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 БЕЗПЕРЕРВНОЇ ВІДПОВІДНОСТІ ФІНАНСОВИХ УСТАНОВ СТАНДАРТАМ PCI DSS ТА SWIFT В ПРОЦЕСІ АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ”

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

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

_____ Кирило КАСТОРНОВ
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-42

Кирило КАСТОРНОВ
Ім’я, ПРІЗВИЩЕ

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

Рецензент: _____
_____ Ім’я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра управління кібербезпекою та захистом інформації

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УКБЗІ
_____ Світлана ЛЕГОМІНОВА
“____”_____2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Касторнову Кирилу Федоровичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Методи забезпечення безперервної відповідності фінансових установ стандартам PCI DSS та SWIFT в процесі аудиту інформаційної безпеки”, керівник кваліфікаційної роботи ЗАПОРОЖЧЕНКО Михайло, доктор філософії з кібербезпеки
(ПРІЗВИЩЕ, Ім’я, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “24” лютого 2025 р. №56.

2. Строк подання кваліфікаційної роботи “12” травня 2025р.
3. Вихідні дані до кваліфікаційної роботи: *інформаційна безпека підприємства, методи та засоби управління станом захищеності підприємства в питаннях інформаційної безпеки, міжнародні стандарти, наукова та технічна література.*
4. Перелік питань, які мають бути розроблені:
   4.1. Проаналізувати вимоги стандартів PCI DSS та SWIFT CSCF, їх структуру, цілі та вплив на безпеку фінансових установ.
   4.2. Визначити особливості впровадження стандартів у внутрішні процеси організації та підходи до забезпечення постійної відповідності.
   4.3. Обґрунтувати методи і засоби аудиту, моніторингу та контролю виконання вимог стандартів.
   4.4. Дослідити стан відповідності фінансової установи та виявити існуючі порушення або прогалини.
   4.5. Розробити план впровадження технічних і організаційних заходів відповідно до вимог PCI DSS та SWIFT CSCF.
   4.6. Провести оцінювання ефективності реалізованих заходів та сформулювати рекомендації щодо подальшого вдосконалення системи управління відповідністю.
5. Перелік ілюстративного матеріалу: *презентація PowerPoint*
6. Дата видачі завдання “5” березня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	14.03.2025	
2.	Збір та аналіз літератури.	20.03.2025	
3.	Аналіз заходів та процесів підтримки безперервної відповідності в компанії.	15.04.2025	
4.	Практична реалізація заходів та процесів підтримки безперервної відповідності в компанії.	20.04.2025	
5.	Розробка рекомендацій стосовно застосування та впровадження заходів та процесів підтримки безперервної відповідності в компанії.	25.04.2025	
6.	Формулювання висновків за результатами проведеного дослідження.	29.04.2025	
7.	Оформлення роботи.	06.05.2025	
8.	Оформлення презентації.	09.05.2025	
9.	Отримання рецензії на роботу.	12.06.2025	
10.	Захист в ДЕК.	__.06.2025	

Здобувач вищої освіти _____ Кирило КАСТОРНОВ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

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

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

Направляється здобувач Касторнов К. Ф. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Методи забезпечення безперервної відповідності фінансових установ стандартам PCI DSS та SWIFT в процесі аудиту інформаційної безпеки"

Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач КАСТОРНОВ Кирило у кваліфікаційній роботі продемонстрував системний підхід до дослідження методів забезпечення безперервної відповідності фінансових установ міжнародним стандартам PCI DSS та SWIFT CSCF. У роботі ґрунтовно проаналізовано вимоги та структуру зазначених стандартів, розкрито теоретичні та методичні засади інтеграції контролів у бізнес-процеси, внутрішній аудит та програми відповідності.

Кирило КАСТОРНОВ також представив практичні підходи до впровадження контролів безпеки, включаючи технічні та організаційні заходи, засоби автоматизації моніторингу відповідності, самооцінки та коригувальні дії. Увагу приділено синхронізації вимог обох стандартів у межах єдиної програми відповідності, що відповідає сучасним практикам GRC.

Здобувач продемонстрував високий рівень обізнаності у темі, вміння критично мислити, узагальнювати практики інформаційної безпеки, застосовувати інструменти аудиту та аналізу. Результати роботи апробовані на науковій конференції.

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

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

"____"_____2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Касторнов К.Ф. допускається до захисту даної роботи в Екзаменаційній комісії.

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

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти КАСТОРНОВА Кирила
на тему “Методи забезпечення безперервної відповідності фінансових установ стандартам PCI DSS та SWIFT в процесі аудиту інформаційної безпеки”

Актуальність. У сучасних умовах стрімкого зростання кіберзагроз і посилення регуляторних вимог до фінансових установ особливої важливості набуває забезпечення постійної відповідності міжнародним стандартам інформаційної безпеки. Стандарти PCI DSS і SWIFT CSCF встановлюють критично необхідні заходи захисту карткових даних і систем міжбанківського обміну. Враховуючи, що аудити відповідності проводяться щороку або частіше, а загрози постійно змінюються, безперервна відповідність стає ключовим підходом до захисту інформаційних активів. Це зумовлює необхідність дослідження методів впровадження, моніторингу та підтримання відповідності вимогам PCI DSS та SWIFT CSCF у постійному режимі, інтегрованому в бізнес-процеси установи. Отже, тема є актуальною, практично значущою та відповідає потребам галузі у підвищенні захищеності та відповідності міжнародним стандартам.

Позитивні сторони:

1. В роботі приділено значну увагу синхронізації вимог стандартів PCI DSS і SWIFT CSCF у межах єдиної програми відповідності.
2. В роботі детально проаналізовано практичні механізми впровадження контролів та забезпечення безперервної відповідності.
3. Робота структурована, має логічний виклад, супроводжується ілюстративним матеріалом та обґрунтованими висновками та практичними рекомендаціями.
4. Матеріал викладено грамотно, з належним оформленням і використанням актуальних джерел.

Недоліки:

1. Було б доцільно надати приклад практичної реалізації запропонованих рішень у конкретній фінансовій установі, з оцінкою вартості їх впровадження.

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

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

Рецензент:

_____ _____ _____

підпис Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена забезпеченню безперервної відповідності фінансових установ стандартам PCI DSS та SWIFT. Робота складається зі вступу, трьох розділів, що містять 6 рисунків, висновків і списку використаних джерел із 45 найменувань. Загальний обсяг роботи становить 85 аркушів, з яких 7 аркушів займає перелік умовних позначень та список використаних джерел.

Метою роботи є забезпечення безперервної відповідності фінансових установ вимогам стандартів PCI DSS та SWIFT CSCF шляхом впровадження методів контролю, автоматизації процесів аудиту та інтеграції стандартів у внутрішню політику інформаційної безпеки організацій.

Об'єкт дослідження **–** процес управління відповідністю стандартам інформаційної безпеки у фінансових установах.

Предмет дослідження – методи впровадження контролів PCI DSS та SWIFT CSCF у бізнес-процеси фінансової установи.

Методи дослідження. В роботі використано методи порівняльного аналізу вимог стандартів, системного підходу до аудиту, практичної апробації заходів безпеки, а також кейс-дослідження з впровадження контролів у межах умовної фінансової установи.

Галузь застосування. Результати роботи можуть бути використані в практичній діяльності фінансових установ для створення ефективних програм відповідності стандартам PCI DSS та SWIFT, а також для підвищення рівня інформаційної безпеки в межах системи управління ризиками.

Ключові слова: PCI DSS, SWIFT CSCF, КОНТРОЛІ БЕЗПЕКИ, АУДИТ ВІДПОВІДНОСТІ, ФІНАНСОВА УСТАНОВА, ІНФОРМАЦІЙНА БЕЗПЕКА, МОНИТОРИНГ, БІЗНЕС-ПРОЦЕСИ.

ABSTRACT

The qualification work is devoted to ensuring continuous compliance of financial institutions with PCI DSS and SWIFT standards. The work consists of an introduction, three chapters containing 6 figures, conclusions and a list of 45 references. The total volume of the work is 85 pages, of which 7 pages are occupied by the list of symbols and references.

The purpose of the study is to ensure continuous compliance of financial institutions with PCI DSS and SWIFT CSCF standards through the implementation of control measures, audit process automation, and integration of standards into internal security policies.

The object of the study is the compliance management process with information security standards in financial institutions.

The subject of the study are methods of implementing PCI DSS and SWIFT CSCF controls into the business processes of financial institutions.

Research methods. The study applies methods of comparative analysis of standards' requirements, a systemic approach to auditing, practical implementation of security controls, and a case study of applying compliance measures within a model financial institution.

Scope of application. The proposed approaches can be applied by financial institutions to develop effective compliance programs with PCI DSS and SWIFT CSCF and to strengthen security management in the context of risk-based frameworks.

Keywords: PCI DSS, SWIFT CSCF, SECURITY CONTROLS, COMPLIANCE AUDIT, FINANCIAL INSTITUTION, INFORMATION SECURITY, MONITORING, BUSINESS PROCESSES.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

MFA	Багатофакторна автентифікація (Multi-Factor Authentication)
VPN	Віртуальна приватна мережа (Virtual Private Network)
CHD	Дані власників карток (Cardholder Data)
DLL	Динамічно приєднувана бібліотека (Dynamic-link library)
NSC	Засоби мережевої безпеки (Network Security Controls)
ROC	Звіт про відповідність (Report on Compliance)
ІБ	Інформаційна безпека
МПС	Міжнародна (-і) Платіжна (-і) Система (-и)
CDE	Середовище даних карткотримачів (Cardholder Data Environment)
IT	Інформаційні Технології
SAD	Чутливі автентифікаційні дані (Sensitive Authentication Data)
BAU	Business as Usual
CSCF	Customer Security Controls Framework
CSP	Customer Security Programme
GRC	Governance, Risk and Compliance
NTP	Network Time Protocol
PCI DSS	Payment Card Industry Data Security Standard
PAN	Primary Account Number
PIN	Personal Identification Number
RMA	Relationship Management Application
SIEM	Security Information and Event Management
IAF	Framework of Independent Assessment
ISO	International Organization for Standardization
TPSP	Third Party Service Provider
TLS	Transport Layer Security
UEBA	User and Entity Behavior Analytics

ВСТУП

Актуальність теми. Фінансові установи залишаються пріоритетною ціллю кіберзлочинців, що зумовлює зростаючу потребу у дотриманні міжнародних стандартів інформаційної безпеки. Стандарти PCI DSS та SWIFT CSCF відіграють ключову роль у захисті платіжних систем і міжбанківських транзакцій, забезпечуючи високий рівень довіри до фінансового сектору.

Забезпечення безперервної відповідності цим стандартам вимагає системного підходу до аудиту, адаптованого до динамічних змін в IT-інфраструктурі, регуляторних вимог і бізнес-процесів. Невиконання вимог може призвести до суттєвих фінансових і репутаційних ризиків. У цьому контексті розробка ефективних методів підтримки відповідності є важливим напрямом для підвищення кіберстійкості фінансових установ.

Метою роботи є забезпечення безперервної відповідності фінансових установ вимогам стандартів PCI DSS та SWIFT CSCF шляхом впровадження методів контролю, автоматизації процесів аудиту та інтеграції стандартів у внутрішню політику інформаційної безпеки організацій.

Об'єкт дослідження **–** процес управління відповідністю стандартам інформаційної безпеки у фінансових установах.

Предмет дослідження – методи впровадження контролів PCI DSS та SWIFT CSCF у бізнес-процеси фінансової установи.

Для досягнення цієї мети в роботі необхідно виконати наступні завдання:

1. Проаналізувати вимоги стандартів PCI DSS та SWIFT CSCF, їх структуру, цілі та вплив на безпеку фінансових установ.
2. Визначити особливості впровадження стандартів у внутрішні процеси організації та підходи до забезпечення постійної відповідності.
3. Обґрунтувати методи і засоби аудиту, моніторингу та контролю виконання вимог стандартів.
4. Дослідити стан відповідності фінансової установи та виявити існуючі порушення або прогалини.

5. Розробити план впровадження технічних і організаційних заходів відповідно до вимог PCI DSS та SWIFT CSCF.

6. Провести оцінювання ефективності реалізованих заходів та сформулювати рекомендації щодо подальшого вдосконалення системи управління відповідністю.

Методи дослідження. В роботі використано методи порівняльного аналізу вимог стандартів, системного підходу до аудиту, практичної апробації заходів безпеки, а також кейс-дослідження з впровадження контролів у межах умовної фінансової установи.

Практичне значення одержаних результатів. Практична значущість полягає в адаптації підходів до реальних умов діяльності фінансової установи, що дозволяє підвищити ефективність системи інформаційної безпеки.

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

Розділ 1 ТЕОРЕТИЧНІ ЗАСАДИ УПРАВЛІННЯ ВІДПОВІДНІСТЮ ВИМОГАМ СТАНДАРТІВ

У першому розділі розглянуто теоретичні основи стандартів PCI DSS та SWIFT CSCF, визначено їх цілі, структуру та принципи. Проведено порівняння підходів до безпеки платіжної інформації та міжбанківських трансакцій, а також проаналізовано концепції BAU як основи безперервної відповідності. Розділ формує базу для практичної реалізації заходів у фінансових установах.

1.1 Визначення вимог стандарту PCI DSS та аналіз його структури і сфери застосування

Стандарт безпеки даних індустрії платіжних карток (PCI Data Security Standard, PCI DSS) - набір вимог, розроблений Радою із стандартів безпеки PCI (PCI Security Standards Council) за участі міжнародних платіжних систем. Метою PCI DSS є підвищення рівня захисту платіжних даних та впровадження єдиних підходів до безпеки даних у фінансовій сфері. Іншими словами, стандарт забезпечує базовий набір технічних та організаційних заходів безпеки для захисту даних держателів платіжних карток від компрометації.

PCI DSS v4.0.1 (оновлення від червня 2024 року) є актуальною редакцією стандарту, що враховує сучасні загрози та технології й продовжує розвиток вимог попередньої v4.0 (оновлення від березня 2024 року) [35]. Стандарт призначений для всіх компаній, які зберігають, обробляють або передають дані карток чи чутливі автентифікаційні дані, включно з компаніями, торговельними підприємствами та TPSP, пов'язаних із платіжними транзакціями.

Стандарт PCI DSS містить 12 основних вимог, об'єднаних у 6 логічних категорій [39]. У таблиці 1.1 наведено огляд цих вимог відповідно до PCI DSS v4.0.1.

Таблиця 1.1

Основні вимоги стандарту PCI DSS та їх мета

Назва розділу	Мета розділу
Побудувати та підтримувати захищені мережі та системи	Установлення та підтримка засобів мережевої безпеки. Застосування безпечних конфігурацій до всіх системних компонентів. Ці вимоги спрямовані на захист периметру мережі та належне налаштування обладнання, зокрема міжмережевих екранів та інших мережевих пристроїв, захист їх від відомих вразливостей тощо.
Установити та підтримувати засоби мережевої безпеки	Застосування безпечних конфігурацій до всіх системних компонентів. Ці вимоги спрямовані на захист периметру мережі та належне налаштування обладнання, зокрема міжмережевих екранів і мережевих пристроїв, захист їх від відомих вразливостей тощо.
Захищати карткові дані	Захист даних держателів карток, які зберігаються. Шифрування карткових даних при передачі у ненадійних мережах. Ці вимоги спрямовані на механізми шифрування й маскування даних карток у місцях, де вони зберігаються та під час передачі, для запобігання перехопленню або витоку.
Підтримувати програму управління вразливостями	Підтримка програми управління вразливостями. Захист всіх системних компонентів та мереж від шкідливого програмного забезпечення. Розробка та підтримка захищених систем і програмного забезпечення. Ці вимоги спрямовані на регулярне оновлення механізмів захисту від шкідливого програмного забезпечення, застосування оновлень безпеки, проведення сканування на вразливості та безпечної розробки застосунків.
Реалізувати надійні заходи контролю доступу	Обмеження доступу до системних компонентів і карткових даних виключно необхідним обсягом (за принципом найменших привілеїв та необхідності знання). Ідентифікація користувачів та автентифікація доступу до систем. Обмеження фізичного доступу до карткових даних. Ці вимоги спрямовані на визначення політики управління обліковими записами, впровадження багатофакторної автентифікації, розмежування прав користувачів, а також заходи фізичної безпеки (контроль зон доступу, замки, відеоспостереження, журнали відвідувань тощо) для захисту приміщень, де обробляються карткові дані.
Моніторити мережі та тестувати системи	Журналювання та моніторинг всіх доступів до системних компонентів та карткових даних. Регулярне тестування безпеки систем та мереж. Ці вимоги спрямовані на налаштування систем журналювання подій, централізованого моніторингу (SIEM), регулярного аналізу журналів подій, проведення сканувань мереж на вразливості та тестування на проникнення для виявлення слабких місць.
Підтримувати інформаційну безпеку на рівні управління	Підтримка заходів інформаційної безпеки за допомогою організаційних політик і програм. Остання вимога встановлює необхідність комплексної політики безпеки, навчання персоналу, процедури реагування на інциденти та регулярного оцінювання ризиків

Кожна з 12 вимог містить детальні підвимоги та процедури тестування для перевірки їх виконання. Таким чином, PCI DSS охоплює широкий спектр заходів від мережевої безпеки і криптографії до управління доступом, моніторингу та корпоративної політики. Важливо зазначити, що PCI DSS надає мінімально необхідний рівень забезпечення безпеки, який може доповнюватися додатковими заходами залежно від специфіки компанії. Якщо законодавство чи регуляторні норми висувають вимоги відмінні від стандарту (наприклад, щодо захисту персональних даних), вони мають перевагу над вимогами стандарту PCI DSS.

Стандарт PCI DSS не має фіксованої сфери застосування, для кожної компанії вона має бути визначена окремо відповідно до визначених у стандарті інструкцій. Визначення правильного обсягу (скоупу) середовища, до якого застосовуються вимоги PCI DSS, є критично важливим першим кроком до досягнення відповідності. PCI DSS поширюється на CDE - сукупність усіх системних компонентів, людей та процесів, що зберігають, обробляють або передають дані держателів карток та/або чутливі автентифікаційні дані. До CDE також включаються будь-які інші системні компоненти, які мають необмежене з'єднання з системними компонентами, переліченими вище (наприклад, привілейоване сусідство в мережі). Іншими словами, межі CDE охоплюють не лише бази даних з картковими даними чи сервери платіжних застосунків, а й усі системні компоненти, здатні вплинути на безпеку цих даних (включно з підтримуючими сервісами - DNS, автентифікація, системи моніторингу тощо). Прикладами компонентів, що входять до скоупу PCI DSS, є: платіжні термінали і сервери авторизації, сховища та сервери обробки транзакцій, системи запобігання вторгненням (IDS/IPS) і міжмережеві екрани (firewall), сервери автентифікації та управління доступом, системи збору журналів і SIEM, засоби сегментації мережі, які ізолюють CDE від іншої інфраструктури, хмарні сервіси або віртуальні машини, у яких обробляються або зберігаються карткові дані тощо. Для належного визначення скоупу стандарт вимагає складати детальні мережеві діаграми та діаграми потоків даних, аби чітко розуміти, де саме

проходять, зберігаються та обробляються карткові дані. Правильна сегментація мережі може ізолювати CDE й суттєво зменшити обсяг систем, які підпадають під PCI DSS, проте помилки сегментації можуть призвести до розширення скоупу на весь IT-ландшафт компанії [1, с. 9].

BAU - безперервна відповідність. Одним з ключових принципів PCI DSS v4.0 є інтеграція вимог безпеки у повсякденні процеси організації. Це означає, що дотримання вимог стандарту має стати невід'ємною частиною операційної діяльності, а не лише періодичним проєктом перед аудитом. Впровадження BAU-підходу гарантує, що заходи, реалізовані для досягнення відповідності, працюють належним чином та на постійній основі, а контроль за ними здійснюється у штатному режимі [6]. Деякі вимоги PCI DSS прямо передбачають регулярний моніторинг як BAU-процес (наприклад, щоденний перегляд журналів або постійний моніторинг стану міжмережевих екранів) - це забезпечує своєчасне виявлення відхилень і підтримання захищеності між аудитами [42]. Стандарт також надає рекомендації щодо найкращих практик BAU, зокрема: призначення відповідальних осіб або команди за програму відповідності стандарту PCI DSS і чіткої управлінської підтримки їх роботи, впровадження метрик ефективності для відстеження стану безпеки (наприклад, регулярність встановлення патчів, результати сканувань, статистика інцидентів), оперативне реагування на збої засобів безпеки (з відновленням контролю, аналізом причин і вжиттям заходів для попередження повторення), впровадження процедур управління змінами з урахуванням вимог PCI DSS (оцінка ризиків перед внесенням змін, перевірка впливу на скоуп і існуючі контролі, оновлення документації після змін), періодичний перегляд зовнішніх підключень та доступів третіх сторін, регулярне виконання внутрішніх перевірок на відповідність (самооцінок) для своєчасного виявлення прогалин у безпеці до аудиту [7; 8]. Таким чином, BAU-підхід фактично переносить акцент з одноразового регулярного проходження аудиту на постійне підтримання належного рівня безпеки [1, с. 19].

PCI DSS установлює конкретні вимоги, так званий визначений підхід, але в певних випадках зазначається, що існують різні способи досягти тієї ж мети безпеки. У версії 4.0 уведено поняття індивідуального підходу - альтернативного способу виконання вимоги, що дозволяє компанії застосувати інноваційні чи відмінні від стандарту заходи, якщо вони досягають визначеної мети вимоги не менше, ніж стандартний підхід. Для більшості вимог у стандарті тепер сформульовано мету індивідуального підходу, якої має бути досягнуто у разі його використання. Такий підхід підтримує гнучкість та інновації в засобах захисту, однак вимагає від організації ретельнішого документування та обґрунтування. При оцінці реалізації індивідуального підходу аудитор має визначити методи тестування і переконатися, що впроваджені заходи не поступаються за ефективністю традиційним вимогам [1, с. 372]. У той же час, стандарт дозволяє й третій варіант - компенсаційні заходи. Це тимчасові або постійні альтернативні рішення, які застосовуються, якщо компанія через об'єктивні технічні, бізнес- або законодавчі обмеження не може напряму виконати вимогу. Компенсаційні заходи повинні бути задокументовані, забезпечувати еквівалентний рівень захисту та зниження ризику, як і початкова вимога, і щорічно переоцінюватися та затверджуватися аудитором. Критерії прийнятності компенсуючих контролів включають: відповідність меті та суворості оригінальної вимоги, надання еквівалентного рівня захисту, відсутність залежності від нерелевантних факторів, актуальність (контроль має закривати поточний ризик, а не попередні реалізації). Наприклад, якщо через відсутність патчу для критичної вразливості неможливо своєчасно її усунути, компанія може тимчасово застосувати компенсуючі заходи: сегментувати мережу, обмежити доступ до вразливого сервісу тільки довіреною зоною, посилити моніторинг і застосувати додаткові засоби захисту, щоб знизити ризик експлуатації вразливості. Усі такі компенсаційні заходи мають бути детально описані в спеціальному документі та включені до звіту про відповідність для перевірки їх повноти та достатності [1, с. 371].

Отже, стандарт PCI DSS пропонує як чітко визначені вимоги - засоби контролю, так і механізми гнучкого підходу, що дозволяють компаніям підтримувати безперервну відповідність, адаптуючись до своїх технологічних особливостей. Головне, щоб кінцева мета безпеки (захист карткових даних) була досягнута, а процеси контролю стали невід'ємною частиною BAU.

1.2 Характеристика програм SWIFT CSP і CSCF та класифікація контролів

SWIFT - міжнародна кооперативна система міжбанківських повідомлень. У відповідь на зростання кіберзагроз і серію інцидентів компрометації банківських систем (зокрема відомий випадок із Банком Бангладеш у лютому 2016 року), SWIFT у 2016 році започаткувала CSP - програму, спрямовану на підвищення рівня захищеності учасників мережі SWIFT [36; 40]. Мета CSP полягає у зміцненні захисту локальної інфраструктури клієнтів SWIFT та запобіганні шахрайським операціям, впровадивши обов'язкові мінімальні заходи безпеки для всіх користувачів системи. Центральним елементом CSP є CSCF, який встановлює конкретні вимоги (контролі) до захисту середовища SWIFT-клієнта. Крім CSCF, CSP включає процес щорічної атестації (самостійного підтвердження відповідності) з боку учасників та механізм прозорості результатів у спільноті, а також навчальні й інформаційні ресурси від SWIFT.

CSCF визначає набір з десятків контрольних заходів безпеки для користувачів SWIFT, поділених на категорії за рівнем обов'язковості та напрямками безпеки. Актуальна редакція - CSCF v2025 - містить 32 вимоги, з яких 25 є обов'язковими для виконання, а 7 мають рекомендаційний характер [9; 11; 16]. Обов'язкові вимоги формують базовий рівень кібербезпеки, обов'язковий до впровадження усіма компаніями в локальному середовищі SWIFT [10]. Вони спрямовані на зменшення ризиків та встановлюють спільний мінімум захисту для всієї спільноти. Рекомендаційні вимоги є галузевими кращими практиками, які SWIFT наполегливо радить впровадити всім компаніям [11]. SWIFT

переглядає та оновлює CSCF щороку відповідно до еволюції загроз та технологій: щороку в середині року анонсуються зміни (нові вимоги або підвищення статусу існуючих), і з наступного року компанії повинні підтвердити відповідність оновленим обов'язковим контролям [37]. Зазвичай нові вимоги спершу додаються як рекомендаційні, даючи учасникам принаймні рік-два на підготовку, і лише потім набувають статусу обов'язкових. Уже оголошено, що один з нинішніх рекомендаційних контролів (2.4A - безпека потоків даних бек-офісу) стане обов'язковим у 2026 році, що підкреслює необхідність завчасного впровадження кращих практик [26].

Усі контрольні вимоги CSCF згруповані за трьома основними стратегічними цілями безпеки SWIFT:

- "Secure your environment" (Захистити своє середовище)
- "Know and limit access" (Знати та обмежувати доступ)
- "Detect and respond" (Виявляти та реагувати)

Кожна ціль розкривається через відповідні принципи безпеки.

Нижче (рис. 1.1) наведено принципи CSCF згідно з зазначеними цілями [2, с. 8; 27].

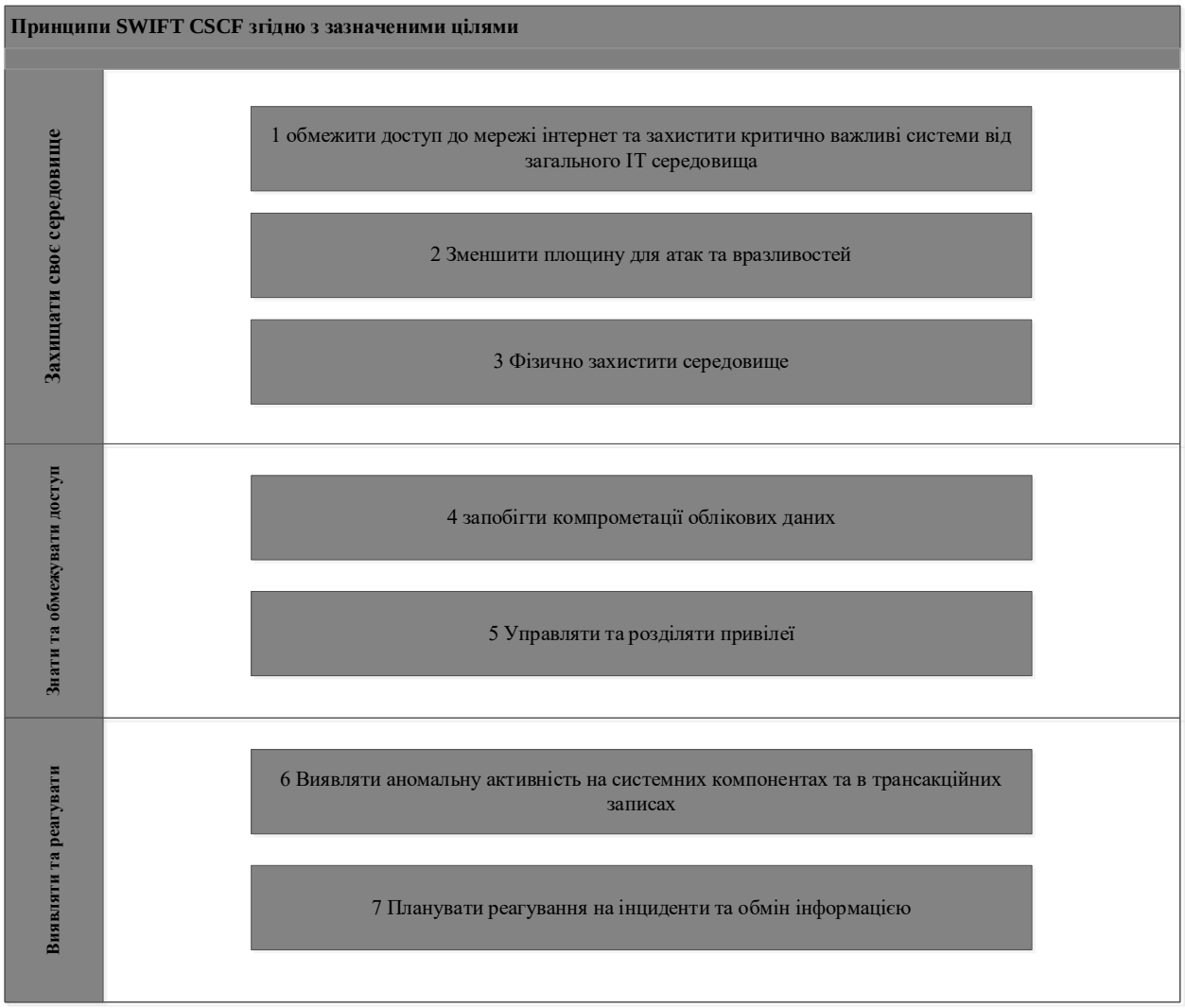

Рис. 1.1. Принципи CSCF та їх цілі

Кожному з принципів відповідає один або декілька конкретних вимог у CSCF. Наприклад, принцип "Обмеження доступу до Інтернету" реалізується заходами щодо ізоляції SWIFT-середовища від прямого виходу в Інтернет, використання проміжних шлюзів тощо. Принцип "Запобігання компрометації облікових даних" охоплює вимоги з впровадження багатофакторної автентифікації для адміністраторів і користувачів SWIFT, впровадження парольних політик тощо.

Важливо, що визначення контролів CSCF узгоджене з галузевими стандартами інформаційної безпеки - при розробці SWIFT спиралася на вже існуючі стандарти (такі як NIST, ISO 27002, PCI DSS тощо), а також на власний

аналіз кіберзагроз та реальні інциденти [12; 41]. Таким чином досягається сумісність вимог SWIFT з іншими загальноприйнятими підходами до безпеки.

Як зазначено, CSCF поділяє всі контролі на два ключові типи обов'язкові та рекомендаційні. Обов'язкові контролі є предметом щорічної оцінки відповідності: кожен користувач SWIFT зобов'язаний впровадити всі застосовні до нього обов'язкові вимоги і підтвердити це у встановленому порядку. Невиконання щонайменше одного обов'язкового контролю означає невідповідність і тягне за собою заходи з боку SWIFT. Рекомендовані вимоги не є обов'язковими для відповідності на поточний рік, але SWIFT очікує, що установи будуть планувати їх впровадження мірою можливості. Із часом такі вимоги можуть стати обов'язковими - з урахуванням розвитку загроз та рівня підготовленості спільноти. Наприклад, контроль 2.4A (захист потоків даних бек-офісу) впродовж певного часу був рекомендаційним, а оголошено, що у 2026 стане обов'язковим. SWIFT завчасно інформує про такі зміни, щоб учасники могли проактивно впровадити і протестувати нові заходи безпеки. Процес поступового підвищення вимог дозволяє досягти колективного підвищення рівня безпеки в глобальному масштабі, не ставлячи учасників перед непосильними негайними змінами.

Важливою частиною програми CSP є щорічна атестація безпеки кожного користувача SWIFT. Атестація полягає у тому, що установи щороку самостійно оцінюють свою відповідність вимогам CSCF і офіційно засвідчують рівень виконання всіх обов'язкових контролів через спеціальний сервіс KYC-Security Attestation (KYC-SA). Кінцевий термін подання річної оцінки - не пізніше грудня поточного року або дати завершення дії актуальних вимог (як правило, оцінка відбувається в період з липня по грудень кожного року). Нові учасники SWIFT повинні пройти оцінку перед початком роботи у мережі SWIFT. Оцінка включає заповнення анкети, де зазначається статус кожної обов'язкової вимоги (впроваджено, не впроваджено, не застосовується), та підтвердження на рівні керівництва установи.

З 2021 року SWIFT увів вимогу про незалежну оцінку результатів атестації відповідно до IAF [45]. Це означає, що кожна компанія повинна залучити кваліфікованих незалежних експертів для перевірки достовірності своєї самооцінки. Таку роль може виконати як внутрішній аудитор, так і зовнішній консультант або аудитор, за умови належного рівня компетентності та незалежності від процесів, що перевіряються. SWIFT запровадила сертифікацію для зовнішніх оцінювачів (Certified CSP Assessor), і багато великих фірм надають послуги з незалежної перевірки CSCF. Вимоги IAF передбачають, що незалежна оцінка має проводитися щонайменше раз на 3 роки для всіх учасників, а для деяких категорій - щороку. Проте багато фінансових установ вважають за краще здійснювати таку перевірку щорічно, інтегруючи її з внутрішнім аудитом, щоб мати впевненість у поточному стані захищеності.

Результати оцінки (відповідність чи наявність невідповідностей) стають видимими для контрагентів через KYC-SA: банки можуть переглядати статус виконання контролів своїх кореспондентів (що підвищує прозорість та стимулює кожного учасника підтримувати відповідність).

Якщо компанія не подає атестацію або заявляє про невиконання якихось обов'язкових контролів, SWIFT може застосувати ряд заходів: від оповіщення інших учасників про статус, до вимоги розробити план ремедації та ескалації до наглядових органів чи відключення від мережі SWIFT. Такий жорсткий підхід мотивує фінансові установи відповідально ставитися до вимог CSCF.

Отже, SWIFT CSP і CSCF установлюють чіткі вимоги до захищеності компаній у частині систем SWIFT, класифікують ці вимоги на обов'язкові та рекомендаційні, а через механізм щорічної оцінки та незалежного оцінювання забезпечують контроль їх виконання. Завдяки CSP у глобальному банківському співтоваристві створено єдиний базовий рівень безпеки, який знижує ризики успішних атак на системи міжбанківських платежів і підвищує довіру між контрагентами.

1.3 Оцінка впливу стандартів PCI DSS та SWIFT CSCF на інформаційну безпеку фінансових установ

Стандарти PCI DSS і SWIFT CSCF суттєво впливають на стан інформаційної безпеки фінансових компаній, визначаючи мінімально необхідні заходи захисту в різних сегментах фінансової діяльності. Їх впровадження підвищує загальну кіберстійкість компанії, зменшує вразливість до інцидентів та формує процеси підтримки безперервної відповідності.

Для компаній, які працюють з картковими даними, відповідність PCI DSS є обов'язковою вимогою від МПС. Дотримання PCI DSS безпосередньо сприяє підвищенню безпеки CDE та зменшенню ризику компрометації карткових даних.

По-перше, впровадження 12 вимог PCI DSS забезпечує всебічний захист: від міжмережевих екранів до шифрування даних і моніторингу аномалій. Наприклад, шифрування PAN в базах даних і захищений протокол передачі TLS унеможливлюють перехоплення або зчитування даних зловмисником у відкритому вигляді. Регулярне сканування на вразливості та встановлення патчів знижують ймовірність того, що відомі вразливості можуть бути застосовані проти систем компанії. Вимоги PCI DSS щодо багатофакторної автентифікації та жорсткого розмежування прав істотно ускладнюють дії інсайдерів та зловмисників, які здобули облікові дані співробітників - це знижує ризик несанкціонованого доступу до критичних систем.

По-друге, відповідність PCI DSS підвищує готовність до виявлення та реагування на інциденти. Обов'язковий моніторинг журналів доступу та подій означає, що компанія постійно відстежує потенційно підозрілі дії у CDE. Це дозволяє своєчасно виявляти спроби зламу або аномальну поведінку та оперативно реагувати. Наявність чітких процедур реагування на інциденти та планів безперервності означає, що компанія заздалегідь готується до можливих витоків даних: визначені команди реагування, канали повідомлення МПС та клієнтів, плани зменшення шкоди. Це значно скорочує час реагування і зменшує збитки, якщо інцидент все ж трапляється.

По-третє, впровадження PCI DSS загальний рівень інформаційної безпеки в компанії. Оскільки стандарт вимагає формалізації політик, навчання персоналу щодо інформаційної безпеки та відповідальності керівництва за програми відповідності, співробітники компанії краще усвідомлюють важливість захисту даних і дотримуються встановлених процедур. У випадку порушення відповідності компанія зіштовхується з ризиками: можливі штрафні санкції від МПС, підвищення комісій за транзакції або навіть призупинення права працювати з картками. Натомість підтверджена відповідність додає довіри з боку партнерів і клієнтів, адже свідчить про серйозне ставлення до захисту карткових даних.

Стандарт SWIFT CSCF орієнтований на захист дуже специфічної, але критично важливої ділянки - систем, що взаємодіють із мережею SWIFT, які за своєю природою оперують великими сумами в міжбанківських переказах. Незважаючи на цей вузький фокус, підтримка відповідності CSCF має широкий позитивний ефект на інформаційну безпеку банку. Обов'язкові вимоги, такі як повне відділення SWIFT-систем від офісної мережі, мінімізація кількості серверів та робочих станцій з доступом до SWIFT значно ускладнюють проникнення зловмисників у потрібний сегмент.

По-перше, SWIFT CSCF приділяє особливу увагу захисту автентифікаційних даних та управлінню доступом. Вимоги передбачають обов'язкове використання MFA для будь-якого адміністративного доступу до систем SWIFT та банківських додатків, що відправляють платежі - це знижує ризик компрометації облікових записів шляхом підбору паролю або фішингу. Регулярний перегляд прав користувачів і принцип мінімальних привілеїв гарантує, що коло осіб з доступом до функцій SWIFT є обмеженим і кожен має лише необхідний мінімум прав. У сукупності ці заходи практично унеможливлюють сценарії атак, подібні до згаданого випадку 2016 року, коли зловмисники отримали доступи та відправили фальшиві повідомлення SWIFT.

По-друге, CSCF орієнтує компанії на проактивне виявлення та реагування на інциденти в середовищі SWIFT. Вимоги передбачають впровадження засобів

виявлення аномалій - наприклад, системи, що відслідковують відхилення у шаблонах транзакцій або незвичні дії користувачів SWIFT. Так, якщо зазвичай банк відправляє платежі до певної країни у межах певної суми, та раптом фіксується спроба відправити значно більшу суму на нетипового контрагента, система виявлення аномалій оповістить відповідальний персонал. У той же час, вимоги зобов'язують компанії мати план реагування на інциденти, що охоплює як кібератаки, так і заходи інформаційного обміну - з регуляторами, правоохоронцями, SWIFT ISC/ISAC (форум з обміну інформацією). У випадку аномальної активності, компанія повинна мати готовність негайно відключити вузол від SWIFT, повідомити SWIFT про інцидент, сповістити інших учасників про можливі фальшиві повідомлення. Це підвищує оперативність реагування і обмежує масштаб потенційного шахрайства.

По-третє, виконання CSCF часто стимулює загальне підвищення рівня захищеності в компанії, виходячи за межі лише SWIFT-систем. Багато вимог CSCF узгоджені з найкращими практиками, що корисні для всіх IT-систем. Вимоги до убезпечення серверів SWIFT можуть бути застосовані як модель для всіх серверів компанії. Таким чином, дотримуючись SWIFT CSCF, компанія водночас підвищує загальний стан захищеності. Варто згадати, що SWIFT має орієнтацію вимог CSCF на інші стандарти, що дозволяє компаніям використовувати підтримку CSCF для закриття суміжних вимог у інших стандартах. Наприклад, вимога з управління вразливостями SWIFT відповідає розділу управління вразливостями ISO 27001, якщо компанія це робить для SWIFT, їй легше продемонструвати відповідність як SWIFT, так і ISO, і PCI водночас.

Обидва стандарти - PCI DSS і SWIFT CSCF - доповнюють один одного у контексті охоплення різних напрямів безпеки. PCI DSS фокусується переважно на захисті карткових даних, тоді як SWIFT CSCF адресує міжбанківським платежам. Разом вони охоплюють критичні для компаній інформаційні активи, які оперують фінансовими транзакціями.

Нижче, у таблиці 1.2 наведено порівняння основних характеристик та області застосування PCI DSS та SWIFT CSCF з точки зору інформаційної безпеки компанії.

Таблиця 1.2

Порівняльна характеристика стандартів PCI DSS та SWIFT CSCF

Параметр	**PCI DSS v4.0.1**	**SWIFT CSCF v2025**
Сфера захисту	Карткові дані та CDE	Локальна інфраструктура SWIFT
Кількість і тип вимог	12 основних вимог та близько 250 підвимог, усі є обов'язковими до виконання, є можливість використання індивідуального підходу та компенсаційних заходів	32 вимоги, з яких 25 обов'язкових та 7 рекомендаційних, певні вимоги не застосовуються в залежності від типу архітектури
Орган управління стандартом	Рада PCI SSC створена МПС	Кооператив SWIFT
Оцінка відповідності	Обов'язковий щорічний аудит відповідності	Щорічна самооцінка в KYC-SA з підтвердженням виконання всіх обов'язкових вимог до кінця року. Щонайменше 1 раз на 3 роки незалежна оцінка відповідно до SWIFT IAF
Вплив на безпеку компанії	Зменшення ризику витоку карткових даних та шахрайства з картковими даними. Підвищення рівня захисту IT-інфраструктури	Зниження ризику несанкціонованих міжбанківських транзакцій. Ізоляція критичних систем та контроль доступу до них

Компанії, які дотримуються обох стандартів, отримують комплексний захист фінансових даних та процесів. Багато вимог PCI DSS і SWIFT CSCF доповнюють одна одну. Наприклад, PCI DSS вимагає управління вразливостями і встановлення патчів, так само SWIFT вимога 3.1 покладає регулярне усунення вразливостей - тобто, налагодивши один процес, компанія автоматично задовольняє обидва стандарти. Вимоги обох стандартів щодо MFA (PCI DSS вимога 8, SWIFT вимога 5.1) сприяють впровадженню єдиної корпоративної системи MFA для всіх критичних доступів. Таким чином, інвестиції в безпеку окуповуються двічі, покриваючи різні напрямки ризиків. У результаті знижується ймовірність як масового витоку карткових даних, так і цільового пограбування через підробку платіжних повідомлень.

Варто підкреслити, що вплив стандартів виходить за межі суто технічної безпеки - він також стимулює вдосконалення процесів управління ризиками. Регулярні аудити й атестації змушують керівництво банку бути обізнаним про стан безпеки, інвестувати в сучасні засоби захисту та навчання персоналу.

1.4 Аналіз підходів до впровадження вимог стандартів у систему внутрішнього аудиту

Ефективне дотримання стандартів PCI DSS та SWIFT CSCF вимагає не лише одноразових зусиль із впровадження вимог, але й постійного контролю та перевірки їх виконання [13; 14; 23]. Внутрішній аудит інформаційної безпеки відіграє ключову роль у забезпеченні безперервної відповідності - він виступає незалежним механізмом оцінки, що дозволяє виявляти та усувати недоліки до того, як це призведе до зовнішніх невідповідностей чи інцидентів.

Першим кроком є інтеграція вимог стандартів у внутрішню контрольну середу компанії. Практично це означає, що всі 12 вимог PCI DSS та застосовні вимоги SWIFT CSCF повинні бути відображені у внутрішніх політиках, процедурах та планах внутрішніх аудитів. Компанія може створити матрицю відповідності, яка зіставляє вимоги стандартів з конкретними внутрішніми політиками та відповідальними підрозділами. Наприклад, вимогу PCI DSS щодо щоденного перегляду журналів подій (10.6) можна відобразити у внутрішній процедурі моніторингу SIEM, за яку відповідає відділ безпеки, а внутрішній аудит перевіряє журнал виконання цієї процедури щомісяця. Аналогічно, контроль SWIFT про ізоляцію мережі (принцип 2) відображається у політиці мережевої безпеки з відповідними налаштуваннями міжмережевих екранів, і аудит може шляхом вибіркового тестування переконатися, що правила фільтрації відповідають вимогам (наприклад, відсутність прямих підключень Інтернет - SWIFT).

Внутрішній аудит повинен врахувати частоту зовнішніх оцінок відповідності стандартам PCI DSS та SWIFT CSP при формуванні свого плану.

Оскільки офіційна оцінка PCI DSS виконується щонайменше 1 раз на рік, а атестація SWIFT - теж, внутрішні перевірки мають передувати цим подіям [15]. Наприклад, рекомендується проводити комплексний внутрішній аудит PCI DSS за кілька місяців до приходу аудиторів, аби виявити слабкі місця та мати час на коригування. Такий "попередній аудит" може імітувати зовнішній - внутрішні аудитори проходять по всіх вимогах PCI DSS, перевіряючи наявність необхідних доказів для кожного пункту [18]. Виявлені невідповідності оформлюються як зауваження, а відповідальні підрозділи повинні оперативно їх усунути - подібний підхід значно підвищує шанси успішно пройти зовнішню сертифікацію з першого разу [17].

Для SWIFT CSCF внутрішній аудит може щороку проводити незалежну оцінку виконання вимог SWIFT IAF. Якщо компанія вирішила покладатися на внутрішній аудит як незалежну функцію, слід забезпечити, щоб аудитори не були залучені до операційного виконання самих вимог. Внутрішній аудит також варто планувати заздалегідь до моменту зовнішньої оцінки (до липня, коли відкривається вікно подачі KYC-SA). Перевірка охоплює: технічні тести (наприклад, спроби доступу до сегментованої зони з загальної мережі - щоб перевірити, чи справді ізоляція працює), аналіз конфігурацій (налаштування міжмережевих екранів, систем доступу), опитування відповідальних адміністраторів щодо виконання процедур (наприклад, чи регулярно змінюються паролі, чи оновлюється антивірус) і огляд документів (наявність актуальних політик, протоколів навчань тощо). Результати внутрішньої перевірки потім використовуються керівництвом для заповнення офіційної самооцінки SWIFT: фактично, внутрішній аудит стає гарантом позитивного проходження оцінки, що затверджується вищим керівництвом.

Окрім періодичних повних аудитів, світовою тенденцією є впровадження елементів неперервного аудиту та моніторингу стану відповідності. Для стандартів, які вимагають BAU-процесів (як PCI DSS), внутрішній аудит може розробити систему постійного відстеження ключових контрольних показників (KPI/KRI). Наприклад, за вимогою PCI DSS 11.5 - налаштовано інструмент FIM,

що генерує оповіщення; аудитор може отримувати щомісячний звіт: скільки оповіщень спрацювало і як швидко вони були досліджені. За вимогою 5 - звіт про оновлення антивірусних баз на 100% системних компонентів, які було оцінено як такі, що підпадають під ризик зараження шкідливим програмним забезпеченням. Таким чином, аудит виконує роль другого рівня контролю, автоматично збираючи інформацію про дотримання вимог. Якщо KPI виходить за межі норми, аудитор ініціює позачергову перевірку або запит до IT-безпеки, щоб вжити негайних заходів, не очікуючи планового аудиту чи, тим більше, інциденту.

Для SWIFT-контролів можливе аналогічне відстеження: наприклад, вимога 7 - якщо впроваджено систему, що рахує аномальні транзакції, внутрішній аудит може щоквартально переглядати зведення про виявлені аномалії та дії, які на них вживалися. Контроль 2 (сегрегація) - аудит може раз на півроку ініціювати тестове сканування порушення сегрегації (переконатися, що ізольована мережа лишається ізольованою і нові підключення не з'явилися без погодження). Такий проактивний моніторинг підсилює BAU-процеси: якщо IT-служби є першою лінією, які здійснюють щоденний контроль, то внутрішній аудит - третя лінія, що періодично перевіряє самі контролі і сигналізує про ризики керівництву.

Підходом до вдосконалення внутрішнього аудиту є аналіз висновків зовнішніх оцінок. Кожен цикл зовнішньої перевірки може виявити нюанси або кращі практики, які варто імплементувати. Внутрішній аудит має брати ці рекомендації до уваги. Наприклад, зовнішній аудитор міг вказати, що журнал адміністрування міжмережевого екрану ведеться нерегулярно - внутрішній аудит додасть цей пункт до регулярної перевірки. Або аудитор SWIFT порадив удосконалити процес перегляду облікових записів - аудит проконтролює впровадження цієї поради і перевірить її виконання в наступній ітерації.

Внутрішній аудит за результатами кожної перевірки стандартів повинен готувати детальний звіт керівництву з описом знайдених невідповідностей і рекомендаціями. У контексті PCI DSS та SWIFT CSCF ці звіти часто

направляються не лише IT-підрозділам, а й комітету з управління ризиками або аудиторському комітету при раді банку, оскільки питання відповідності цим стандартам знаходяться під пильною увагою регуляторів і партнерів.

Впровадження стандартів у практику аудиту потребує від самих аудиторів високої кваліфікації. Тому банки інвестують у навчання внутрішніх аудиторів специфіці PCI DSS та SWIFT CSCF. Деякі аудитори отримують сертифікації як, наприклад, Internal Security Assessor (ISA) від PCI SSC - програма, що навчає працівників компаній проводити внутрішні оцінки PCI DSS на рівні, наближеному до QSA. Для SWIFT внутрішні аудитори можуть проходити офіційні тренінги SWIFT по CSP або навчання від сертифікованих асесорів, щоб розуміти тонкощі.

Нарешті, забезпечення безперервної відповідності - це спільне завдання, тому внутрішній аудит тісно координується з першою та другою лініями захисту. У багатьох компаніях створені окремі групи комплаєнсу PCI DSS/CSP, які знаходяться у другій лінії і відповідають за щоденний моніторинг виконання вимог, підготовку до аудитів. Внутрішній аудит взаємодіє з ними, обмінюючись результатами: наприклад, аудит надає свої виявлені недоліки цій групі для супроводу їх усунення, а група комплаєнсу ділиться з аудиторами своїми регулярними звітами і спостереженнями. Такий постійний зворотний зв'язок гарантує, що жоден аспект не залишиться без уваги. На рисунку 1.2 умовно зображено модель такої взаємодії, де цикли виконання вимог і моніторингу доповнюються незалежною оцінкою, результатом чого є керованість процесу відповідності стандартам у безперервному режимі.

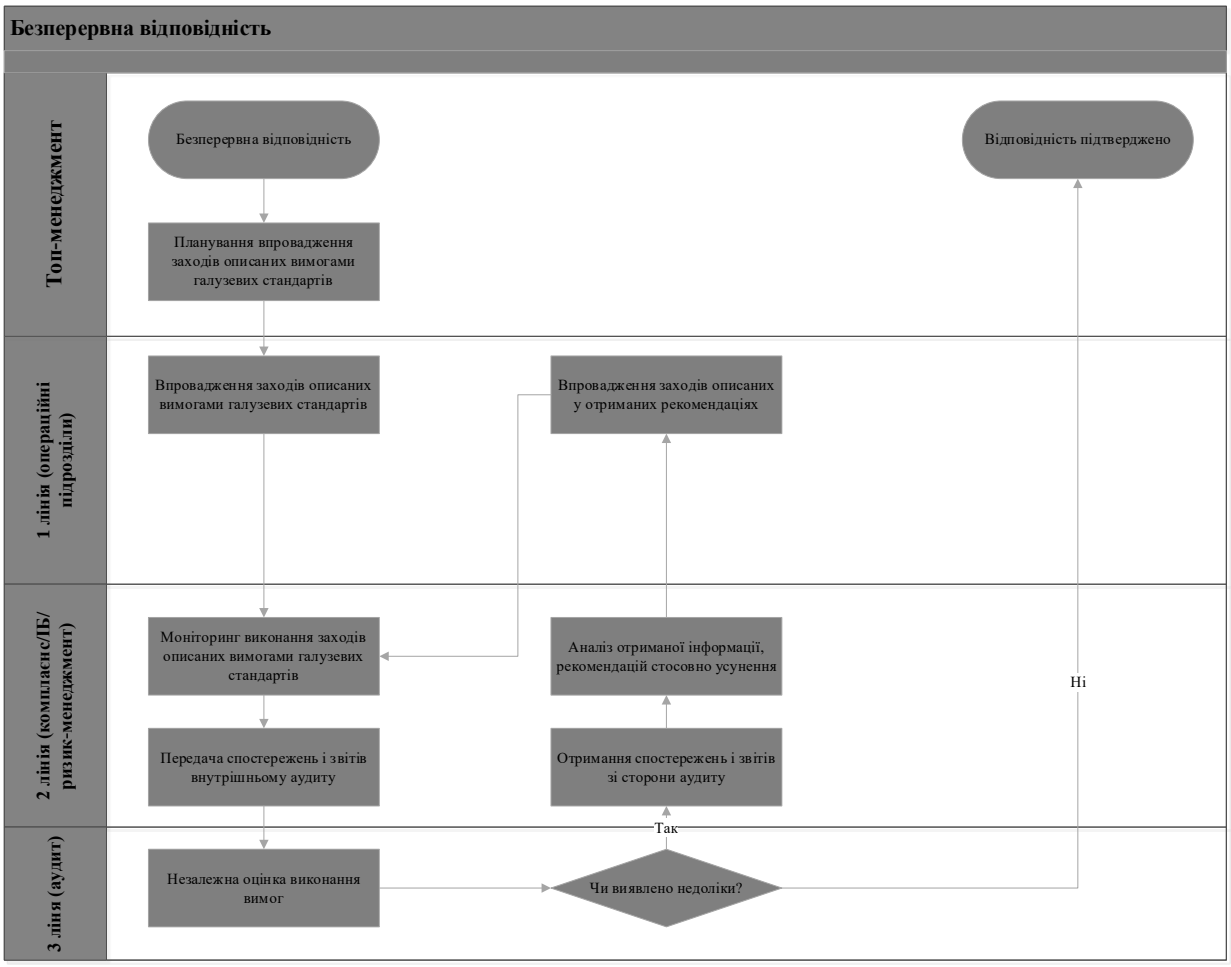

Рис. 1.2. Модель безперервної відповідності стандартам PCI DSS та SWIFT CSCF

Висновки до розділу 1

Підсумовуючи, впровадження вимог PCI DSS та SWIFT CSCF у систему внутрішнього аудиту дозволяє компаніям підтримувати високий рівень інформаційної безпеки на постійній основі. Внутрішній аудит, діючи проактивно, забезпечує своєчасне виявлення відхилень, допомагає бізнесу залишатися у відповідності з жорсткими галузевими стандартами і тим самим оберігає установу від фінансових, юридичних та репутаційних втрат. Це створює ситуацію, коли відповідність перестає бути разовою проблемою "підготуватися до перевірки", а стає частиною щоденного управління ризиками та культури безпеки компанії - що і є кінцевою метою як PCI DSS, так і SWIFT CSP.

Розділ 2 МЕТОДИЧНІ ПІДХОДИ ДО ВПРОВАДЖЕННЯ ТА ПІДТРИМАННЯ БЕЗПЕРЕРВНОЇ ВІДПОВІДНОСТІ СТАНДАРТАМ PCI DSS ТА SWIFT CSCF

У другому розділі досліджено методи інтеграції вимог стандартів PCI DSS та SWIFT CSCF у бізнес-процеси фінансової установи. Розкрито підходи до формування внутрішньої програми відповідності, організації аудиту та самооцінки, а також застосування автоматизованих засобів моніторингу. Узагальнено організаційні й технічні аспекти забезпечення безперервного контролю та управління відповідністю.

2.1 Інтеграція вимог стандартів у бізнес-процеси фінансової установи

Безперервна відповідність вимогам стандартів - підхід, за якого дотримання вимог PCI DSS та SWIFT CSCF інтегрується у бізнес-процеси компанії як BAU. Такий підхід означає, що виконання вимог безпеки стає невід'ємною частиною операційної діяльності, а не разовим проєктом під час підготовки до аудиту. PCI DSS прямо рекомендує організаціям впроваджувати заходи безпеки в режимі BAU для збереження постійної відповідності між періодичними аудитами. SWIFT аналогічно декларує, щоб вимоги безпеки SWIFT CSCF виконувались безперервно: оскільки CSP щорічно їх оновлює для протидії новим кіберзагрозам, компанії повинні впроваджувати процеси та процедури в щоденну діяльність.

Першочергово необхідно визначити ролі та відповідальність за відповідність вимогам. Керівництво має призначити окрему уповноважену особу або команду, відповідальну за програму дотримання PCI DSS та SWIFT. Вище керівництво повинно офіційно закріпити цю відповідальність та надати необхідні повноваження і ресурси для реалізації вимог. Вимоги стандартів мають бути відображені у внутрішніх політиках і процедурах: наприклад, політики управління доступом, шифрування даних, мережевої безпеки, реагування на

інциденти тощо повинні враховувати як вимоги PCI DSS, так і SWIFT CSCF. Важливо інтегрувати контроль виконання вимог у вже існуючі бізнес-процеси компанії: процеси управління персоналом повинні включати перевірку дотримання вимог безпеки; процес управління підрядниками має враховувати вимоги PCI DSS щодо взаємодії із TPSP та вимоги SWIFT щодо безпеки TPSP; процес розробки продуктів та послуг - містити етап перевірки відповідності вимогам. Таким чином, питання безпеки включаються до бізнес-рішень на ранніх стадіях, а не вирішуються постфактум.

Технічні заходи безпеки повинні стати частиною стандартних операцій IT-підрозділу. Зокрема, інфраструктурні зміни мають проходити через процедури оцінку ризиків та впливу на відповідність: перед впровадженням будь-якого нового IT-рішення воно аналізується, на предмет впливу на область застосування PCI DSS або безпеку середовища SWIFT. Наприклад, зміна мережевих конфігурацій повинна супроводжуватися оцінкою, чи не додає вона нові системи до CDE. Якщо так - ці системи потрібно включити до сфери застосування PCI DSS та захистити згідно вимог стандарту. Усі нові проекти і процеси слід розробляти з урахуванням принципів "Secure by Design" і вимог стандартів. Наприклад, при розгортанні нових сервісів компанія одразу впроваджує вимоги PCI DSS щодо мережевої сегментації та вимоги SWIFT щодо відділення середовища SWIFT від загальної IT-мережі. Важливо, щоб усі підрозділи усвідомлювали свою роль у підтриманні відповідності: IT-служби відповідають за технічне виконання вимог, бізнес-підрозділи - за дотримання процедур безпеки у своїй діяльності.

Стандарти PCI DSS та SWIFT передбачають конкретні регулярні заходи, які мають виконуватися на постійній основі. Наприклад, PCI DSS вимагає щоденного перегляду журналів безпеки (Вимога 10) та безперервного моніторингу мережевого середовища на наявність аномалій. Щоб інтегрувати це в повсякденну роботу, компанія налаштовує щоденні процедури аналізу журналів - як правило, це покладається на SOC або відповідальних адміністраторів, які переглядають журнали подій у SIEM-системі. Ще один

критично важливий BAU-процес - управління змінами: у компанії впроваджується процедура, за якою будь-яка зміна IT-систем попередньо оцінюється на предмет впливу на відповідність стандартам. Перед внесенням змін проводиться аналіз ризиків і за необхідності - тестування безпеки; документація оновлюється відповідно до змін. Завдяки цьому середовище залишається підконтрольним навіть у процесі розвитку: жодна система не випадає області аудиту.

Отже, інтеграція вимог PCI DSS та SWIFT CSCF у бізнес-процеси дозволяє компанії підтримувати належний рівень відповідності на постійній основі. Компанія не лише виконує вимоги для чергового аудиту, але й постійно проактивно контролює безпеку.

2.2 Формування внутрішньої програми забезпечення відповідності стандартам

Для системного підтримання вимог PCI DSS та SWIFT CSCF компанія має сформувати внутрішню програму забезпечення відповідності - комплексну систему заходів управління відповідністю, інтегровану у структуру компанії [28]. Така програма визначає політики, процеси, ресурси та метрики, необхідні для постійного виконання вимог стандартів. Вона охоплює як організаційні елементи (управлінські рішення, розподіл відповідальності, навчання персоналу), так і технічні.

На першому етапі формується нормативна база програми відповідності. Розробляється комплект внутрішніх політик та процедур, узгоджених із вимогами стандартів [29]. Зокрема, відповідно до вимоги 12 PCI DSS, організація повинна мати інформаційну безпекову політику, яка охоплює захист карткових даних і регламентує ролі та обов'язки. Така політика доповнюється процедурами, що деталізують виконання кожної з вимог PCI DSS у повсякденній діяльності. Одночасно розробляються політики та стандарти безпеки для середовища SWIFT: політика користування системою SWIFT, процедури управління

ключами й паролями SWIFT, процедури моніторингу трансакційної активності тощо. Усі ці документи узгоджуються між собою та із загальною політикою інформаційної безпеки компанії, щоб виключити протиріччя і дублювання.

Програма відповідності повинна функціонувати за підтримки вищого керівництва. Керівництво компанії затверджує офіційно створення програми, призначає менеджера програми відповідності та формує робочу групу з представників різних підрозділів. До такої групи зазвичай входять: спеціалісти інформаційної безпеки, IT-інфраструктури, підрозділу платежів/процесингу, операційного підрозділу, відповідального за SWIFT-платежі, представники внутрішнього аудиту та ризик-менеджменту. Робоча група координує впровадження вимог: оцінює поточний рівень відповідності, планує заходи з удосконалення, відстежує виконання завдань. Від вищого керівництва очікується нагляд за програмою - на засіданнях IT-комітету або комітету з операційних ризиків мають розглядатися питання статусу відповідності, ключові показники і проблеми [31]. Такий підхід гарантує, що вимоги стандартів пріоритизуються на рівні всієї компанії, а не залишаються турботою лише ІБ-підрозділу.

Формування внутрішньої програми варто розпочати з комплексної оцінки - аналізу розривів між поточним станом систем безпеки і вимогами PCI DSS та SWIFT CSCF. На цьому етапі залучена робоча група проводить інвентаризацію всіх процесів, систем і активів, на які поширюються стандарти - визначається сфера відповідності - середовища PCI DSS та SWIFT). Для PCI DSS ідентифікуються всі системні компоненти, що зберігають, обробляють або передають CHD, оцінюється їхній захист згідно вимог стандарту. Для SWIFT - визначаються усі компоненти, що входять до середовища, та оцінюється виконання кожного з 25 обов'язкових контролів CSCF. Результатом проміжного аналізу є перелік невідповідностей. Для кожного виявленого недоліку оцінюється критичність ризику та зусилля для усунення.

Наступний етап - планування заходів щодо забезпечення відповідності. На основі результатів оцінки розробляється внутрішній план досягнення та

підтримання відповідності. У ньому встановлюються конкретні заходи (технічні та організаційні), відповідальні особи, ресурси та строки виконання для усунення кожної прогалини. Кожен захід повинен відображати відповідність певним вимогам стандартів. Таким чином, формується дорожня карта відповідності. Важливо закласти в план не лише разові проєкти, а й постійні процеси. План затверджується керівництвом, щоб забезпечити виділення фінансування та ресурсів на реалізацію.

Останній етап - безпосереднє впровадження та експлуатація програми. Згідно з розробленим планом, банк виконує необхідні технічні та організаційні зміни. Це може включати: модернізацію інфраструктури, впровадження нових систем безпеки, оновлення конфігурацій і правил, розробку нових процедур. Паралельно проводиться навчання персоналу щодо нових процесів і контролів: наприклад, якщо вводиться правило, що всі адміністратори SWIFT повинні використовувати робочі станції з належною обачністю, це забезпечується за допомогою тренінгів та інструктажів. Після впровадження необхідних змін здійснюється внутрішня перевірка на повноту виконання плану: команда відповідності або внутрішній аудит повторно перевіряють статус відповідності вимогам і переконуються, що всі ключові моменти впроваджено та задокументовано, а програма перейшла у фазу підтримання.

Внутрішня програма відповідності не є статичною - вона працює в циклі PDCA (Plan - Do - Check - Act) (рис. 2.1), постійно вдосконалюючись. Необхідно визначити метрики і ключові показники (KPI/KRI) для оцінки ефективності контролів та процесів програми. Наприклад, час реагування на інцидент, відсоток серверів з актуальними патчами, кількість виявлених вразливостей високого рівня, кількість порушень політик користувачами тощо - все це може слугувати індикаторами відповідності [21]. Регулярний моніторинг цих показників дозволяє виявляти тенденції та проактивно реагувати, ще до виникнення проблем. PCI DSS рекомендує впроваджувати метрики для безперервного моніторингу ключових контролів із метою впевнитись, що вони постійно працюють ефективно. Якщо метрика показує деградацію, це сигнал до

перегляду процесів або підсилення ресурсів. Крім того, програма має передбачати процес управління змінами у контексті змін стандартів: коли з'являються нові версії PCI DSS або оновлення SWIFT CSCF, відповідальні особи оперативно аналізують нові вимоги і коригують внутрішню програму. Так, перехід від PCI DSS v3.2.1 до v4.0 вимагав суттєвого оновлення ряду заходів, і програма відповідності повинна була заздалегідь врахувати ці зміни, запланувавши їх впровадження до моменту, коли вимоги стануть обов'язковими. Аналогічно, якщо SWIFT анонсує, що певна рекомендаційна вимога стане обов'язковою в наступному році (як це було, наприклад, із контролем 2.4A "Безпека потоків даних бек-офісу", який лишається рекомендаційним у 2025-му, але планується до переведення до категорії обов'язкових) - компанія проактивно готується, приділяючи увагу виконанню цієї вимоги вже зараз.

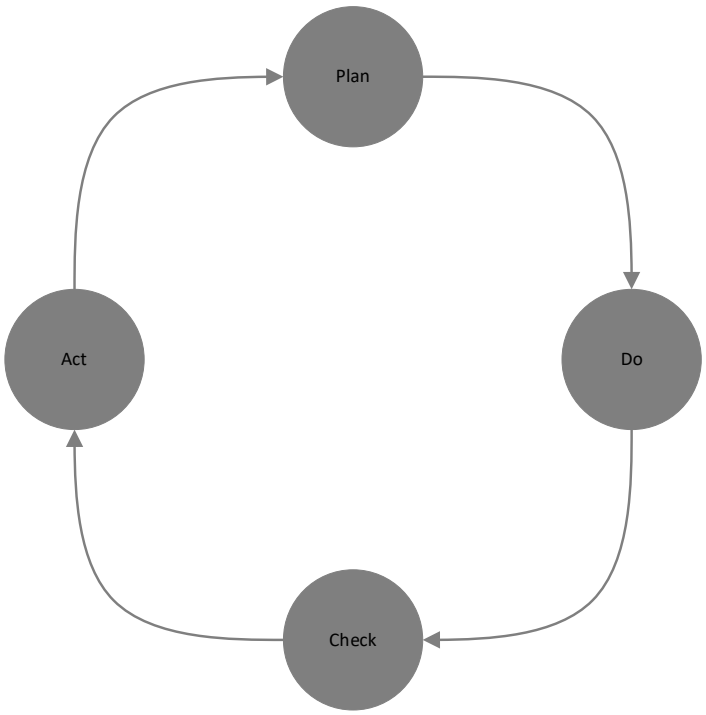

Рис. 2.1. Цикл PDCA

Оскільки обидва стандарти можуть бути впроваджені паралельно у компанії, доцільно об'єднати їх виконання в рамках єдиної програми відповідності, щоб оптимізувати ресурси та уникнути дублювання [22]. Багато

вимог перегукуються або доповнюють одна одну. Наприклад, вимоги PCI DSS щодо керування вразливостями (вимога 11) і SWIFT-принцип "Reduce Attack Surface and Vulnerabilities" фактично вимагають схожих процесів сканування і патч-менеджменту [1, с. 260; 2, с. 44]. Замість двох окремих процесів, компанія може мати одну централізовану процедуру управління вразливостями, яка забезпечує виконання вимог обох стандартів. Так само управління доступом: PCI DSS регламентує унікальні ідентифікатори та регулярний перегляд прав, SWIFT - контроль привілей і MFA. Це означає, що бажаним результатом є єдиний процес IAM з урахуванням вимог обох стандартів. У програмі відповідності варто здійснити співвідношення вимог - зіставлення PCI DSS та SWIFT CSCF, щоб виявити, де одна дія забезпечує відповідність обом стандартам. Наприклад, впровадження сегментації ізоляції критичних систем - виконує вимогу 1 стандарту PCI DSS і вимогу 1.1 стандарту SWIFT. На базі такого співвідношення програма може встановлювати універсальні заходи замість окремих для кожного стандарту. Це спрощує підтримку: одна команда та процес відповідає за виконання певної функції, звітуючи про її ефективність у розрізі одразу обох стандартів.

2.3 Організація аудиту, самооцінки та документального супроводу відповідності

Аудит інформаційної безпеки є ключовим механізмом перевірки того, наскільки ефективно компанія виконує вимоги стандартів PCI DSS та SWIFT CSCF [43]. Правильна організація аудитів (як зовнішніх, так і внутрішніх) і постійних самооцінок забезпечує виявлення слабких місць, контроль прогресу та надання впевненості керівництву і регуляторам у надійності захисту. Принцип "довіряй, але перевіряй" тут застосовується повною мірою: навіть якщо налагоджено усі процеси (BAU, програма відповідності), без регулярної незалежної перевірки важко гарантувати, що не виникли нові проблеми чи що персонал не відходить від встановлених процедур.

У контексті PCI DSS більшість великих фінансових установ зобов'язані щорічно проходити зовнішню оцінку відповідності із залученням сертифікованого аудитора - QSA. QSA проводить повноцінний аудит, перевіряючи всі вимоги стандарту, і за його результатами складає ROC. Компанія, яка підтвердила відповідність, отримує сертифікат або лист про відповідність PCI DSS, який може надаватися платіжним системам чи банкам-партнерам як доказ стану відповідності вимогам стандарту. Водночас для менших установ або окремих підрозділів можливі самооцінки за стандартом PCI DSS - заповнення SAQ. Такі анкети містять перелік питань по кожній вимозі PCI DSS, на які компанія відповідає самостійно, підтверджуючи або невідповідність, або наявність компенсуючих заходів. Багато компаній прагнуть проводити внутрішні перевірки з рівнем строгості, наближеним до роботи QSA, щоб уникнути помилок при інтерпретації вимог. Внутрішній аудит може скористатися чек-листами, підготовленими на основі офіційних тестових процедур PCI DSS v4.0.1, та незалежно зібрати необхідні докази виконання вимог.

Для SWIFT CSCF процедура оцінки реалізується через щорічну оцінку у спеціальному порталі KYC-SA. Усі користувачі SWIFT зобов'язані щорічно до 31 грудня подавати свою атестацію, підтверджуючи рівень виконання обов'язкових вимог CSCF [44]. Навіть якщо певні вимоги не виконані, компанія мусить прозоро заявити про це - невідповідності будуть видимі контрагентам і, за необхідності, регуляторам. Починаючи з 2021-2022 років SWIFT посилила вимоги до таких аудитів, запровадивши концепцію незалежної оцінки: згідно з IAF, кожна подана атестація повинна бути підтверджена незалежним аудитором. Відтепер самостійна декларація без незалежної перевірки вважається неповною/некоректною і прирівнюється до невідповідності. SWIFT дозволяє два підходи до незалежної оцінки: внутрішня та зовнішня. У будь-якому випадку аудитори мають бути компетентними і незалежними від команд, відповідальних за впровадження заходів, аби забезпечити об'єктивність. SWIFT навіть реалізував програму сертифікації для зовнішніх аудиторів - CSP Assessment Provider/Assessor, щоб компанії могли наймати кваліфікованих аудиторів.

Таким чином, організація аудиту відповідності SWIFT CSP тепер дуже схожа на PCI DSS: щороку проводиться незалежна перевірка всіх обов'язкових вимог SWIFT CSCF, результати якої документуються і затверджуються керівництвом перед поданням сертифікації. Згідно кращих галузевих практик, компанія може чергувати зовнішні та внутрішні аудити: наприклад, 1 раз на 2 - 3 роки залучати зовнішніх експертів, а в проміжні роки проводити оцінку силами внутрішнього аудиту, який має відповідну кваліфікацію. У багатьох випадках внутрішній аудит виступає гарантом успішного проходження зовнішнього аудиту: спочатку аудиторська команда детально перевіряє виконання всіх вимог, складає внутрішній звіт і рекомендації, керівництво компанії аналізує звіт та призначає відповідальних за виправлення знайдених невідповідностей, і тільки потім заповнюється та підтверджується у KYC-SA. Подібний дворівневий підхід внутрішній попередній аудит перед зовнішнім незалежним значно підвищує довіру до результатів і знижує ризик потрапити в ситуацію несформованої відповідності.

Для ефективності програми відповідності слід заздалегідь планувати графік аудитів і самооцінок. Зовнішні аудити PCI DSS, як правило, проводяться щорічно приблизно в однаковий період. Внутрішні самооцінки доцільно проводити на постійній основі - наприклад, щокварталу виконувати вибіркові перевірки декількох вимог. BAU-підхід у PCI DSS передбачає саме такі регулярні перегляди: стандарт рекомендує здійснювати періодичні огляди стану виконання вимог на всіх локаціях, щоб підтвердити, що політики дотримуються, конфігурації відповідають стандартам, паролі змінюються, журнали переглядаються тощо. Відповідальність за ці внутрішні перевірки може нести підрозділ внутрішнього аудиту або спеціаліст з підрозділу комплаєнсу. Результати кожної перевірки оформляються у вигляді звіту з переліком знайдених невідповідностей та рекомендаціями щодо виправлення. Важливо, щоби керівництво оперативно реагувало на такі проміжні звіти - виділяло ресурси на усунення невідповідностей, поки вони не стали проблемою.

На практиці корисно використовувати підхід аудитів фокусних тем: кожен квартал сфокусуватись на окремому напрямі. Таким чином, за 1 рік усі сфери

покриваються перевірками, і до часу зовнішнього аудиту компанія підходить з більшою впевненістю у своїй відповідності.

Не менш важливою частиною забезпечення відповідності є належний документальний супровід. Документація виконує дві функції: по-перше, слугує набором доказів для аудиторів і регуляторів, що вимоги виконуються, по-друге, допомагає самій компанії структурувати та контролювати процеси безпеки. До документального супроводу належать: політики, процедури, стандарти конфігурації, архітектурні схеми, журнали безпеки, звіти про сканування і тестування на проникнення, записи про навчання персоналу, акти або звіти внутрішніх перевірок, плани дій щодо усунення недоліків тощо. PCI DSS прямо вимагає наявності ряду документів, а SWIFT CSCF більше зосереджений на технічному виконанні вимог, але успішне проходження аудиту також передбачає наявність документальних підтверджень. Відповідно, компанія повинна налаштувати процес управління записами та доказами: усі релевантні документи систематизуються, оновлюються і зберігаються у центральному репозиторії.

Особливу увагу слід приділити веденню журналів та звітів. Журнали подій систем мають зберігатися достатній час: згідно PCI DSS не менше 1 року, з них не менше 3 місяців у оперативному доступі та регулярно аналізуватися [1, с. 252]. Для підтвердження цього процесу аудитор може запросити журнали за останні 3 місяці і звіти про їх щоденний перегляд. Якщо компанія використовує SIEM, то надаються вибіркові приклади подій та інцидентів і реакції на них. Вимога SWIFT про виявлення аномальної активності також потребує журналів або звітів систем моніторингу, що аномалії відстежуються і розслідуються. Не менш важливими є звіти про сканування на вразливості і тестувань на проникнення: необхідно архівувати результати кожного з них та будь-яких тестів безпеки SWIFT-інфраструктури. Ці звіти слугують доказом проактивного пошуку вразливостей. Компанія також має зберігати акти аналізу ризиків для тих процесів та заходів, де допускається гнучкість щодо виконання: наприклад, якщо за PCI DSS дозволено визначити інтервал виконання певної вимоги за умови проведення цільового аналізу ризиків - такий аналіз документується і надається під час аудиту.

Документування процесів включає і фіксацію інцидентів та реагування. Ведеться журнал інцидентів інформаційної безпеки, куди вносяться деталі кожного випадку, вжиті заходи реагування, час виявлення і вирішення. Наявність такого журналу є необхідним для виконання вимог PCI DSS 12.10 та SWIFT. Аудитор перевіряє, чи проводивсь аналіз після інциденту, чи оновлювались та/або корегувались процедури за результатами аналізу.

Необхідно забезпечити й актуалізацію документації. Документи повинні регулярно переглядатися та оновлюватися, щойно відбулися відповідні зміни у середовищі або вимогах. PCI DSS вимагає щорічного перегляду політики інформаційної безпеки та періодичного перегляду всіх інших безпекових політик - це має виконуватися автоматично в рамках підтримки програми відповідності: призначається відповідальний за кожну політику, хто переглядає її та вносить правки за підсумками аудитів, інцидентів або оновлення стандартів, те ж стосується і архітектурних схем та інвентаризаційних списків. Це завдання слід формалізувати як частину документального супроводу - відповідальний архітектор або менеджер ІБ звіряє перелік систем з реальністю, оновлює схеми, доводить розбіжності до відома команди. SWIFT CSCF також вимагає розуміння своєї архітектури: якщо компанія змінює тип підключення до SWIFT або додає нові компоненти, вона має актуалізувати атестацію відповідним чином. Звідси випливає практика: після кожної значної зміни в IT-ландшафті - проводити позачергову самооцінку і коригувати документацію та аналізувати область аудиту.

Частиною документального супроводу також є ведення реєстру відповідності - переліку всіх вимог стандартів із зазначенням статусу виконання кожної з них в компанії. Такий реєстр може бути таблицею або вестися в GRC-системі; він допомагає наочно бачити, які вимоги виконані, які в процесі, а які не застосовні. Такий реєстр використовується як для внутрішніх потреб, так і для зовнішніх - його можна надавати аудиторам для пришвидшення певних етапів аудиту.

Керівництву фінансової установи варто періодично отримувати консолідовану звітність щодо статусу відповідності - відповідальний за програму комплаєнсу з певною періодичністю готує звіт для правління або профільного

комітету. У звіті бажано висвітлювати щонайменше: загальний рівень відповідності, динаміку порівняно з попереднім періодом, ключові події, статус виконання плану заходів, ризики та проблеми. Такий підхід дозволяє керівництву приймати зважені рішення - наприклад, про додаткове фінансування на критичні поліпшення, або про перерозподіл ресурсів для закриття пробілів до дедлайну. Загальний принцип аудиту відображено на рисунку 2.2, але варто зазначити, що певні етапи в залежності від контексту ситуації можуть проводитись раніше чи пізніше, але еталонним можна вважати саме такий варіант.

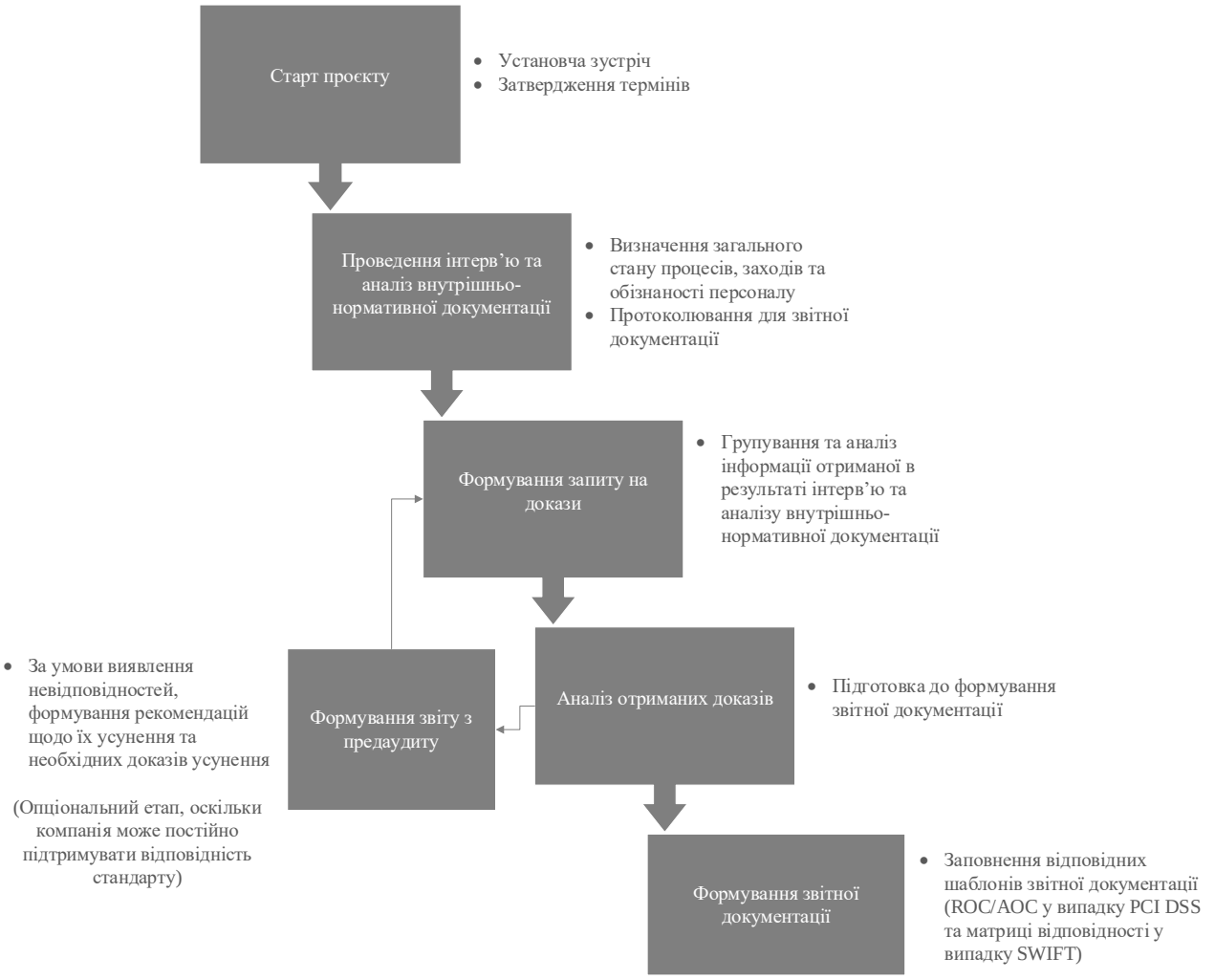

Рис. 2.2. Еталонна схема етапів проводження аудиту

Як підсумок, аудити та самооцінки тісно пов'язані з документальним супроводом, а регулярна самооцінка фактично є "міні-аудитом" власними силами. Зовнішній аудит, у свою чергу, спирається на надану документацію і

залишає по собі офіційний аудиторський звіт, який теж варто зберігати і враховувати. Грамотно організований процес аудиту і документування створює цикл постійної відповідності: після кожної перевірки коригуються документи і процеси, що готує компанію до наступної перевірки на вищому рівні готовності. Це втілення принципу безперервної відповідності.

2.4 Використання засобів автоматизації для постійного моніторингу та управління відповідністю

Сучасний масштаб IT-середовища та складність вимог безпеки роблять майже неможливим ефективне підтримання відповідності без залучення автоматизованих засобів. Автоматизація дозволяє цілодобово відстежувати стан заходів, оперативно виявляти відхилення та полегшувати управління численними завданнями комплаєнсу. Стандарти PCI DSS і SWIFT CSCF прямо або опосередковано заохочують використання технологічних рішень для моніторингу: багато вимог неможливо виконати вручну з необхідною частотою, тому впровадження спеціалізованих систем є фактично обов'язковим для безперервної відповідності.

Одним із ключових інструментів є SIEM. Вони автоматично збирають журнали подій з різноманітних джерел - серверів, мережевого обладнання, баз даних, додатків - і виконують кореляційний аналіз для виявлення підозрілих шаблонів або інцидентів. У контексті PCI DSS це дозволяє виконати вимогу 10 у ефективний спосіб: SIEM в режимі реального часу збирає журнали та виявляє аномалії [1, с. 236-259]. Для SWIFT-середовища SIEM чи аналогічні системи можуть відслідковувати специфічні події, як-от: спроби підключення до SWIFT-компонентів з неавторизованих системних компонентів, зміни в конфігурації Alliance Access, нестандартні послідовності трансакцій. Автоматизовані оповіщення спрямовуються відповідальним фахівцям негайно, що відповідає принципу швидкого виявлення та реагування. Без автоматизації подібний аналіз

був би надзвичайно трудомістким або взагалі не здійсненним на постійній основі.

До комплексу моніторингу належать IDS/IPS, а також спеціалізовані рішення для відстеження аномальної активності. IDS/IPS контролюють мережевий трафік і події на предмет відомих сигнатур атак чи поведінкових аномалій. Їх використання прямо або опосередковано відповідає вимогам PCI DSS та принципу SWIFT про виявлення аномалій. Інші інструменти, орієнтовані саме на SWIFT, можуть включати системи аналізу фінансових операцій: деякі банки впроваджують рішення, що аналізують потік SWIFT-повідомлень і попереджають про незвичні транзакції, доповнюючи цим обов'язкові контролі CSCF.

PCI DSS вимагає впровадження механізмів відслідковування змін, найпоширенішим варіантом реалізації яких є FIM. FIM-рішення автоматично порівнюють геші або стан файлів з еталонним і повідомляють про будь-які несанкціоновані зміни. У контексті постійної відповідності це дозволяє виявляти спроби компрометації або порушення конфігурацій негайно, а не під час наступного аудиту. Наприклад, якщо хтось вручну змінив конфігурацію міжмережевого екрану або відключив журналювання на сервері - система FIM згенерує оповіщення. Компанія може інтегрувати такі рішення і для SWIFT-середовища: контролювати цілісність критичних файлів додатка Alliance або серверної операційної системи, де він працює, слідкувати за тим, щоб параметри безпеки не змінювалися поза затвердженими змінами.

Автоматизоване управління конфігураціями допомагає проводити регулярний аналіз змін у конфігураціях: періодично система перевіряє, чи конфігурації систем відповідають встановленим конфігураційним еталонам. Це охоплює налаштування операційних систем, баз даних, мережевого обладнання. Якщо виявлено розбіжності, програма сигналізує про це командам ІБ для вжиття заходів.

Як зазначалося вище, управління вразливостями також має бути безперервним процесом. Сканери вразливостей (Qualys, Nessus, Rapid7 тощо)

можуть бути налаштовані на періодичне сканування всіх мережевих сегментів, які підпадають під PCI DSS та SWIFT. Вони автоматично генеруватимуть звіти про знайдені вразливості з їх критичністю. Сучасні системи також дозволяють інтегруватися з системами управління патчами: щойно виходить оновлення для закриття виявленої критичної уразливості, воно автоматично завантажується в систему розгортання (наприклад, WSUS, SCCM для Windows або аналогічні інструменти для Linux) і позначається "для якнайшвидшого застосування". Автоматизація тут мінімізує людський фактор - сервери оновлюються згідно із заданим графіком і політиками, а адміністраторам приходять лише звіти про успішність або помилки. Це суттєво сприяє безперервній відповідності вимогам SWIFT 2 та PCI DSS 6 і 11 [2, с. 44-64; 1, с. 134-160, 290-333].

У частині керування доступом автоматизація проявляється у впровадженні систем IAM та PAM. IAM-система централізує управління обліковими записами: всі створення, зміни та видалення користувачів, який включає необхідні затвердження і автоматичне призначення ролей. Це дозволяє гарантувати, що користувач отримує лише ті доступи, які передбачені його роллю, і не більше. У рамках PCI DSS це покриває вимоги 7 і 8, а в рамках SWIFT - 4 та 5 [1, с. 161-209; 2, с. 67-87]. PAM-рішення особливо актуальні для привілейованих доступів: вони зберігають адміністративні паролі в електронному сховищі, ведуть облік облікових даних адміністраторів, можуть періодично змінювати паролі. Таким чином, компанія може автоматично виконувати вимоги, які перевіряються на аудиті: надання списку усіх привілейованих акаунтів, підтвердження, що для доступу адміністратора обов'язково використовується MFA через PAM. Якщо хтось намагається обійти PAM, система це заблокує, зафіксує та оповістить безпеку.

GRC платформи - інструменти, які допомагають керувати програмою відповідності на високому рівні. У них можна оцифрувати всі вимоги стандартів, призначити відповідальних за кожну вимогу, прикріпити політики та докази, фіксувати результати оцінок. Це знімає навантаження з менеджера програми підтримки відповідності. Більш просунуті GRC інтегруються з вищезгаданими

технічними інструментами: вони можуть підтягувати дані зі сканерів, SIEM, тощо, і відображати показники відповідності. За допомогою таких платформ легше готуватися до аудитів - вся доказова база і статуси знаходяться в одному місці, і на запит аудитора можна швидко сформувати необхідні звіти [32]. Хоча стандарти PCI DSS та SWIFT CSCF не вимагають прямо використання GRC, їх наявність демонструє зрілість процесів управління відповідністю і значно підвищує надійність підтримання стандартів на постійній основі [19; 38].

Висновки до розділу 2

Підсумовуючи, інтеграція вимог PCI DSS та SWIFT CSCF у внутрішні процеси фінансової установи створює основу для побудови стійкої системи управління відповідністю. Формування програми відповідності, що охоплює політики, процедури, контрольні точки та відповідальних осіб, дозволяє забезпечити цілісне охоп лення вимог стандартів у щоденній діяльності. Автоматизовані засоби моніторингу та регулярна самооцінка перетворюють відповідність на постійно діючий процес, а не одноразову подію. У результаті відповідність стає невід’ємною частиною корпоративної культури безпеки, що відповідає принципам безперервної відповідності, закладеним у обох стандартах.

Розділ 3 ПРАКТИЧНА РЕАЛІЗАЦІЯ КОНТРОЛІВ ВІДПОВІДНОСТІ PCI DSS ТА SWIFT CSCF У ДІЯЛЬНОСТІ ФІНАНСОВОЇ УСТАНОВИ

У розділі представлено кейс-дослідження впровадження вимог стандартів PCI DSS та SWIFT CSCF у діяльність умовної фінансової установи. На основі аналізу поточного стану системи безпеки розглянуто виявлені невідповідності та обґрунтовано комплекс технічних і організаційних заходів для їх усунення [24]. Деталізовано впровадження контролів у ключових напрямках – доступ, журналювання, моніторинг, мережевий захист – з урахуванням особливостей кожного стандарту. Завершальним етапом є узгодження вимог PCI DSS та SWIFT CSCF у межах єдиної програми відповідності, а також оцінювання досягнутого рівня безпеки.

3.1 Аналіз поточного стану відповідності стандартам

У даному пункті буде розглянуто дослідження анонімізованої компанії (далі - Банк), яка одночасно підпадає під дію стандарту PCI DSS і вимог програми SWIFT CSP. Банк обробляє карткові дані та здійснює міжнародні перекази через мережу SWIFT. На момент аналізу поточного стану встановлено, що Банк формально проходив необхідні щорічні аудити, однак мав труднощі з підтриманням безперервної відповідності вимогам між аудитами. Зокрема, аудит виявив, що підхід був переважно реактивним і орієнтованим на разову сертифікацію, а не на постійне дотримання стандартів у повсякденній діяльності. Така ситуація типова: за даними досліджень, у світі менш ніж третина організацій здатні підтримувати повну відповідність PCI DSS на постійній основі, що пояснюється браком довгострокової стратегії безпеки та належної підтримки з боку керівництва [3; 33; 34]. Тому банк визначив необхідність переходу від разових заходів до системного процесу постійного контролю відповідності.

У контексті PCI DSS, була проведена оцінка поточного стану мережевої та інформаційної безпеки CDE банку. На момент аналізу банк уже мав базові засоби захисту: периметрові міжмережеві екрани, сегментовану мережу для CDE, засоби захисту від шкідливого програмного забезпечення на робочих станціях та серверах, тощо. Проте, багато вимог PCI DSS виконувалися не повністю або формально. Наприклад, було виявлено, що сегменти мережі, де обробляються дані карток, не достатньо ізольовані від загальної корпоративної мережі - деякі міжмережеві екрани мали недостатні обмеження у правилах доступу, наприклад відсутність явного правила "deny all" у кінці, що ставило під сумнів відповідність вимогам сегментації середовища (1.3.1 та 1.3.2) [1, с. 51; 1. с. 52]. Поза тим, деякі сервери та бази даних працювали на застарілих операційних системах або містили облікові записи з паролями за замовчуванням, що є порушенням вимог безпечної конфігурації (2.2.1 та 2.2.2) [1, с. 64; 1. с. 65]. Система журналювання подій і моніторингу була фрагментованою - журнали безпеки зберігалися локально на серверах і переглядалися адміністраторами лише епізодично. Це не відповідало вимогам PCI DSS щодо регулярного аналізу журналів (10.3.3) та створювало ризик пропустити інциденти [1, с. 245]. Не було впроваджено централізованого SIEM для кореляції подій, тому контроль за аномаліями був обмеженим. IDS також були відсутні в певних сегментах мережі або охоплювали не весь трафік, хоча стандарт PCI DSS вимагає застосування технологій для виявлення мережевих атак (11.5.1) [1, с. 283].

Кадрові та організаційні аспекти також мали недоліки. Аналіз показав, що не було чітко призначено відповідальних осіб за програму відповідності PCI DSS, а процес управління цією програмою не був інтегрований у повсякденну діяльність. Відповідно, багато заходів виконувалися лише перед черговим аудитом і не підтримувалися постійно. Наприклад, хоча політики безпеки були розроблені, персонал не був достатньо обізнаний з ними, що порушувало вимогу регулярного навчання з безпеки (12.6) [1, с. 309-311]. Перевірки співробітників на наявність судимостей чи інших ризик-факторів проводилися не для всіх, хоча стандарт прямо вимагає скринінгу персоналу перед прийомом на посаду з

доступом до карткових даних (12.8.3) [1, с. 318]. Отже, поточний стан відповідності PCI DSS можна було охарактеризувати як неповний: ключові заходи та процеси присутні, але їх ефективність і постійність реалізації недостатні.

Окрім карткових систем, банк експлуатує інфраструктуру для доступу до мережі SWIFT і тому підпадає під вимоги SWIFT CSCF. На момент аналізу банк щорічно проходив самооцінку та атестацію KYC-SA за програмою SWIFT CSP, підтверджуючи виконання обов’язкових вимог. Виявлено, що більшість обов’язкових вимог SWIFT були впроваджені, але деякі з них - частково. Наприклад, вимога 1.1 "Захист середовища SWIFT" вимагає суворого відокремлення безпечної зон - сегменту, де знаходяться сервери SWIFT - від загальної IT-мережі [2, с. 29]. У Банку було впроваджено сегментацію, але були знайдені зайві мережеві з’єднання між захищеною зоною SWIFT та іншими сегментами, що створювало потенційні уразливості. вимога 1.4 "Обмеження доступу до Інтернет" також не був цілком виконаний: сервери SWIFT не мали прямого доступу до Інтернет, але робочі станції операторів SWIFT могли виходити у зовнішню мережу, що суперечить рекомендаціям ізоляції критичних систем [2, с. 38].

Вимога 2.2 "Безпекові оновлення" встановлює необхідність своєчасного встановлення патчів безпеки [2, с. 46]. Під час аудиту було виявлено, що оновлення на серверах SWIFT встановлювались із затримками, інколи раз на квартал, замість оперативного застосування патчів для вразливостей, оцінених як "critical". Вимоги 2.7 "Сканування вразливостей" вимагає регулярного сканування систем на вразливості - це виконувалось лише раз на рік під час підготовки до сертифікації, що недостатньо для проактивної безпеки (необхідно хоча б щоквартал, як передбачено PCI DSS для карткових систем; SWIFT CSP також вимагає регулярних перевірок) [1, с. 266-270; 2, с. 46]. Вимога 6.4 "Журналювання та моніторинг" передбачає моніторинг безпекових подій у реальному часі та ведення журналів подій у захищеній зоні SWIFT. У банку журнали з додатків SWIFT (наприклад, з Alliance Access) збиралися, але їх аналіз

здійснювався вручну і несистематично, не в режимі реального часу та без оповіщень про інциденти - тобто вимога 6.4 формально порушено [2, с. 84]. Окремо було відзначено людський фактор: вимога 5.3A "Перевірка персоналу" носить рекомендаційний характер у CSCF, але є важливою практикою [2, с. 75]. Банк не проводив повноцінної процедури перевірки біографічних даних співробітників, залучених до роботи з системою SWIFT, що потенційно збільшувало ризики. Також вимога 7.2 "Навчання з питань безпеки та обізнаність" декларує проведення регулярних тренінгів зі спеціалізованої безпеки SWIFT, проте на момент аудиту в Банку проводилися лише загальні тренінги з інформаційної безпеки і не для всього залученого персоналу [2, с. 90].

Таким чином, аналіз поточного стану виявив як спільні невідповідності стандартам, так і специфічні невідповідності по кожному з них. Загальний процес аналізу та його результати відображено на рисунку 3.1. Спільним було те, що організації бракувало інтегрованої програми управління безпекою та відповідністю: заходи здійснювалися фрагментарно, механізми відслідковування не працювали постійно, а частина вимог виконувалась лише напередодні аудитів. Це підтверджує необхідність переходу до проактивної моделі безперервної відповідності, коли вимоги PCI DSS та SWIFT CSCF інтегровані в бізнес-процеси банку на постійній основі. На основі отриманих результатів було розпочато етап аналізу невідповідностей та розроблення плану коригувальних заходів.

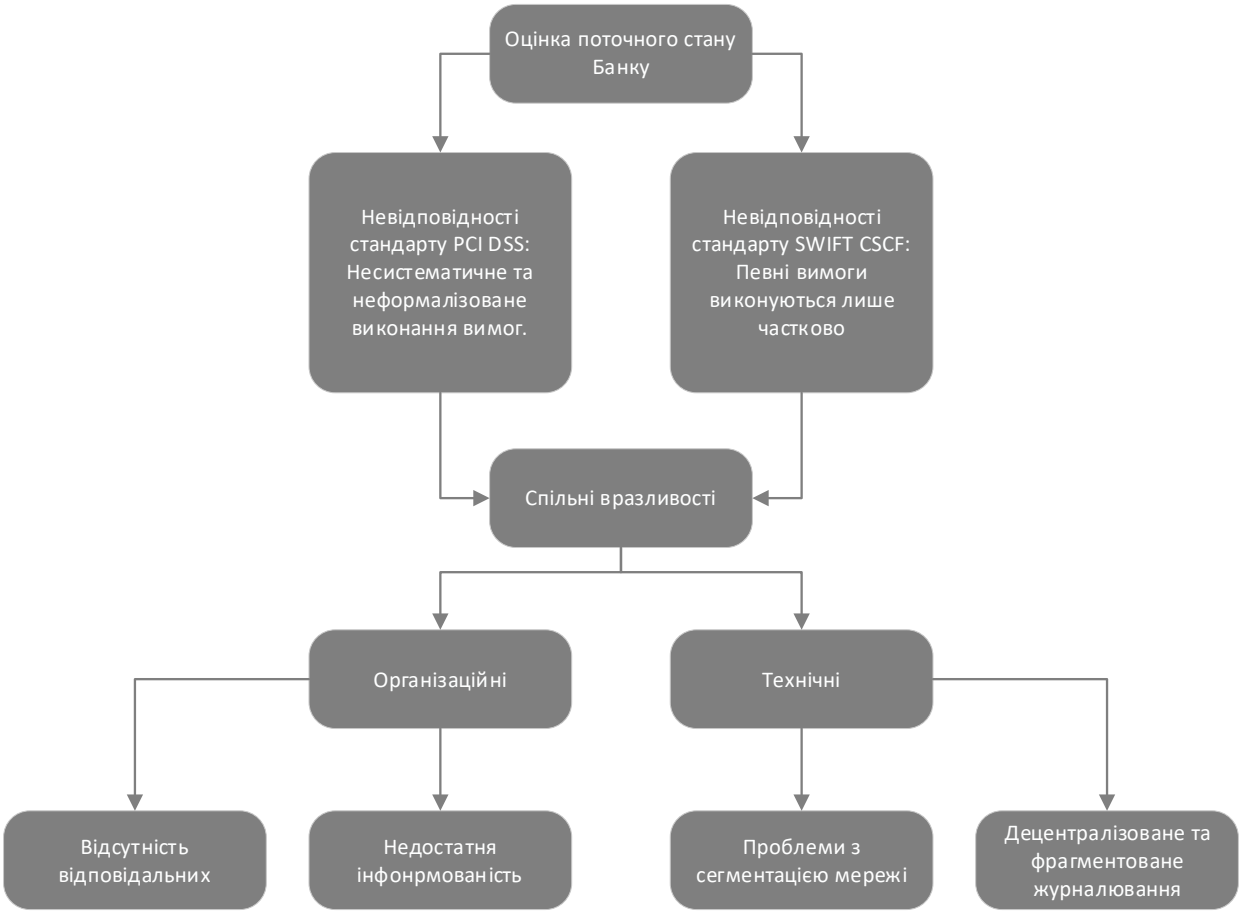

Рис. 3.1. Класифікація виявлених спільних вразливостей за результатами оцінки відповідності стандартам PCI DSS та SWIFT CSCF

3.2 Ідентифікація невідповідностей та планування коригувальних заходів

На цьому етапі проведено детальний попередній аналіз - зіставлення фактичного стану інформаційної безпеки банку з вимогами стандартів PCI DSS та SWIFT CSCF. Усі виявлені невідповідності були задокументовані. Сукупно вищеописані проблеми означали відсутність належних процесів керування мережевим обладнанням, адміністрування серверів та робочих станцій, виявлення інцидентів та реагування, управління кадрами та підвищення обізнаності персоналу.

Хоча в банку існували політики інформаційної безпеки, ряд процедур не були формалізовані. Не було розроблено документованої процедури реагування

на інциденти, яка б відповідала вимогам PCI DSS 12.10.1 і SWIFT 7.1 [1, с. 327; 2, с. 88]. Персонал не був чітко обізнаний, які кроки необхідно виконати у випадку підозри на компрометацію, не проводилось навчальних за сценаріями кібератак. Також були відсутні метрики ефективності та регулярна звітність щодо ефективності заходів безпеки, що перешкоджало об'єктивному контролю керівництвом [1, с. 19].

Після ідентифікації кожної з невідповідностей вище керівництво Банку провело оцінку ризиків, та визначило пріоритети коригувальних заходів. Вищезазначені проблеми було визнано критичними, тож їх усунення було заплановано в першу чергу. Менш критичні відхилення (наприклад, незначні недоліки у веденні документації) планувалося виправити на наступних етапах. Важливим принципом планування стало об'єднання вимог двох стандартів там, де вони перетинаються. Команда з безпеки сформувала єдиний план покращення стану відповідності, в якому заходи згруповані за напрямками безпеки, а не за окремими стандартами. Такий підхід дозволяє одним заходом закривати вимоги одразу двох стандартів. Наприклад, впровадження SIEM вирішить одночасно невідповідність PCI DSS (10.3.3) і SWIFT (6.4) [1, с. 245; 2, с. 84]. Пріоритетними було визначено технічні заходи з високим ефектом зниження ризику. Зокрема, план першочергових дій включав: посилення мережевої безпеки (перегляд логіки сегментації та правил на міжмережевих екранах, впровадження механізмів IDS/IPS), впровадження систем FIM та SIEM для постійного відслідковування, закриття вразливостей шляхом оновлення програмного забезпечення та сканування на вразливості, впровадження MFA для будь-якого привілейованого доступу. Одночасно, було заплановано організаційні заходи: призначення персоналу, відповідального за стан відповідності стандартам PCI DSS та SWIFT, перегляд програми навчання співробітників, оновлення та актуалізація політик безпеки. Для кожного заходу визначені відповідальні особи, ресурси та терміни виконання. Формат картки ризиків Банку відображено на рисунку 3.2.

Вплив на цільові показники (Наслідки)

Ймовірність реалізації	Можна знехтувати	Невеликий	Помірний	Значний	Суттєвий
Дуже ймовірно	Нижче середнього	Середня	Вище середнього	Висока	Висока
Ймовірно	Низька	Нижче середнього	Середня	Вище середнього	Висока
Можливо	Низька	Нижче середнього	Середня	Вище середнього	Вище середнього
Малоймовірно	Низька	Нижче середнього	Нижче середнього	Середня	Вище середнього
Дуже малоймовірно	Низька	Низька	Нижче середнього	Середня	Середня

Рис. 3.2. Картка ризиків Банку

Таким чином, за результатами попереднього аудиту Банк сформував цілісну програму підвищення та постійної підтримки безпеки та стану відповідності.

3.3 Впровадження технічних і організаційних заходів відповідно до вимог PCI DSS

Першим пріоритетом стало посилення мережевого захисту. У Банку реалізовано повну сегментацію CDE від офісної мережі: налаштовано окремі VLAN і міжмережеві екрани, дозволено лише мінімально необхідний трафік. Зокрема, NGFW було налаштовано таким чином, щоб забороняти будь-який необов’язковий доступ із загальної IT-мережі до сегменту CDE. Оновлено мережеві діаграми та правила доступу (ACL) у відповідності до всіх підвимог 1.2 [1, с. 42-50]. Оновлені правила маршрутизації передбачають, що тільки визначені системи можуть з’єднуватися з серверами баз даних які зберігають карткові дані, і лише на необхідних портах. Усі прямі підключення до мережі Інтернет із сегменту CDE заблоковані. Ці заходи одночасно відповідають і принципам

SWIFT щодо захисту критичних систем від загального IT-середовища. Додатково Банк впровадив та налаштував окремий WAF перед веб-застосунками, які обробляють карткові дані. WAF перевіряє весь трафік на предмет веб-атак (SQL-ін’єкцій, XSS тощо) і блокує підозрілі запити. Такий WAF є прикладом технічного рішення, яке дозволяє автоматично виявляти й запобігати веб-атакам на публічні застосунки, що допомагає виконати вимоги 6.4.2 та 6.4.3 [1, с. 152-153].

Для виконання вимог розділу 11 Банк впровадив декілька ключових систем. По-перше, було розгорнуто IDS/IPS. Обрано рішення на базі Suricata із правил мережевого трафіку Emerging Threats; його налаштовано моніторити весь трафік на периметрі і між сегментами CDE [4]. IDS працює в режимі реального часу: при спрацюванні правила відповідне оповіщення надсилається до SOC. Таким чином виконується вимога 11.5.1 [1, с. 283].

По-друге, запроваджено системи FIM на критичних серверах. Для цього Банк використав рішення OSSEC на серверах баз даних та додатків процесингу. OSSEC відстежує зміни у критичних файлах (системні файли конфігурації, виконувані файли застосунків, скрипти обробки платежів), порівнюючи контрольні суми з еталонними. У випадку несанкціонованої модифікації чи додавання файлу - система генерує оповіщення. Це забезпечує відповідність вимозі 11.5.2 [1, с. 286].

Обидва рішення - IDS і FIM - було інтегровано в загальну систему оповіщення, щоб відповідальні фахівці з безпеки одразу отримували повідомлення (електронною поштою та в консоль SIEM) про інциденти, такі як спроби мережевих атак чи зміни файлів.

Відповідно до вимоги 10, Банк реалізував централізоване журналювання всіх подій безпеки та ключових операцій. Встановлено систему SIEM Splunk Enterprise Security, куди в режимі реального часу надходять журнали від різних системних компонентів: міжмережевих екранів, IDS/IPS, серверів баз даних, додатків, OSSEC, механізмів захисту від шкідливого програмного забезпечення тощо. Усі ці події автоматично корелюються та аналізуються в режимі реального

часу на предмет аномалій. Такий підхід дозволяє виконати вимогу 10.4 [1, с. 247-251]. Також було впроваджено процедуру щоденного перегляду інцидентів у SIEM аналітиками безпеки. Таким чином, Банк перейшов від ручного і вибіркового перегляду журналів до автоматизованого безперервного моніторингу, що істотно підвищує шанси раннього виявлення компрометації.

Для виконання вимог 11.3 Банк впровадив регулярні процеси перевірки своїх систем [1, с. 266-273]. По-перше, налагоджено процес сканування на вразливості: придбано рішення QualysGuard Vulnerability Management, яким охоплено усі системи в CDE. Встановлено розклад автоматичного внутрішнього сканування - щомісячно, що є частішим від мінімуму, який вимагається стандартом - щоквартально, а також негайно після кожних значних змін [1, с. 266].

Зовнішнє сканування проводиться щоквартально незалежним ASV. Усі виявлені вразливості заносяться до системи відслідковування та призначаються відповідальним адміністраторам системних компонентів для усунення. Встановлено чіткі SLA: критичні вразливості (CVSS вище 7.0) мають бути пропатчені або іншим чином виправлені протягом 1-2 тижнів. Таким чином, Банк тепер проактивно виявляє слабкі місця та виконує вимогу 6.3.1 [1, с. 143].

По-друге, організовано щорічне тестування на проникнення сторонньою компанією, яка має організаційну незалежність від IT-відділу Банку. Це відповідає вимозі 11.4.3 [1, с. 277]. У межах тестування на проникнення в тому числі перевіряється ефективність впроваджених заходів (IDS, WAF, сегментація), і спроби їх обходу. Результати тестування аналізуються керівництвом та використовуються для подальшого вдосконалення захисту.

Для набуття відповідності вимогам 7 та 8 Банк здійснив організаційно-технічні зміни у цій сфері. Впроваджено принцип найменших привілеїв: проаналізовано ролі усіх користувачів систем CDE та видалено надлишкові права. Для централізованого управління обліковими записами використано Active Directory - усі користувачі системних компонентів у CDE тепер автентифікуються за допомогою доменних облікових записів AD, що дозволяє

застосувати єдину парольну політику та відстежувати автентифікацію. Парольна політика містить наступні вимоги: мінімум 12 символів, великі, малі літери, цифри, спеціальні символи (8.3.6), строк дії паролю - не більше 90 днів (8.3.9) [1, с. 190; 1, с. 193]. Відповідно до вимог 8.6, паролі зберігаються в системах тільки в гешованому вигляді з використанням стійкої криптографії (AD використовує геші, такі як NTLMv2). Крім того, для будь-якого адміністративного та віддаленого доступу впроваджено MFA - адміністратори при підключенні до серверів повинні окрім паролю підтвердити особу через апаратний токен (8.4-8.5) [1, с. 198-204]. В банку обрано рішення на базі YubiKey (апаратні токени) - другий фактор тепер обов’язковий для встановлення адміністративного або віддаленого з'єднання. Це суттєво підвищує безпеку облікових записів та в тому числі дозволяє забезпечити відповідність вимозі SWIFT 4.2 [2, с. 69].

Скасовано практику використання спільних облікових записів: кожен адміністратор має особистий персоналізований обліковий запис, а доступ до критичних систем здійснюється через механізми регулювання привілейованого доступу - через Jump Server, що фіксує сесію. Також посилено контроль за наданням і відкликанням доступів: HR тепер інформують IT-безпеку про звільнення чи переведення співробітників, і доступ відповідно оперативно скасовується (7.2.4) [1, с. 168]. Запроваджено регулярний щоквартальний перегляд актуальності прав доступу - керівники підрозділів отримують список користувачів зі своїми системами і підтверджують або коригують рівні доступу (7.2.4, 8.2.6) [1, с. 168; 1, с. 183].

У рамках виконання вимоги 5, банк уніфікував та централізував механізми захисту від шкідливого програмного забезпечення [1, с. 119-133]. Раніше використовувались різні розрізнені рішення, тепер впроваджено корпоративну платформу захисту кінцевих точок на базі рішення від Symantec. Антивірусне програмне забезпечення встановлено на всіх серверах і робочих станціях в межах CDE. Налаштовано автоматичне щоденне оновлення сигнатур і регулярне сканування. Адміністративна консоль дозволяє відстежувати стан захищеності системних компонентів, отримувати оповіщення про виявлення шкідливого

програмного забезпечення та формувати звіти. Антивірусне рішення інтегровано із SIEM для кореляції журналів подій та додаткового аналізу. Крім традиційного антивірусу, Банк впровадив механізми EDR у Symantec, що забезпечує проактивне виявлення підозрілої поведінки на системних компонентах. Ці заходи задовольняють не лише вимоги стандарту PCI DSS, але й контроль SWIFT 6.1 "Захист від шкідливого програмного забезпечення" - який визначає, що на всіх критичних системних компонентах повинно бути встановлене антивірусне програмне забезпечення з актуальними сигнатурами.

Значна увага була приділена виконанню вимог 3 та 4 стандарту PCI DSS, які стосуються безпеки карткових даних. Банк переглянув процеси зберігання і шифрування даних. Установлено наступні правила: PAN не має відображатись у відкритому вигляді в адміністративних інтерфейсах - у випадках, де це має задокументовану бізнес-необхідність реалізовано маскування, яке робить видимим лише перші 6 і останні 4 цифри. Якщо виникає потреба у повному PAN, це може зробити лише визначене коло осіб через спеціальний запит, і такий доступ окремо фіксується. Карткові дані в базах даних зашифровані із застосуванням алгоритму AES-256; керування ключами здійснюється відповідно до вимоги 3.6 - ключі шифрування зберігаються у HSM і ніколи не беруть участь в процесах шифрування карткових даних у відкритому вигляді [1, с. 96-101]. Впроваджено дворівневу систему ключів (ключі шифрування даних захищені майстер-ключами HSM), регулярну ротацію ключів (3.6.1) [1, с. 96]. Для передачі карткових даних використовується лише шифрування за сучасними протоколами: увесь трафік між компонентами CDE та зовнішніми сервісами проходить через TLS 1.2+ з використанням стійкої криптографії (4.2) [1, с. 113-118]. Також задокументовано заборону пересилати PAN електронною поштою чи месенджерами у відкритому вигляді - впроваджено відповідну політику та технології DLP для контролю вихідного трафіку: якщо система DLP виявляє шаблон, схожий на номер картки в електронному листі, вона блокує таке повідомлення для подальшого розслідування. Ці дії значно знижують ризик

витоку карткових даних і забезпечують відповідність вимогам PCI DSS (4.2.2) [1, с. 118].

Технічні рішення мають доповнюватися процесами - це один із ключових принципів PCI DSS, який акцентує на інтеграції вимог безпеки до BAU процесів. Банк здійснив ряд організаційних змін: призначено персонал, відповідальний за програму відповідності PCI DSS та SWIFT. Йому делеговано повноваження контролювати аспекти відповідності та регулярно звітувати перед вищим керівництвом. Розроблено внутрішній документ, схвалений правлінням, який окреслює цілі програми відповідності, метрики ефективності і відповідальність учасників. Так, встановлено KPI: час реагування на інцидент, відсоток вчасно усунених вразливостей, охоплення навчанням співробітників тощо. Ці метрики постійно відстежуються та аналізуються, а результати щоквартально представляються на IT-комітеті Банку. Запроваджено регулярні операційні процедури: щотижневі зустрічі команди безпеки з обговорення виконання плану, щорічна оцінка ризиків, щоквартальні внутрішні вибіркові аудити вимог - внутрішній аудитор раз на квартал перевіряє декілька вимог PCI DSS вибірково, щоб впевнитися, що вони належно виконуються після проходження основного аудиту.

Таким чином, Банк створив систему самоперевірки, яка раніше була відсутня. Аналогічно, для SWIFT-контролів заплановано щороку залучати незалежного аудитора для перевірки виконання обов’язкових контролів CSP, навіть якщо SWIFT не вимагає зовнішнього щорічного аудиту, враховуючи що для певних типів архітектур оцінка може бути внутрішньою. Такий підхід - регулярно перевіряти впроваджені заходи та процеси - відповідає очікуванням SWIFT CSCF, де наголошується на постійній готовності підтвердити відповідність протягом року, а не лише одноразово під час планового аудиту.

Важливо, що тепер процес підтримання відповідності став безперервним циклом: автоматизовані засоби моніторингу працюють цілодобово, персонал чітко розуміє зону відповідальності, керівництво залучене через метрики і звіти. Це істотно відрізняється від попереднього стану "підготуватися до аудиту раз на рік". Вимоги PCI DSS інтегровані у BAU. Зіставлення впроваджених

контрзаходів та вразливостей на усунення яких вони спрямовані відображено в таблиці 3.1.

Таблиця 3.1

Зіставлення впроваджених контрзаходів і вразливостей, які вони усувають

Контрзахід	**Вразливість, на яку спрямовано**
Сегментація CDE, VLAN, оновлені ACL	Не ізольованість CDE. Доступ із офісної мережі
NGFW з політикою "deny all"	Відсутність чіткої фільтрації трафіку, необмежений доступ до CDE
Встановлення WAF перед веб-застосунками	Вразливість до веб-атак (SQL injection, XSS тощо)
IDS/IPS Suricata з інтеграцією до SOC	Відсутність виявлення атак у реальному часі (PCI DSS 11.5.1)
FIM (OSSEC) на критичних серверах	Несанкціоновані зміни у системних і конфігураційних файлах (PCI DSS 11.5.2)
SIEM Splunk Enterprise Security	Фрагментоване журналювання. Відсутність кореляції подій та реального часу аналізу
Сканування вразливостей (QualysGuard VM)	Відсутність регулярного та проактивного виявлення технічних вразливостей (6.3.1)
Щорічне незалежне тестування на проникнення	Відсутність тестування на ефективність впроваджених заходів (PCI DSS 11.4.3)
Аудит привілеїв та принцип найменших прав	Надлишкові повноваження користувачів. Порушення принципу "need to know" (7.1, 8.2)
MFA з використанням апаратних токенів YubiKey	Ненадійна автентифікація при адміністративному та віддаленому доступі (PCI 8.4–8.5)
Централізована автентифікація через Active Directory	Відсутність уніфікованої політики доступу. Слабка керованість обліковими записами
Антивірусна платформа Symantec + EDR	Ризик зараження шкідливим ПЗ; неузгоджені захисні засоби на різних вузлах (SWIFT 6.1)
Шифрування карткових даних (AES-256) з керуванням ключами через HSM	Зберігання PAN у відкритому вигляді; відсутність захисту шифруванням (PCI DSS 3.6)
Маскування PAN у системах перегляду	Незахищене відображення повного PAN в інтерфейсах
TLS 1.2+ для передавання, DLP для виявлення витоку PAN	Ризик витоку карткових даних через незашифровані канали або електронну пошту (4.2.2)
Призначення відповідальних осіб за відповідність	Відсутність контролю за виконанням вимог та звітності
Щоквартальні внутрішні аудити вибіркових вимог	Відсутність перевірок між основними аудитами
Впровадження KPI, метрик, щоквартального звітування	Відсутність участі керівництва та оцінки ефективності заходів
Щоквартальний перегляд актуальності прав доступу	Несвоєчасне відкликання або корекція доступів після змін у персоналі (7.2.4)

Отже, після впровадження зазначених технічних та організаційних заходів, Банк досяг відповідності вимогам PCI DSS. Карткові дані наразі захищені на всіх рівнях: від мережевого периметру до програм та даних, а процеси менеджменту безпеки перебувають під постійним контролем.

3.4 Реалізація контролів безпеки згідно з вимогами SWIFT CSCF

Паралельно із заходами, спрямованими на набуття відповідності стандарту PCI DSS, банк здійснив впровадження заходів для набуття відповідності SWIFT CSCF. Оскільки частина рішень з PCI DSS водночас забезпечує відповідність вимогам SWIFT, акцент було зроблено на специфічних для SWIFT аспектах та додаткових кроках, необхідно було впровадити в середовищі SWIFT.

Відповідно до вимоги 1.1 CSCF банк створив чітко визначене ізольоване середовище для своїх компонентів SWIFT [2, с. 29]. Усі системні компоненти, які забезпечують програмно-апаратний комплекс SWIFT (Alliance Access, SWIFTNet Link, API-концентратори тощо), були поміщені в окрему мережеву зону з відповідним рівнем захисту. Ця зона фізично та логічно відокремлена від інших мереж та систем Банку: підключення до внутрішньої мережі проходять через визначені міжмережеві екрани. Реалізовано принцип бастіону: для доступу адміністратора в безпечну зону SWIFT використовується проміжний сервер з обов'язковою MFA, а прямий доступ заблоковано. Такі заходи гарантують, що навіть якщо корпоративна мережа буде скомпрометована, зловмисник не зможе проникнути до середовища SWIFT.

Вимога 1.4 "Обмеження доступу до Інтернет" також є повністю виконаною - сервери SWIFT не мають жодного виходу в Інтернет; усі необхідні оновлення чи обмін даними здійснюються через проміжні вузли в DMZ [2, с. 38]. Робочі станції операторів SWIFT також налаштовано відповідним чином: тепер для їх роботи в SWIFTAlliance введено окремі тонкі клієнти, на яких заблоковано доступ до використання браузеру та електронної пошти, щоб зменшити ризик зараження шкідливим програмним забезпеченням.

SWIFT CSCF висуває вимоги до керування обліковими записами в системах SWIFT. Банк впровадив політики, які відповідають вимогам 5 [2, с. 71-78]. По-перше, всі користувачі SWIFT тепер мають персоналізовані облікові записи з мінімально необхідними привілеями (5.1) [2, с. 71].

Ролі в програмному забезпеченні Alliance Access періодично переглядаються: в результаті оператори, що лише відправляють платежі, не мають доступу до адміністративних функцій або до змін конфігурації. Парольна політика для цих облікових записів відповідає вимозі 4.1: встановлено механізми, які забезпечують обмеження мінімальної складності паролів, ротацію в щонайменше 90 днів, заборону на повторне використання останніх 4 паролів тощо. Особливо критичні облікові записи захищені додатково: їх паролі зберігаються в зашифрованому вигляді в окремому сховищі з обмеженим доступом - виконується вимога 5.4 [2, с. 77].

По-друге, реалізовано MFA для всіх користувачів з доступом до SWIFT. Це виконання вимоги 4.2: тепер при вході до інтерфейсу SWIFT операторам окрім пароля потрібно використати апаратний токен. Як згадувалось раніше, Банк обрав рішення у вигляді USB-токенів з сертифікатами (PKI-токени) для кожного оператора SWIFT. Ці токени виконують роль другого фактора: користувач вводить PIN від токена, який розблоковує цифровий сертифікат, необхідний для доступу.

З огляду на використання апаратних токенів, Банк також приділив увагу вимозі 5.2 [2, с. 73]. Введено процедуру, за якою всі токени операторів SWIFT реєструються у спеціальному журналі, видаються під розпис, а у випадку звільнення співробітника токен негайно відключається. Сертифікати на токенах випущені внутрішнім центром сертифікації банку з обмеженим строком дії, після чого потребують перевипуску - таким чином, якщо токен буде загублено, його дія автоматично припиниться через відносно короткий час. Належна поведінка та безпечне збереження токенів також описані внутрішньо-нормативною документацією Банку. Адміністратори проводять перевірку токенів кожні

півроку: чи всі видані токени присутні та використовуються тільки персоналом, для якого вони призначені.

Вимога 2.2 і 2.3 зобов'язують банк підтримувати усі системні компоненти SWIFT актуальними і захищеними [2, с. 46; 2, с. 48]. Для цього розроблено стандарти конфігурації для серверів SWIFT-інфраструктури: відключено всі непотрібні служби та порти, увімкнено шифрування дисків, налаштовано політики аудиту у операційних системах. Патч-менеджмент тепер відбувається за чітким графіком: оновлення операційних систем встановлюються щомісячно під час визначеного вікна технічного обслуговування. Оновлення самого програмного забезпечення застосовуються негайно після їх виходу та проходження тестування у окремому тестовому середовищі. Таким чином, середовище SWIFT постійно отримує останні виправлення безпеки, які усувають вразливості, що дозволяє встановити відповідність вимозі 2.2 [2, с. 46]. Для вимоги 2.3 Банк також користується рекомендаціями від вендорів і галузевими стандартами CIS Benchmarks. Регулярні внутрішні аудити конфігурацій (використовуючи скрипти перевірки) гарантують, що жоден сервер SWIFT не відхиляється від затвердженої безпечної конфігурації.

Вимога 6.2 є унікальною для SWIFT - вона вимагає забезпечити, щоб програмні компоненти SWIFT не були непомітно модифіковані, що схоже на вимогу 11.5.2 стандарту PCI DSS, але ключова різниця полягає у тому, що PCI DSS концентрується на цілісності файлів та конфігурацій, у той час як вимога SWIFT спрямована на цілісність програмного забезпечення [2, с. 81; 1, с. 286]. Тут Банк застосував кілька підходів. По-перше, використано можливості самого SWIFT Alliance Access: ця платформа надає контрольні суми своїх модулів; при кожному старті системи перевіряється цілісність ключових файлів. Адміністратор безпеки SWIFT щомісяця переглядає журнали Alliance Access на предмет повідомлень про порушення цілісності. По-друге, FIM-система OSSEC, впроваджена в контексті виконання вимог PCI DSS, також налаштована на SWIFT-додатки: вона відстежує каталоги встановлення SWIFT та пов'язаних компонентів. Усі геші інсталяційних файлів програмного забезпечення SWIFT

постійно відслідковуються; будь-яка зміна одразу генерує оповіщення. Крім того, заходи, спрямовані на виконання вимоги 6.3 реалізовано шляхом використання засобів СУБД: бази даних SWIFT налаштовано на ведення журналів трансакцій і контроль цілісності записів [2, с. 83]. Регулярно проводиться перевірка цілісності резервних копій бази, щоб впевнитися у відсутності несанкціонованих змін історії подій.

Значну увагу приділено виконанню вимоги 6.4, яка зобов’язує Банк збирати безпекові журнали з середовища SWIFT та аналізувати їх у режимі реального часу [2, с. 84]. Для цього налаштовано, щоб усі події з серверів SWIFT централізовано надходили в згадану систему SIEM (Splunk). У SIEM було створено окрему панель моніторингу "SWIFT Security", де відображаються спроби неправильного входу до системи, зміни конфігурацій, відключення сервісів, підозрілі трансакції. Події безпеки у середовищі SWIFT моніторяться та журналюються в режимі реального часу, а також визначено, що аналітики SOC мають реагувати на них негайно, як і на інші інциденти. Таким чином, вимога 6.4 вважається виконаною - банк має централізоване журналювання та проактивний моніторинг та аналіз подій середовища SWIFT.

Хоча вимога 6.5 у CSCF позначена як рекомендаційна, Банк вирішив її впровадити [2, с. 86]. Розгорнуту в контексті набуття відповідності вимогам стандарту PCI DSS IDS/IPS Suricata було інтегровано також і для трафіку, який стосується середовища SWIFT. Наприклад, виділено окремий сенсор IDS на сегменті мережі, де розташовані сервери SWIFT, який аналізує трафік між системою SWIFT та внутрішніми бек-офісними системами, а також трафік до шлюзів SWIFT. Це дозволяє виявити аномальну активність - наприклад, якщо з бек-офісного сервера раптом почнеться сканування сегменту SWIFT, або якщо всередині захищеної зони з’явиться трафік, схожий на шкідливе програмне забезпечення (як було у випадку відомого інциденту з банком Бангладеш, де шкідливе програмне зобачення перехоплювало SWIFT-повідомлення). Отримані попередження IDS обробляються за тим же процесом спеціалістами SOC. Таким

чином, навіть рекомендаційна вимога 6.5 фактично виконується, що підвищує загальну безпеку.

Вимога 3.1 SWIFT CSCF вимагає забезпечити фізичний захист середовища SWIFT [2, с. 65]. Банк провів додаткові заходи в своїх дата-центрах: стійки із серверами SWIFT обладнані замками, доступ до них мають лише авторизовані інженери. Системи відеоспостереження (CCTV) покривають всі точки входу до приміщень з обладнанням SWIFT, записи зберігаються протягом щонайменше 3 місяців. Журнали відвідування дата-центру перевіряються службою безпеки - тільки авторизований персонал має доступ до обладнання SWIFT.

У межах виконання вимоги 2.9 Банк впровадив додаткові процедури для відстеження аномалій у платіжних повідомленнях SWIFT [2, с. 60]. Хоча технічно SWIFTNet забезпечує передачу повідомлень, необхідно мати й бізнес-рівень контролю - щоб виявити, наприклад, шахрайські перекази. Банк налаштував щоденну звірку відправлених платежів: виділений незалежний підрозділ кожного ранку перевіряє звіт з усіма SWIFT-повідомленнями за попередню добу та співставляє з внутрішніми записами про перекази. У випадку виявлення невідповідності інцидент негайно ескалюється для розслідування. Також було реалізовано ліміти на рівні Alliance Access: повідомлення на суму понад визначений поріг тепер потребують додаткового підтвердження від керівництва.

Відповідно до вимоги 2.8, банк переглянув свої відносини з TPSP, що мають доступ або впливають на середовище SWIFT [2, с. 58]. Було складено повний перелік таких третіх сторін: наприклад, зовнішній партнер, що обслуговує програмне забезпечення SWIFT, підрядник з адміністрування баз даних, провайдер каналів зв’язку. Із кожним із них оновлено договірні зобов’язання: додано положення про необхідність відповідності мінімальним вимогам безпеки, про проходження щорічної оцінки відповідності, негайне повідомлення Банку у випадку виникнення чи підозри інцидентів, що можуть вплинути на SWIFT. Також вимагається, щоб TPSP дотримувалися контролів CSP. Банк запросив у TPSP їх атестації безпеки для впевненості у їх рівні захисту.

Таким чином, ризики, пов’язані зі сторонніми компаніями, було взято під контроль.

Щодо бек-офісних систем: вимога 2.4, яка є рекомендаційною, але після виходу CSCF v2026 стане обов'язковою, вимагає захистити "першу ланку" бек-офісу, що з’єднується зі SWIFT [2, с. 50; 2, с. 128]. Банк, усвідомлюючи майбутню обов’язковість цього контролю, вирішив ідентифікувати такі системи - наприклад, АБС (автоматизована банківська система), яка передає платежі у SWIFT, та ERP-систему для міжнародних виплат. Було впроваджено додаткові заходи для їх захисту: між цими системами і SWIFT-зоною було встановлено окремий шлюз з контролем протоколів, усі передані дані шифруються, а на бек-офісних системах було ввімкнено журналювання доступу до файлів, які містять платіжні дані. Також ці системи включено до периметру сканування на вразливості та моніторингу відділом SOC.

Також Банк розробив спеціальну програму навчання для співробітників, дотичних до систем SWIFT: підрядники, бек-офіс, адміністратори та аудитори. У межах цієї програми щороку проводиться навчання, яке охоплює актуальні загрози, огляд вимог CSP і зону відповідальності кожного співробітника у підтриманні безпеки. Персонал повинен успішно скласти тест після навчання - це дозволяє забезпечити, що 100% відповідних співробітників пройшли підготовку. Окрім регулярного навчання, Банком було впроваджено практику оповіщення відповідального персоналу - якщо SWIFT випускає попередження про нові тактики атак або нові версії вимог, служба безпеки готує коротке оголошення і розсилає всім відповідальним особам. Ці процеси та процедури забезпечують безперервну відповідність вимозі 7.2 [2, с. 90].

Щодо вимоги 7.1, Банк розробив окремий план реагування на інциденти, пов’язані зі SWIFT [2, с. 88]. Цей план є додатком до загального плану реагування на інциденти Банку, розробленого в рамках набуття відповідності вимогам стандарту PCI DSS, але містить специфічні сценарії: наприклад, підозри компрометації SWIFT, шахрайського платежу. Призначено відповідальних членів команди реагування, встановлено канали оповіщення SWIFT. План

протестовано - було проведено навчальне моделювання інциденту: команда відпрацювала, як би діяли у випадку виявлення невідомого процесу в системі SWIFT, що намагається відправити повідомлення. Було виявлено елементи, у яких можливе покращення - оптимізація ланцюгу ескалації, після чого план реагування на інциденти було відповідно скориговано.

У результаті реалізації наведених контролів, Банком було досягнуто повної безперервної відповідності всім 25 обов'язковим контролям SWIFT CSCF, а також добровільно впроваджено низку заходів, спрямованих на підтримку відповідності рекомендаційних вимог, як-от 2.4 та 6.5, що підвищило загальну кіберстійкість [2, с. 50; 2, с. 86]. Важливо, що більшість цих заходів інтегровані в загальну систему безпеки банку і перетинаються з заходами, впровадженими для PCI DSS. Це створює синергію: одна інвестиція дозволяє набути відповідності одразу декільком стандартам.

3.5 Узгодження паралельного впровадження вимог стандартів у рамках єдиної програми відповідності

Впровадження вимог PCI DSS та SWIFT CSCF проводилося не ізольовано, а як єдина узгоджена програма відповідності та безпеки. Це дозволило Банку уникнути дублювання зусиль, ефективно використати ресурси та забезпечити цілісність процесу аудиту інформаційної безпеки. Ключовим завданням було виявлення перетинів між вимогами обох стандартів і побудова універсальних заходів, які задовольняють відразу обидва стандарти.

Банком було створено централізоване управління програмою відповідності. Хоча PCI DSS і SWIFT CSP історично могли відноситись до різних підрозділів, було прийнято рішення об'єднати ці функції під керівництвом однієї команди інформаційної безпеки. Відповідальний менеджер координує виконання вимог як PCI, так і SWIFT, що забезпечує єдине бачення ризиків і пріоритетів. Було створено робочу групу, до якої увійшли експерти з підрозділів платіжних карток, розрахунків, IT-інфраструктури та інформаційної безпеки.

Задачою цієї групи є проведення регулярних нарад, де обговорюється прогрес по кожному напрямку. Наприклад, питання контролю мережевого доступу розглядається одразу в контексті обох стандартів: чи відповідають сегментація і брандмауери вимогам PCI DSS 1.2 і SWIFT 1.1/1.4. Така взаємодія підвищує ефективність впроваджених рішень та враховує усі нюанси (регуляторні, технічні, операційні). Співставлення вимог і розробка універсальних заходів. Одним з перших кроків стала розробка мапи відповідностей між вимогами PCI DSS та SWIFT CSCF. Спеціалістами було проаналізовано кожну вимогу PCI DSS і було проведено співставлення еквівалентним або подібним вимогам SWIFT, якщо такі були наявні. Нижче, у таблиці 3.2 продемонстровано основні результати цього зіставлення - багато сфер суттєво збігаються: стандарти SWIFT спираються на галузеві кращі практики безпеки, тож не дивно, що між певними вимогами існує кореляція.

Таблиця 3.2

Відповідність вимог стандарту PCI DSS вимогам SWIFT CSCF

Вимога PCI DSS (v4.0.1)	**Відповідний контроль SWIFT CSCF (v2025)**
1.1, 1.2 Визначення меж CDE та конфігурації мережевого обладнання	1.1, 1.4 Захист середовища SWIFT від загальної мережі. Частково 1.5 принципи сегментації
1.3 Заборона небезпечних сервісів і адресації з/до CDE, мережеве розмежування внутрішніх зон	1.1 Аналогічно вимагає відокремлення критичних систем. 2.6 Шифрування сесій, перекликається із забороною небезпечних сервісів або пом'якшення за рахунок використання стійкої криптографії при встановленні з'єднань
2.1, 2.2 Відсутність паролів за замовчуванням на пристроях і системах Безпечна конфігурація систем	2.3, 5.4 Безпечна конфігурація систем та захист сховищ паролів, перекликається зі скасуванням паролів за замовчуванням Частково 2.2 підтримання актуальності систем
3.4 Маскування і шифрування PAN 3.5-3.6 Захист та управління ключами шифрування	6.1, 2.5A Опосередковано: SWIFT вимагає захисту даних при передаванні (шифрування каналів); прямого аналога управління картковими даними в SWIFT немає, оскільки SWIFT не оперує PAN; Частково 2.6 шифрування сесій оператора

Продовження таблиці 3.2

Вимога PCI DSS (v4.0.1)	**Відповідний контроль SWIFT CSCF (v2025)**
4.1 Шифрування карткових даних при передачі через відкриті мережі (TLS, IPSec тощо) 4.2 Заборона надсилання PAN електронною поштою або іншими технологіями обміну повідомленнями	2.5A Рекомендаційний контроль SWIFT про захист даних при зовнішніх передаваннях. 6.4 Опосередковано, контролює передачу даних через моніторинг. SWIFT не має прямого контролю на кшталт "не відправляти карткові дані у відкритому вигляді", оскільки інша сфера застосування
5.2 Встановлення механізмів захисту від шкідливого програмного забезпечення на всі системні компоненти, вразливі до шкідливого програмного забезпечення 5.3 Постійне оновлення та моніторинг механізмів захисту від шкідливого програмного забезпечення	6.1 Обов’язково вимагає встановлення механізмів захисту від шкідливого програмного забезпечення на усі відповідні системи SWIFT і актуальні бази даних. Відповідність майже пряма: вимоги щодо механізмів захисту від шкідливого програмного забезпечення співпадають.
6.2 Встановлення патчів для критичних вразливостей протягом щонайбільше 1 місяця. 6.3.1 Відстеження нових вразливостей, процес керування вразливостями	2.2 Повний аналог, вимагає своєчасного патч-менеджменту на системах SWIFT 2.7 Обов’язкове регулярне сканування, також корелює з вимогами PCI 11.3. 7.3A Рекомендаційна, але аналогічна PCI 11.4 (щорічне тестування на проникнення).
7.1-7.2 Обмеження доступу за ролями, принцип найменших прав; регулярний перегляд прав доступу	5.1 Пряма відповідність: контроль доступів користувачів SWIFT. 4.1 Частково відповідає вимогам до парольних та автентифікаційних політик (PCI 8 розділ). 5.3 Доповнює, вимагаючи періодичної перевірки персоналу щонайменше 1 раз на 5 років, PCI DSS теж вимагає тільки попередньої (12.7).
8.1-8.3 Унікальні ідентифікатори, керування життєвим циклом облікових записів, відключення неактивних. 8.4 MFA для адміністративного та віддаленого доступу. 8.5 Безпечне імплементування MFA	4.2 Вимагає MFA для всіх критичних доступів у SWIFT (повна кореляція з PCI 8.4) 5.1, 5.2 Охоплює унікальні ідентифікатори (токени, сертифікати) і управління привілейованим доступом. 5.4 Захист паролів (доповнює PCI 8.2.1 щодо зберігання паролів).

Продовження таблиці 3.2

Вимога PCI DSS (v4.0.1)	**Відповідний контроль SWIFT CSCF (v2025)**
9.1-9.3 Фізичний контроль доступу до приміщень (зони) з CDE. 9.5-9.8 Захист носіїв інформації, журналів доступу, знищення даних	3.1 Повна відповідність: вимагає контролю фізичного доступу до приміщень SWIFT, авторизація, відеонагляд. SWIFT не регулює носії інформації так детально, але загальні принципи фізичного захисту корелюють.
10.1-10.5 Журналювання подій, захист журналів від змін, регулярний огляд журналів. 10.7 Збереження журналів ≥ 1 року	6.4 Практично еквівалент: вимагає реєстрації всіх безпекових подій у середовищі SWIFT та їх моніторинг. SWIFT також через інші вимоги (наприклад 5.2, 2.11A) посилює важливість журналювання; загальне збереження журналів ≥ 1 року.
11.3 Сканування внутрішніх і зовнішніх вразливостей щокварталу та після значних змін. 11.4 Тестування на проникнення щорічно. 11.5 IDS/IPS та FIM для виявлення атак і змін.	2.7 Однозначно вимагає регулярних сканувань (аналог PCI 11.3). 7.3A Рекомендаційна, але по суті відповідає PCI 11.4. 6.5A Рекомендована вимога, але аналог IDS/IPS. Прямої вимоги FIM стосовно файлів конфігурацій у SWIFT немає, але 6.2 Виконує схожу функцію (контроль цілісності додатків та інсталяційних файлів).
12.1-12.2 Політики безпеки, щорічний перегляд; аналіз ризиків. 12.5 Призначення відповідальних осіб. 12.6 Програма навчання з безпеки (щорічна). 12.8 Управління TPSP (договори, моніторинг відповідності). 12.10 План реагування на інциденти, навчання персоналу реагування, тестування плану.	1.1 Узгоджується з наявністю політик і відповідальних осіб. 2.8 Еквівалент PCI 12.8, вимагає управління ризиками TPSP. 7.2 Аналог PCI 12.6, обов’язково проводить навчання персоналу. 7.1 Відповідає PCI 12.10, вимагає план реагування і обміну інформацією. 7.4A Рекомендаційна, але корелює з PCI 12.2 (стосовно проведення оцінки ризиків).

Як показано у таблиці 3.2, більшість вимог PCI DSS мають еквівалентні вимоги у SWIFT CSCF. Це дає змогу будь-якій компанії використовувати інтегровані рішення: однаково задовольняти дві групи вимог одним набором політик, процедур і заходів. Спираючись на співставлення, Банк оптимізував

свою програму відповідності. Були створені уніфіковані політики інформаційної безпеки, які враховують обидва стандарти. Наприклад, політика управління вразливостями охоплює як системні компоненти CDE, так і системні компоненти середовища SWIFT, встановлюючи однакові або сумісні процеси сканування вразливості. Політика контролю доступу об’єднує вимоги до всіх критичних систем середовища SWIFT та системних компонентів CDE у контексті унікальних ідентифікаторів, ролей, MFA тощо. Це дозволяє уникнути дублювання документів і потенційних конфліктів між ними. Також у процесі реалізації було виявлено, що SWIFT CSCF офіційно корелює свої контролі з відомими фреймворками (зокрема, SWIFT розробила таблиці відповідності своїх контролів з NIST CSF, ISO 27002, PCI DSS та ін. стандартами) [20]. Це підтвердило правильність обраного підходу.

Згідно з даними компаній-аудиторів, контролі SWIFT співставляються з вимогами PCI DSS та інших стандартів, тому фінансові установи можуть використовувати одні й ті самі процеси й заходи для різних сертифікацій [5].

Важливим аспектом паралельного виконання стандартів було узгодити їхні терміни та дедлайни. Перехід на PCI DSS v4.0.1 вимагав повної відповідності до початку 2025 року, тоді як для SWIFT CSCF щорічна атестація за версією 2025 мала бути подана до кінця 2025 року. Банк поставив собі внутрішній дедлайн - виконати всі нові вимоги PCI DSS і SWIFT до останнього кварталу 2024 року, щоб мати запас часу перед обома перевірками. Завдяки інтегрованому підходу, більшість заходів було реалізовано вже в середині 2024.

3.6 Оцінювання результатів реалізації та визначення напрямів подальшого вдосконалення

Після завершення впровадження запланованих заходів було проведено підсумкове оцінювання - як внутрішнє (самооцінка), так і зовнішні аудити на відповідність PCI DSS та незалежна перевірка вимог SWIFT. Результати однозначно продемонстрували значний прогрес у покращенні стану

інформаційної безпеки Банку. Нижче наведено порівняльну таблицю 3.3, що зіставляє початковий стан системи (до впровадження, за результатами аналізу) та цільовий стан (після реалізації програми) за ключовими аспектами. Ця таблиця наочно відображає підвищення рівня якості процесів, процедур та заходів безпеки.

Таблиця 3.3

Аспект / контроль	**Початковий стан (до впровадження)**	**Цільовий стан (після впровадження)**
Мережна сегментація	Часткова сегментація: CDE відокремлений логічно, але існують необґрунтовані з'єднання. Набори правил міжмережевих екранів неповні. Безпечна зона SWIFT не повністю відокремлена.	Повна сегментація: суворе розділення мереж. Набори правил міжмережевих екранів з мінімальними необхідними дозволами. Безпечна зона SWIFT відокремлена, прямий трафік лише за необхідністю, відсутні непередбачені з'єднання.
Контроль доступу та автентифікація	Спільні облікові записи для адміністраторів. MFA застосовувався обмежено. Паролі могли бути простими або не змінюватись довго. Не проводився перегляд прав.	Усі користувачі мають унікальні ідентифікатори. Привілеї розмежовані за ролями за моделлю найменших привілеїв. MFA впроваджено для всіх адміністраторів і критичних вузлів. Політика паролів забезпечує надійність паролів/парольних фраз та їх періодичну ротацію. Щоквартальний перегляд доступів. Облікові записи видаляються/блокуються при звільненні негайно.
Моніторинг та журналювання	Журнали розподілені по системах. Відсутня кореляція журналів. Аналіз журналів - епізодичне та вручну. Інциденти можуть лишатися непоміченими.	Централізований збір журналів у SIEM. Моніторинг усіх безпекових подій у режимі реального часу. Налаштовані кореляційні правила (IDS + FIM + Антивірус). Цілодобове реагування SOC. Журнали захищені від змін. Журнали централізовано зберігаються ≥1 рік.
Виявлення атак (IDS, FIM)	IDS/IPS відсутні або покривають лише периметр. FIM відсутній - цілісність критичних файлів не контролюється. Можливі атаки чи зміни на серверах залишаються непоміченими.	Розгорнуто IDS/IPS як на периметрі, так і між сегментами (у тому числі середовищем SWIFT) - весь трафік контролюється. Впроваджено FIM на критичних системних компонентах - несанкціоновані зміни файлів одразу генерують оповіщення. Виявлення атак та аномалій покращено.

Продовження таблиці 3.3

Аспект / контроль	**Початковий стан (до впровадження)**	**Цільовий стан (після впровадження)**
Управління вразливостями	Нерегулярне сканування на вразливості (≈ 1 раз на 12 місяців). Процес оновлення не формалізовано, затримки з встановленням патчів. Можливі довготривалі незакриті вразливості. Тестування на проникнення або не виконується, або поверхневе.	Налагоджений процес керування вразливостями. Внутрішнє сканування щонайменше 1 раз на місяць. Зовнішнє сканування щонайменше 1 раз на 3 місяці. Критичні патчі встановлюються ≤ 1 міс. (фактично - за 1-2 тижні). Ведеться реєстр вразливостей та їх виправлень. Щорічно незалежне тестування на проникнення із звітністю.
Політики, процедури, управління	Політики безпеки існують, але не охоплюють всі нові вимоги. Персонал не повністю ознайомлений. Програми навчання епізодичні. План реагування на інциденти загальний, специфіка інцидентів SWIFT не врахована. Відповідальність явно не призначена.	Оновлений комплект політик, що інтегрує вимоги PCI DSS та SWIFT CSCF, у тому числі нові. Призначено відповідального за відповідність стандартам. Регулярні навчання для всіх співробітників з урахуванням специфіки стандартів. Проведено доведення політик до відома під підпис. Впроваджено процедури реагування на інциденти, включно із сценаріями SWIFT. План реагування протестовано. Керівництво залучене через періодичні звіти та метрики KPI.
Відповідність аудитам	Попередні аудити проходили з зауваженнями. Частина вимог закривалась тимчасово "під аудит". Був ризик неуспішного проходження PCI DSS через нові вимоги. Атестація SWIFT CSP раніше вимагала плану ремедації по декількох вимогах.	Останній аудит PCI DSS пройдено успішно, отримано ROC без невідповідностей. Аудитори відзначили зрілість процесів, процедур та механізмів забезпечення безпеки. Атестація SWIFT CSP 2025 подана з позитивними відповідями по всіх обов’язкових контролях і кількох рекомендованих), без вимоги додаткового плану ремедації. Банк продемонстрував безперервну відповідність протягом року (імплементацію підтримки відповідності у BAU).

Як видно з таблиці 3.3, у цільовому стані безпекова інфраструктура банку набагато ефективніша. Ризики витоку даних чи несанкціонованих платежів знижено до мінімуму завдяки поєднанню оновлених технологічних рішень і налагоджених процесів. Також підвищено рівень обізнаності в питаннях безпеки

серед персоналу: завдяки навчанням і чіткому визначенню відповідальності співробітники усвідомлюють важливість своїх дій. Зовнішні аудити підтвердили відповідність: на кінець 2024 р. Банк отримав сертифікацію PCI DSS без жодного умовного зауваження - усі 12 розділів стандарту виконано. Одночасно на початку 2025 р. банк заповнив та подав самоатестацію SWIFT KYC-SA, вказавши виконання 25/25 обов'язкових контролів у тому числі 5 із 7 рекомендаційних контролів були позначені як "впроваджені". Це було підтверджено незалежною оцінкою, яку Банк добровільно замовив для підвищення довіри контрагентів.

Таким чином, кінцева мета - безперервна відповідність - досягнута: рівень захищеності Банку став динамічно підтримуватися на належному рівні постійно, а не лише на період аудиту. Це забезпечує не лише виконання формальних вимог, а й реальне зниження ймовірності успішних кібератак чи фінансового шахрайства.

Незважаючи на досягнутий прогрес, інформаційна безпека - це процес постійного розвитку. Банк визначив кілька напрямів для подальшого вдосконалення своєї системи з урахуванням еволюції загроз і стандартів:

Наступним кроком планується впровадження SOAR-платформи, яка інтегрується з SIEM і дозволяє автоматично виконувати окремі дії у відповідь на інциденти. Наприклад, при виявленні IOC на робочій станції оператора SWIFT, SOAR зможе автоматично ізолювати цей системний компонент від мережі та створити тікет на перевірку. Це скоротить час реагування і знизить вплив людського фактора. Такий підхід відповідає принципам проактивного реагування, закладеним у сучасні фреймворки.

Також Банк планує застосувати набуті практики і до інших регуляторних вимог. Наприклад, регламент DORA (Digital Operational Resilience Act) в ЄС, що набирає чинності, містить вимоги до кіберстійкості фінансових установ, багато з яких перетинаються з PCI DSS та SWIFT. Завдяки вже впровадженим процесам (управління інцидентами, тести на проникнення, моніторинг) банк буде краще готовий до впровадження заходів націлених на відповідність DORA та іншим нормативам (як-от вимогам НБУ, ISO 27001 сертифікації тощо). Планується

провести gap-аналіз щодо DORA/NIST CSF, використовуючи існуючу базу заходів, і за допомогою цього мінімізувати додаткові кроки.

Хоча програма навчання вже існує, Банк прагне зробити її більш інтерактивною і безперервною. Розглядається впровадження інтерактивного підходу: регулярні короткі тести для персоналу з безпеки, симульовані фішингові розсилки з відстеженням, відзначення найпильніших співробітників. Мета - щоб безпека стала частиною корпоративної культури, а не лише формальним тренінгом раз на рік. Також плануються тренінги спільно з іншими фінансовими установами, обмін досвідом стосовно безпеки SWIFT тощо - адже загрози еволюціонують, і колективна обізнаність галузі допоможе їм протистояти.

Банк слідкує за ринком рішень кібербезпеки і оцінює, які з них можуть підсилити існуючі контролі. Наприклад, технології поведінкового аналізу транзакцій UEBA, можуть ще краще виявляти аномальні дії користувачів SWIFT, доповнюючи статичні правила. Так само, розглядається використання Threat Intelligence платформ для отримання актуальних даних про загрози, які пов'язані з картковими шахрайськими схемами чи SWIFT-атаками, і проактивного налаштування захисту проти них.

Окрім безпекових заходів, Банк планує проводити регулярні стрес-тести - моделювати комплексні сценарії і оцінювати здатність команди реагування та систем захисту впоратися з ними. Це виходить за рамки формальних вимог стандартів, проте дає впевненість, що навіть у кризовій ситуації критичні сервіси будуть захищені і продовжать роботу належним чином.

Висновки до розділу 3

Підсумовуючи, впроваджена програма забезпечила Банку високий рівень відповідності як PCI DSS, так і SWIFT CSCF на поточний момент. Банк перейшов від реактивного підходу до проактивного: тепер безпека - це безперервний процес, інтегрований у аудиторську та операційну діяльність. Це підтверджує і

позиція регуляторів: нова версія SWIFT CSCF робить акцент на регулярних перевірках і доказах протягом року, а не тільки разово, а PCI DSS сприяє інтеграції вимог у BAU. Цей приклад продемонстрував, що такі підходи цілком реалістичні - за наявності волі керівництва, компетентної команди та належного планування можна досягти забезпечення постійної відповідності і підвищити кіберстійкість організації. Надалі Банк продовжить розвивати свою систему безпеки, спираючись на отримані результати, та буде готовий до нових викликів - як у галузі оновлення стандартів, так і у галузі кіберзагроз, які постійно розвиваються.

ВИСНОВКИ

У результаті проведеного дослідження проаналізовано вимоги стандартів PCI DSS та SWIFT CSCF, визначено їх вплив на інформаційну безпеку фінансових установ і запропоновано практичні підходи до впровадження та моніторингу відповідності. Розроблено модель програми безперервної відповідності, що охоплює нормативні, організаційні та технічні компоненти. Представлені результати можуть бути використані як методичне підґрунтя для побудови ефективної системи управління відповідністю у фінансових організаціях.

Првоедено аналіз вимог стандартів PCI DSS та SWIFT CSCF, їх структури, цілей та впливу на інформаційну безпеку фінансових установ. Встановлено, що стандарт PCI DSS зорієнтований на захист конфіденційних даних власників платіжних карток , зокрема встановлює вимоги щодо побудови безпечної мережевої інфраструктури, захисту даних, контролю доступу та інших аспектів обробки платіжної інформації. Натомість стандарт SWIFT CSCF складається з обов’язкових і рекомендованих заходів безпеки, які створюють базовий рівень захисту для всіх учасників платіжної системи SWIFT. Наріжним каменем обох стандартів є мінімізація ризиків несанкціонованого доступу, шахрайства та порушень цілісності даних, що має суттєвий позитивний вплив на стійкість фінансової інфраструктури.

Визначено, що ефективна інтеграція вимог стандартів у внутрішні процеси організації потребує гнучкого підходу: необхідно не лише формально дотримуватися норм, а й адаптувати заходи безпеки до реальних загроз та операційних особливостей установи. Зокрема, запропоновано застосовувати поетапну оцінку змін у середовищі та багатофакторну автентифікацію на різних етапах доступу, що забезпечує оптимальний баланс між кібербезпекою, відповідністю нормативним вимогам та економічною ефективністю впровадження заходів .

Обґрунтовано методи та засоби аудиту, моніторингу та контролю виконання вимог стандартів. Визначено, що ключовими технічними заходами є регулярне зовнішнє та внутрішнє тестування на проникнення, сканування вразливостей систем і мереж, а також впровадження системи виявлення вторгнень і централізованого збору та аналізу журналів. Зокрема, встановлено відповідність вимоги PCI DSS 11.4.3 щодо проведення зовнішніх тестувань на проникнення після кожних значних змін в інфраструктурі . Рекомендовано також автоматизувати процеси моніторингу та регулярно оновлювати інструменти аудиту. Поєднання технічних засобів із регулярними процедурними аудитами (внутрішнім та зовнішнім) забезпечує комплексну оцінку стану інформаційної безпеки і своєчасне виявлення відхилень від вимог.

Проведено дослідження поточного стану відповідності фінансової установи стандартам PCI DSS і SWIFT CSCF. Встановлено, що низка процесів та систем ще не досягла повної відповідності: зокрема, мережеві сегменти, що обслуговують обробку платіжних даних, недостатньо ізольовані від загальної IT-інфраструктури, а рівень журналювання подій безпеки є фрагментарним. Зафіксовано також затримки з оновленням програмного забезпечення та невчасним виправленням виявлених вразливостей. Окрім того, виявлено неповне документування політик та процедур безпеки, що посилює ризик людських помилок. Аналіз SWIFT-процесів виявив часткову відсутність обов’язкових заходів багатофакторної автентифікації та моніторингу активності користувачів у системі SWIFT. Узагальнення цих результатів дозволило виокремити ключові прогалини у системі безпеки та сформулювати рекомендації щодо їх усунення.

Розроблено детальний план впровадження технічних і організаційних заходів відповідно до вимог PCI DSS та SWIFT CSCF. Технічні заходи передбачають посилення сегментації мережі (виділення окремої довіреної зони для обробки платіжних даних), шифрування інформації, розширення застосування багатофакторної автентифікації та впровадження системи централізованого моніторингу безпеки (SIEM). Також заплановано регулярні оновлення і патчинг систем, а також проведення періодичних внутрішніх і

зовнішніх аудитів. Організаційні заходи включають оновлення та формалізацію політик безпеки, чіткий розподіл зон відповідальності, навчання персоналу з питань кібербезпеки та впровадження процесів управління змінами і ризиками. Реалізація цього плану спрямована на усунення виявлених недоліків і забезпечення безперервної відповідності стандартам.

Проведено оцінювання ефективності реалізованих заходів та сформульовано рекомендації щодо подальшого вдосконалення системи управління відповідністю. Після впровадження запропонованих змін відзначено позитивну динаміку: зменшилася кількість невдалих спроб несанкціонованого доступу, покращився процес збору і аналізу журналів, скоротився час реагування на інциденти. Проте оцінювання показало, що необхідно підтримувати безперервний цикл удосконалення: рекомендується впровадити додаткові автоматизовані інструменти моніторингу та звітності, а також забезпечити регулярне оновлення контролів відповідно до нових версій стандартів та постійне навчання персоналу. Варто також здійснювати періодичні незалежні аудити для підтвердження відповідності стандартам. Загалом, гнучке впровадження заходів безпеки і постійне удосконалення практик забезпечення відповідності сприяють підвищенню кіберстійкості фінансової установи, забезпечуючи баланс між інформаційною безпекою, відповідністю нормативам та економічною ефективністю.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Pci Security Standards Council. Payment Card Industry Data Security Standard. *Pci Security Standards Council website*. *Document Library*. 01.06.2024. URL: https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0_1.pdf (дата звернення: 12.05.2025).

2. Swift. Swift Customer Security Controls Framework v2025. *SWIFT*. 01.07.2024. URL: https://www2.swift.com/knowledgecentre/rest/v1/publications/cscf_dd/63.0/CSCF_v2025_20240701.pdf?logDownload=true (дата звернення: 12.05.2025).

3. It Grc Forum. Verizon reports sharp decline in PCI compliance. *IT GRC Forum*. *Home. Payment Security. Verizon reports sharp decline in PCI compliance*. URL: https://executiveitforums.org/9571-verizon-reports-sharp-decline-in-pci-compliance (дата звернення: 12.05.2025).

4. Rich A. Emerging Threats PRO/OPEN Ruleset for Suricata 7.0.3 Now Available. *Suricata*. 24.06.2024. URL: https://forum.suricata.io/t/emerging-threats-pro-open-ruleset-for-suricata-7-0-3-now-available/4714 (дата звернення: 12.05.2025).

5. SWIFT Customer Security Programme (CSP). *Schellman*. URL: https://www.schellman.com/services/cybersecurity-assessments/swift-csp (дата звернення: 12.05.2025).

6. Pci Security Standards Council. Information Supplement: Best Practices for Maintaining PCI DSS Compliance. *Pci Security Standards Council website*. *Document Library*. 01.01.2019. URL: https://docs-prv.pcisecuritystandards.org/Guidance%20Document/PCI%20DSS%20General/PCI_DSS_V2.0_Best_Practices_for_Maintaining_PCI_DSS_Compliance.pdf (дата звернення: 12.05.2025).

7. The Imperative of Continuous PCI DSS Compliance. *Grcmonroe*. 06.09.2024. URL: https://www.grcmonroe.com/pci-dss-continuous-compliance (дата звернення: 12.05.2025).

8. The Benefits of PCI Continuous Compliance Service. *Fortytwo*. 14.05.2024. URL: https://fortytwo.nl/blog/continuous-compliance-benefits/ (дата звернення: 12.05.2025).

9. Swift. Reinforcing the security of the global banking system. *Swift*. URL: https://www.swift.com/myswift/customer-security-programme-csp/security-controls (дата звернення: 12.05.2025).

10. Pwc Vietnam. SWIFT Customer Security Programme (CSP). *Pwc*. URL: https://www.pwc.com/vn/en/services/risk-assurance/cyber-security/swift-csp.html (дата звернення: 12.05.2025).

11. Dionach. Changes in the SWIFT CSCF 2025: What You Need to Know. *Dionach*. URL: https://www.dionach.com/changes-in-the-swift-cscf-2025-what-you-need-to-know/ (дата звернення: 12.05.2025).

12. rogue0xbyte. Zero Exploitation Unified System for Entity Security. *Github*. URL: https://github.com/AADILcrackstheweb/zeus#framework (дата звернення: 12.05.2025).

13. Karp D. A Proactive, Continuous Approach to Automated Compliance. *Isaca*. 24.10.2024. URL: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2024/a-proactive-continuous-approach-to-automated-compliance (дата звернення: 12.05.2025).

14. Scrut Automation. What is continuous compliance and how can your team actually achieve it?. *Scrut*. 05.05.2025. URL: https://www.scrut.io/post/continuous-compliance (дата звернення: 12.05.2025).

15. Protiviti. Understanding SWIFT’s 2021 Customer Security Programme and What the Changes Mean. *Protiviti*. 10.05.2021. URL: https://tcblog.protiviti.com/2021/05/10/understanding-swifts-2021-customer-security-programme-and-what-the-changes-mean/ (дата звернення: 12.05.2025).

16. Olukoya P., Lulu A. SWIFT: meeting updated CSCF attestation requirements. *Grantthornton*. 27.07.2023. URL: https://www.grantthornton.co.uk/insights/swift-meeting-updated-cscf-attestation-requirements/ (дата звернення: 12.05.2025).

17. Krishnan P. What is Continuous Compliance and Why It's More Than "Just a Perk". *Secpod*. 19.11.2020. URL: https://www.secpod.com/blog/continuous-compliance-and-its-benefits/ (дата звернення: 12.05.2025).

18. Rsi Security. ESSENTIAL BEST PRACTICES FOR ENSURING PCI DSS COMPLIANCE. *Rsisecurity*. 14.10.2024. URL: https://blog.rsisecurity.com/essential-best-practices-for-ensuring-pci-dss-compliance/ (дата звернення: 12.05.2025).

19. AWS. What is GRC (Governance, Risk, and Compliance)?. *AWS*. URL: https://aws.amazon.com/what-is/grc/ (дата звернення: 12.05.2025).

20. StandardFusion. Managing Multiple Compliance Frameworks Efficiently. *Standardfusion*. 02.01.2025. URL: https://www.standardfusion.com/blog/manage-multiple-compliance-frameworks (дата звернення: 12.05.2025).

21. Nocero J., Complianceandethics. Compliance and Continuous Improvement. *Complianceandethics*. 21.08.2015. URL: https://complianceandethics.org/compliance-and-continuous-improvement/ (дата звернення: 12.05.2025).

22. Sawant S., SISA. Unified Audits: Enhancing Compliance with a Unified Approach. *SISA*. URL: https://www.sisainfosec.com/executive-perspective/unified-audits-enhancing-compliance-with-a-unified-approach/ (дата звернення: 12.05.2025).

23. Secureframe. What Is Continuous Compliance + How To Achieve It. *Secureframe*. URL: https://secureframe.com/hub/grc/continuous-compliance (дата звернення: 12.05.2025).

24. Курій Є., Опірський І. БЕЗПЕКА ПЛАТІЖНИХ ОПЕРАЦІЙ: ОГЛЯД І ХАРАКТЕРИСТИКА КЛЮЧОВИХ ЗМІН У НОВІЙ РЕДАКЦІЇ СТАНДАРТУPCI DSS. *kubg*. 28.03.2024. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/565/445 (дата звернення: 12.05.2025).

25. Zendesk. All about PCI DSS (and why it's important). *Zendesk*. URL: https://www.zendesk.com/blog/all-about-pci-dds/ (дата звернення: 12.05.2025).

26. Matthias M., Neubert A., bdo. *bdo*. 04.01.2025. URL: https://www.bdo.de/en-gb/insights/updates/advisory-service/swift-customer-security-programme-v2025 (дата звернення: 12.05.2025).

27. Chin K., upguard. Guide to SWIFT CSCF (Customer Security Controls Framework). *upguard*. 07.01.2025. URL: https://www.upguard.com/blog/swift-cscf (дата звернення: 12.05.2025).

28. Auditboard. CI DSS Compliance: Critical Roles and Responsibilities. *auditboard*. 24.03.2021. URL: https://auditboard.com/blog/pci-dss-compliance-roles/ (дата звернення: 12.05.2025).

29. Webb K., Strikegraph. PCI DSS policy essentials: requirements, examples & templates. *Strikegraph*. 27.08.2024. URL: https://www.strikegraph.com/blog/pci-dss-policy (дата звернення: 12.05.2025).

30. Riskwatch. The Ultimate Guide to Compliance Risk Management. *Riskwatch*. 18.06.2024. URL: https://www.riskwatch.com/the-ultimate-guide-to-compliance-risk-management/ (дата звернення: 12.05.2025).

31. Verizon Payment Security Practice. An industry guide to PCI security compliance. *Verizon*. 28.03.2025. URL: https://www.verizon.com/business/resources/articles/s/industry-guide-to-pci-security-compliance/ (дата звернення: 12.05.2025).

32. Vanta. Compliance automation: What it entails and how to get started. *Vanta*. URL: https://www.vanta.com/collection/grc/compliance-automation (дата звернення: 12.05.2025).

33. Mukherjee A., Threatintelligence. Make Sure Your Business Is Ready for PCI 4.0 Requirements in 2023. *Threatintelligence*. 11.01.2023. URL: https://www.threatintelligence.com/blog/pci-4-0 (дата звернення: 12.05.2025).

34. Securityjourney. The True Cost of PCI-DSS Non-Compliance. *Securityjourney*. URL: https://www.securityjourney.com/post/the-true-cost-of-pci-dss-non-compliance (дата звернення: 12.05.2025).

35. Singh H., Securityboulevard. What is PCI DSS 4.0: Is This Still Applicable For 2024?. *Securityboulevard*. 12.01.2025. URL:

https://securityboulevard.com/2025/01/what-is-pci-dss-4-0-is-this-still-applicable-for-2024/ (дата звернення: 12.05.2025).

36. Intervalle Technologies. SWIFT CSCF Evolution. *Intervalle Technologies*. 10.09.2024. URL: https://intervalle-technologies.com/blog/swift-cscf-evolution/ (дата звернення: 12.05.2025).

37. Axletrees. A Glance at the Swift CSP Changes in 2023. *Axletrees*. URL: https://axletrees.com/a-glance-at-the-swift-csp-changes-in-2023/ (дата звернення: 12.05.2025).

38. Drata. 2023 Compliance Trends Report The Rise of Continuous Compliance. *Drata*. URL: https://learn.drata.com/hubfs/Downloadables/Drata_2023%20Compliance%20Trends%20Report.pdf (дата звернення: 12.05.2025).

39. Rane S., Controlcase. What are the 12 requirements of PCI DSS Compliance?. *Controlcase*. URL: https://www.controlcase.com/what-are-the-12-requirements-of-pci-dss-compliance/ (дата звернення: 12.05.2025).

40. SWIFT. Three years on from Bangladesh Tackling the adversaries. *SWIFT*. 01.04.2019. URL: https://www.swift.com/sites/default/files/documents/isac_report_201903_57412_v13.pdf (дата звернення: 12.05.2025).

41. Roffey J. The SWIFT CSP independent assessment and the role of internal audit. *LinkedIn*. 23.06.2023. URL: https://www.linkedin.com/pulse/swift-csp-independent-assessment-role-internal-audit-jonathan-roffey/ (дата звернення: 12.05.2025).

42. URM Consulting Services Ltd. PCI DSS compliance as BAU (business as usual). *URM*. URL: https://www.urmconsulting.com/blog/pci-dss-compliance-as-bau-business-as-usual (дата звернення: 12.05.2025).

43. Arcila C., Verizon. Verizon Business 2024 Payment Security Report: Simplifying the complexities of payment security. *Verizon*. 10.03.2024. URL: https://www.verizon.com/about/news/verizon-business-2024-payment-security-report (дата звернення: 12.05.2025).

44. Fintech. Що потрібно знати банкам про атестацію за Програмою безпеки користувачів Swift?. *FintechInsider*. 17.09.2024. URL: https://fintechinsider.com.ua/shho-potribno-znaty-bankam-pro-atestacziyu-za-programoyu-bezpeky-korystuvachiv-swift/ (дата звернення: 12.05.2025).

45. SWIFT. Independent assessment. *SWIFT*. URL: https://www.swift.com/myswift/customer-security-programme-csp/independent-assessment (дата звернення: 12.05.2025).