (IoC, TTP за MITRE ATT&CK); галузева розвідка для фінансового сектору; фіди для оновлення правил SIEM	ISO: A.5.7 (Threat Intelligence), A.8.8 (вразливості); PCI DSS: вимога 6.3 (захист від відомих вразливостей)	IoC-фіди; TTP-звіти; звіти щодо APT-груп (Lazarus, FIN7, Carbanak); щомісячні бюлетені про загрози для банківського сектору
	MISP			
	ThreatConnect			
	FS-ISAC			
	Mandiant Advantage			
ulnerability Management (VM)	Tenable Nessus / Tenable.io	Безперервне сканування активів; CVSS-пріоритизація вразливостей; відстеження строків усунення; інтеграція з SOAR для remediation tasks	ISO: A.8.8 (управління технічними вразливостями); PCI DSS: вимоги 11.3 (щоквартальне сканування), 11.4 (тест на проникнення)	Звіти сканування з CVSS-оцінками; плани усунення вразливостей; відстеження MTTR (Mean Time to Remediate)
	Qualys VMDR			
	Rapid7 InsightVM			
DLP (Data Loss Prevention)	Symantec DLP	Моніторинг та блокування витоку конфіденційних даних; контроль каналів передачі (email, USB, хмарні сервіси); класифікація даних	ISO: A.5.12 (класифікація інформації), A.8.12 (запобігання витоку); PCI DSS: вимога 3.4 (захист даних платіжних карток)	Звіти заблокованих передач; інциденти витоку з деталями контенту; статистика порушень політики безпеки даних
	Forcepoint DLP			
	Microsoft Purview Information Protection			
UEBA (User and Entity Behavior Analytics)	Splunk UEBA	Аналіз поведінкових базисів користувачів та пристроїв (ML/AI); виявлення аномалій доступу; виявлення інсайдерських загроз та скомпрометованих акаунтів	ISO: A.5.18 (права доступу), A.8.16 (моніторинг діяльності); PCI DSS: вимога 8.6 (моніторинг привілейованих акаунтів)	Звіти аномальної активності; ризик-скори користувачів; alerts на підозрілі патерни доступу до АБС/ДБО
	Microsoft Sentinel UEBA			
	IBM QRadar UBA			
	Exabeam			

ДОДАТОК Б
Таблиця 3.2
Матриця зіставлення контролів СМІБ ISO/IEC 27001:2022, вимог PCI DSS та процесів SOC

Контроль ISO 27001:2022	Вимога PCI DSS v4.0 / НБУ №95	Процес SOC, що генерує доказ	Інструмент SOC	Форма та частота доказу
A.8.15 – Ведення журналів подій	PCI DSS 10.2, 10.3, 10.7; НБУ №95 Розд. V	Централізований збір та WORM-захист журналів з усієї банківської інфраструктури (АБС, ДБО, AD, мережа, хмара). Щоденний автоматичний звіт Log Source Coverage; алерт при покритті < 98%	SIEM (IBM QRadar / Splunk ES / Microsoft Sentinel); WORM-сховище (захищений archive)	Щоденний звіт Log Source Coverage; retention-звіт щомісяця; hash-верифікація immutability при аудиті
A.8.16 – Моніторинг діяльності	PCI DSS 10.6 (щоденний аналіз); НБУ №95 Розд. V (безперервний моніторинг)	Цілодобовий L1-моніторинг алертів SIEM; UEBA-аналіз поведінкових аномалій; тріаж підозрілих подій; відстеження MTTD	SIEM + UEBA (IBM QRadar UBA / Splunk UEBA / Exabeam)	Щотижневий звіт: кількість алертів, FPR, MTTD у порівнянні з SLA; compliance-дашборд у реальному часі
A.5.26 – Реагування на інциденти ІБ	НБУ №95 Розд. VI (72-год. звіт); PCI DSS 12.10 (план реагування на інциденти)	L2-розслідування підтверджених інцидентів; виконання SOAR-плейбуків; підготовка звітів до НБУ; контроль MTTR	SOAR (Palo Alto XSOAR / Splunk SOAR / MS Sentinel Automation); тікет-система	Тікет SOAR з повною хронологією; автотаймер НБУ-72h; chain of custody документ при кожному P1/P2 інциденті
A.5.28 – Збір доказів	ISO 27001 п. 9.1 (вимірювання); юридична обґрунтованість при судовому розгляді	Збір forensic-артефактів при кожному P1/P2 інциденті; hash-верифікація (SHA-256) для доказу незмінності; зберігання у захищеному архіві	EDR/XDR (CrowdStrike Falcon / SentinelOne); forensic tools (Volatility, Autopsy)	Forensic report з SHA-256 хешами; memory dump; process tree; network capture при кожному суттєвому інциденті
A.8.8 – Управління технічними вразливостями	PCI DSS 11.3 (щоквартальне сканування); PCI DSS 11.4 (pentest щорічно); НБУ №95 Розд. IV	Безперервне CVSS-пріоритизоване сканування активів; SOAR-remediation tasks з дедлайном; контроль MTTR вразливостей; tracking патчування	Tenable Nessus / Qualys VMDR / Rapid7 InsightVM; інтеграція з SOAR	Звіт сканування щоквартально; MTTR-статистика; remediation task з дедлайном; підтвердження закриття вразливостей
A.5.7 – Аналіз інформації про загрози (Threat Intelligence)	ISO 27001 A.5.7 (новий контроль 2022); взаємодія з CERT-UA (Закон №2163-VIII)	Отримання та застосування TI-фідів (IoC, TTP); оновлення правил SIEM; Threat Hunting на основі CTI; звітування про APT-загрози для банківського сектору	Recorded Future / MISP / FS-ISAC / CERT-UA фіди; SIEM-інтеграція	Щомісячний TI-бюлетень; звіт про застосовані IoC у SIEM; нові detection rules на основі ATT&CK / квартал
A.5.23 – ІБ при використанні хмарних сервісів	PCI DSS 12.3.4 (оцінка хмарних рішень); GDPR ст. 28 (DPA для cloud-провайдерів)	Моніторинг хмарних середовищ через CSPM; виявлення misconfiguration; контроль доступу та шифрування; перевірка DPA хмарних провайдерів	MS Defender for Cloud / AWS Security Hub / Prisma Cloud; SIEM-інтеграція	Щотижневий CSPM-звіт про хмарні неналежні конфігурації; підтверджені DPA для хмарних провайдерів
A.5.18 – Права доступу	PCI DSS 7, 8 (контроль доступу, MFA для привілейованих); НБУ №95 Розд. IV	Моніторинг аномалій автентифікації; UEBA для привілейованих акаунтів; виявлення privilege escalation та підозрілих AD-сесій	SIEM + UEBA; PAM-інтеграція (CyberArk / BeyondTrust)	Щомісячний звіт аномалій доступу; alert на privilege escalation; щоквартальний access review звіт

ДОДАТОК В
Таблиця 3.4

Параметри доцільності використання методики щодо забезпечення відповідності системи менеджменту ІБ регуляторним вимогам на підприємстві

Компонент	**Малий банк (активи до 50 млрд грн, бюджет КБ 4,5–22,5 млн грн/рік)**	**Середній банк (активи 100–300 млрд грн, бюджет КБ 20–90 млн грн/рік)**	**Великий банк (активи понад 400 млрд грн, бюджет КБ 100–1000+ млн грн/рік)**	**Джерело**
SIEM	Microsoft Sentinel (хмарна, pay-per-GB, ~1,3–3,5 млн грн/рік) або Wazuh (open-source, витрати лише на інфраструктуру)	Microsoft Sentinel або IBM QRadar on Cloud (~6–12 млн грн/рік); Можливий ELK Stack з комерційними доповненнями	IBM QRadar Enterprise, Splunk Enterprise Security або ArcSight ESM (15 – 25 млн грн/рік); On-prem або гібридна інфраструктура	Gartner Magic Quadrant for SIEM 2024
EDR/XDR	Microsoft Defender for Endpoint Plan 1 (~130–220 грн/пристрій/міс.)	Microsoft Defender for Endpoint Plan 2 або SentinelOne Core (~220–440 грн/пристрій/міс.); Покриття ≥ 95% активів	CrowdStrike Falcon Enterprise або SentinelOne Singularity XDR (~440–880 USD/пристрій/міс.); Покриття 100% активів, включно зі спеціалізованими банківськими терміналами	CrowdStrike Threat Report 2024
SOAR	Microsoft Sentinel Automation (вбудована, без додаткових витрат) або Power Automate для базових плейбуків	Splunk SOAR або Microsoft Sentinel Automation; бібліотека 10–20 плейбуків	Palo Alto Networks XSOAR або Splunk SOAR Enterprise (~4–15 млн. грн/рік); Бібліотека 50+ плейбуків; Повна інтеграція з GRC, CMDB, АБС	Gartner Market Guide for SOAR 2024
Threat Intelligence	Безкоштовні фіди: CERT-UA, MISP Community, FS-ISAC (базовий рівень); Інтеграція IoC вручну або через API	FS-ISAC Member (~25 тис. USD/рік) + MISP з регіональними партнерами; Напівавтоматична інтеграція IoC у SIEM	Recorded Future або Mandiant Advantage (~4–10 млн грн/рік); повна автоматизація TI-інтеграції; Власна CTI-аналітика L3	FS-ISAC Membership Tiers 2024
Управління вразливостями (VM)	Tenable Nessus Essentials (безкоштовно до 16 IP) або OpenVAS; Щоквартальне сканування відповідно до PCI DSS 11.3	Tenable.io або Qualys VMDR (~1–3 млн грн/рік); Безперервне сканування; автоматичний CVSS-трекінг	Tenable.io Enterprise або Rapid7 InsightVM (~3–10 млн грн/рік); Інтеграція з SOAR для автоматичного відкриття remediation tasks	PCI DSS v4.0, вимога 11.3; Tenable State of Cybersecurity 2024
GRC / доказова база	Захищена таблиця (SharePoint / Google Workspace з MFA) + автоматичний PDF-експорт через Power Automate; Реєстр контролів ведеться вручну	ServiceNow GRC або Archer GRC (~1,5–5 млн грн/рік); API-інтеграція з SIEM/SOAR; Аудиторський портал з RBAC	ServiceNow GRC Enterprise або MetricStream (~5–20 млн грн/рік); Повна автоматизація доказової бази; Real-time compliance-дашборд для CISO та регуляторів	ServiceNow / Ponemon Institute [39]
Пріоритетність етапів SOCE	Етапи 1–2 у перші 6 міс.; Етапи 3–5 — у міру зростання зрілості	Етапи 1–2 у перші 6 міс.; Етап 3 у 6–12 міс.; Етапи 4–5 у 12–24 міс.	Повне впровадження всіх 5 етапів за 12–18 міс.; GRC-автоматизація — з першого кварталу	Методика SOCE (підрозділ 3.1)
Очікуваний ROI	Уникнення штрафів НБУ (від 1% регулятивного капіталу) та втрати PCI DSS-статусу; Скорочення витрат на підготовку до аудиту на 40–50%	Скорочення вартості кіберінциденту в середньому на 75 млн грн; Зниження витрат на аудит на 60–70%	Повна автоматизація compliance-звітності; Скорочення MTTD на 95–99%; Запобігання репутаційним збиткам від резонансних інцидентів	Ponemon Cost of a Data Breach 2024 [36]; ServiceNow / Ponemon [39]