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

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Дослідження шляхів та розробка рекомендацій щодо збереження конфіденційності та цілісності фінансових даних у банківських установах»

зі спеціальності *125 Кібербезпека*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

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

_____ Яна МАРТИНЕНКО
(підпис)

Виконав: здобувач вищої освіти групи БСД-42
МАРТИНЕНКО Яна
(прізвище, ім'я)

Керівник ГАНЧЕНКО Марія
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

КИЇВ-2024

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

Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Бакалавр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Галина ГАЙДУР
“ 27 ” лютого 2024 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Мартиненко Яні Сергіївні
(прізвище, ім’я)

1. Тема кваліфікаційної роботи: «Дослідження шляхів та розробка рекомендацій щодо збереження конфіденційності та цілісності фінансових даних у банківських установах»
керівник кваліфікаційної роботи Ганченко Марія
(прізвище, ім’я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від « 27 » лютого 2024 року № 36 .

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 31.05.2024 р.

3. Вихідні дані до кваліфікаційної роботи
банківська таємниця;
стандарт ISO/IEC 27002, PCI DSS, постанова НБУ №95;
наукова та технічна література, документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Дослідження забезпечення інформаційної безпеки фінансових даних у банківських установах.

2. Аналіз стандартів забезпечення безпеки фінансових даних у банківських установах.

3. Розроблення рекомендацій щодо підвищення безпеки фінансових даних у банківських установах.

5. Перелік графічного матеріалу
Презентація PowerPoint.

6. Дата видачі завдання 27.02.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності проблеми збереження конфіденційності та цілісності фінансових даних у банківських установах.	27.02.2024 р.	
2.	Аналіз наукової та технічної літератури з питань теми кваліфікаційної роботи.	10.03.2024 р.	
3.	Аналіз методів та засобів захисту конфіденційності та цілісності фінансових даних у банківських установах.	27.03.2024 р.	
4.	Оцінка ефективності використовуваних підходів щодо забезпечення конфіденційності та цілісності фінансових даних у банківських установах.	08.04.2024 р.	
5.	Розроблення рекомендацій щодо застосування методів та засобів захисту фінансових даних у банківських установах.	22.04.2024 р.	
6.	Оформлення результатів дослідження.	27.05.2024 р.	
7.	Підготовка доповіді до захисту.	31.05.2024 р.	

Здобувач вищої освіти _____ Яна МАРТИНЕНКО
(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ Марія ГАНЧЕНКО
(підпис) *(ім'я, прізвище)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача МАРТИНЕНКО Яни

на тему: «Дослідження шляхів та розробка рекомендацій щодо збереження конфіденційності та цілісності фінансових даних у банківських установах »

Актуальність: Актуальність дипломної роботи полягає у необхідності забезпечення високого рівня захисту конфіденційності та цілісності фінансових даних у банківських установах в умовах зростання кіберзагроз. Розвиток сучасних програмно-технічних засобів злому та несанкціонованого доступу вимагає постійного вдосконалення заходів інформаційної безпеки. Дослідження існуючих методів захисту та розробка нових рекомендацій дозволить підвищити рівень захищеності фінансових даних. Це забезпечить стабільність та довіру до банківських установ з боку клієнтів та партнерів.

Позитивні сторони:

1. На основі проведеного аналізу, в роботі встановлено проблеми захисту фінансових даних у банківських установах та розроблено рекомендації для їх збереження.
2. Досліджено методи та засоби захисту фінансових даних у банківських установах.
3. Розглянуто технології захисту фінансових даних у банківських установах.
4. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Таблиці і схему оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою кваліфікаційної роботи.

Недоліки:

1. Запропонований порядок застосування технології захисту фінансових даних у банківських установах бажано було б показати на прикладі конкретної організації.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку **“добре”**, а здобувач(ка) **МАРТИНЕНКО Яна** – присвоєння кваліфікації бакалавр з кібербезпеки за спеціалізацією Інформаційна та кібернетична безпека.

Рецензент

:

_____	_____	_____
(науковий ступінь, вчене звання)	*(підпис)*	*(ім’я, прізвище)*

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

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

на здобуття освітнього ступеня бакалавра

Направляється здобувач МАРТИНЕНКО Яна до захисту кваліфікаційної роботи
(прізвище, ім'я)

спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)

на тему: «Дослідження шляхів та розробка рекомендацій щодо збереження конфіденційності та цілісності фінансових даних у банківських установах ».

Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Віталій САВЧЕНКО
(підпис) *(ім'я, прізвище)*

Висновок керівника кваліфікаційної роботи

Здобувач ***МАРТИНЕНКО Яна*** обрала тему роботи, метою якої було проаналізувати існуючу нормативно-правову і законодавчу базу з питань інформаційної безпеки у банківському секторі, дослідити сучасні програмно-технічні засоби захисту інформації; розробити рекомендації щодо підвищення рівня захищеності фінансових даних банківських установ та зниження ймовірності реалізації ризиків для конфіденційності та цілісності. Перелік використаних джерел свідчить про вміння здобувачем розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи ***МАРТИНЕНКО Яна*** показала добру теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконувала сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача ***МАРТИНЕНКО Яни*** на оцінку **"добре"** та присвоїти їй кваліфікацію бакалавр з кібербезпеки за спеціалізацією Інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ Марія ГАНЧЕНКО
(підпис) *(ім'я, прізвище)*
"____" _____ 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач **МАРТИНЕНКО Яна** допускається до захисту даної кваліфікаційної роботи в Екзаменаційній комісії.

Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Галина ГАЙДУР
(підпис) *(ім'я, прізвище)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 71 сторінки, 2 таблиці, 1 схема, 16 джерел.

Об'єкт дослідження: процес забезпечення конфіденційності та цілісності фінансових даних у банківських установах.

Предмет дослідження: національні та міжнародні стандарти з інформаційної безпеки, нормативно-правова, законодавча база України для побудови системи управління інформаційною безпекою, а також існуючі програмно-технічні засоби захисту фінансових даних банківських установ.

Мета роботи: проаналізувати існуючу нормативно-правову і законодавчу базу з питань інформаційної безпеки у банківському секторі, дослідити сучасні програмно-технічні засоби захисту інформації; розробити рекомендації щодо підвищення рівня захищеності фінансових даних банківських установ та зниження ймовірності реалізації ризиків для конфіденційності та цілісності.

Методи дослідження: опрацювання літератури за даною темою, порівняльний аналіз нормативно-правових актів, міжнародних та вітчизняних стандартів, аналіз використовуваних програмно-технічних засобів забезпечення інформаційної безпеки банківських установ.

Дана робота включає опис теоретичних та методологічних аспектів стратегічного управління діяльністю відповідних служб банківських установ щодо забезпечення захисту платежів, банківських операцій, конфіденційної інформації на основі побудованої згідно із нормативними актами Національного банку України та у відповідності до міжнародних і національних стандартів, системи управління інформаційною безпекою.

У роботі надано перелік і опис категорій банківської інформації, існуючих загроз і ризиків, які можуть впливати на цілісність і конфіденційність інформації. Представлено опис засобів захисту інформації, мережевих ресурсів та даних, що передаються внутрішніми каналами зв'язку, які забезпечують функціонування банківських установ.

На основі проведеного дослідження і вивчення нормативно-правової та технічної документації сформульовано висновок щодо рівня захищеності фінансових даних у банківських установах проаналізовано існуючу нормативно-правову і законодавчу базу з питань інформаційної безпеки у банківському секторі, досліджено сучасні програмно-технічні засоби захисту інформації та розроблено рекомендації щодо підвищення рівня захищеності фінансових даних банківських установ та зниження ймовірності реалізації ризиків для конфіденційності та цілісності.

Галузь використання: банківські та фінансові установи, кібербезпека інформаційних ресурсів організації.

БЕЗПЕКА БАНКІВСЬКИХ УСТАНОВ, PCI DSS, ISO/IEC 27002, ПОСТАНОВА НБУ №95, КІБЕРБЕЗПЕКА, БАНКІВСЬКА ТАЄМНИЦЯ.

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ……..……..…10

ВСТУП……..……....12

1 ДОСЛІДЖЕННЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ФІНАНСОВИХ ДАНИХ У БАНКІВСЬКИХ УСТАНОВАХ…….....14

1.1 Конфіденційність та цілісність фінансових даних у банківських установах……14

1.2 Загрози та ризики конфіденційності та цілісності фінансових даних у банківських установах……...25

2 АНАЛІЗ СТАНДАРТІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ФІНАНСОВИХ ДАНИХ У БАНКІВСЬКИХ УСТАНОВАХ……...…….....…...30

2.1 Підходи до збереження конфіденційності та цілісності фінансових даних у банківських установах……...……30

2.2 Оцінка ефективності використовуваних підходів щодо забезпечення конфіденційності та цілісності фінансових даних у банківських установах відносно наявних загроз та ризиків…….44

3 РОЗРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО ПІДВИЩЕННЯ БЕЗПЕКИ ФІНАНСОВИХ ДАНИХ У БАНКІВСЬКИХ УСТАНОВАХ……...…48

3.1 Рекомендації щодо підвищення рівня забезпечення конфіденційності та цілісності фінансових даних у банківських установах..……..48

3.2 Побудова стратегії та опис практичних кроків з впровадження розроблених рекомендацій……..55

ВИСНОВКИ……..……60

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ…….65

ДОДАТКИ……66

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація) 71

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АБС- автоматизована банківська система

АМКУ - Антимонопольний комітет України

АРМ - автоматизоване робоче місце

ДІС- Департамент Інформаційних систем

ЕЦП- електронно-цифровий підпис

ІБ- інформаційна безпека

ІС- інформаційна система

ІТ- інформаційна технологія

КСЗІ- комплексні системи захисту інформації

НБУ- Національний банк України

ПЗ- програмне забезпечення

СУБД- Система управління базами даних

СУІБ-Системи управління інформаційною безпекою

УІБ- Управління інформаційною безпекою

ЦСК- Центр Сертифікації Ключів

ЮУ - Юридичне управління

DAC- Discretionary Access Control

DDoS- Distributed Denial of Service attack

HTTPS- HyperText Transfer Protocol Secure

IAM- Identity Access Management

IDS- Intrusion Detection System

IPS-Intrusion Prevention System

MAC- Mandatory Access Control

MFA- Multifactory Authentification

NGFW- Next-Generation Firewall

OIM -Oracle Identity Manager

OTP- One Time Password

RBAC- Role Based Access Control

SIEM- Security Information and Event Management

SSL- Secure Sockets Layer

TLS- Transport Level Security

VPN- Virtual Private Network

WAF- Web Application Firewall

XSS- Cross-Site Scripting

ВСТУП

Актуальність дослідження. У сучасних умовах швидкого розвитку ІТ і цифровізації банківської сфери, питання захисту електронної інформації набувають особливої важливості. Банківські установи України щодня стикаються з різноманітними кібератаками, що ставить під загрозу конфіденційність, цілісність та доступність фінансових даних. Дослідження даної кваліфікаційної роботи спрямоване на висвітлення питань, пов'язаних із напрямками діяльності, існуючими методами та засобами захисту електронної інформації у банківських установах України. Основною метою є забезпечення ІБ в умовах постійного вдосконалення сучасних програмно-технічних засобів злому, несанкціонованого доступу до інформації, крадіжок комерційної інформації, втрати або несанкціонованої модифікації фінансових даних, а також порушення роботи інформаційних та телекомунікаційних систем банку.

ІБ є критичним аспектом функціонування банківських установ, адже вона забезпечує захист конфіденційної інформації про клієнтів, фінансових операцій та внутрішніх процесів банку. Втрата або компрометація цієї інформації може призвести до значних фінансових збитків, втрати довіри клієнтів і репутаційних ризиків.

Об’єкт дослідження: процес забезпечення конфіденційності та цілісності фінансових даних у банківських установах

Предмет дослідження: національні та міжнародні стандарти з інформаційної безпеки, нормативно-правова, законодавча база України для побудови СУІБ, а також існуючі програмно-технічні засоби захисту фінансових даних банківських установ.

Мета роботи: проаналізувати існуючу нормативно-правову і законодавчу базу з питань ІБ у банківському секторі, дослідити сучасні програмно-технічні засоби захисту інформації; розробити рекомендації щодо підвищення рівня

захищеності фінансових даних банківських установ та зниження ймовірності реалізації ризиків для конфіденційності та цілісності.

Наукові завдання:

проаналізувати існуючі методи та засоби, що використовуються для збереження конфіденційності та цілісності фінансових даних;

вивчити банківські операцій, категорій та груп інформації, які становлять банківську таємницю;

проаналізувати існуючі загрози конфіденційності та цілісності фінансових даних у банківських установах;

вивчити існуючу нормативно-правову і законодавчу базу з питань інформаційної безпеки у банківському секторі;

розробити рекомендації щодо покращення методів забезпечення цілісності і конфіденційності фінансових даних.

Методи дослідження: опрацювання літератури за даною темою, порівняльний аналіз нормативно-правових актів, міжнародних та вітчизняних стандартів, аналіз використовуваних програмно-технічних засобів забезпечення інформаційної безпеки банківських установ.

Практичне значення одержаних результатів: впровадження розроблених рекомендацій допоможе банківським установам значно підвищити рівень захищеності конфіденційної та цілісної інформації, зменшити ризики кіберзагроз та забезпечити відповідність нормативним вимогам. Це, у свою чергу, сприятиме зміцненню довіри клієнтів до банківських послуг та підвищенню загальної стійкості фінансової системи до кібератак.

1 ДОСЛІДЖЕННЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ФІНАНСОВИХ ДАНИХ У БАНКІВСЬКИХ УСТАНОВАХ

1.1 Конфіденційність та цілісність фінансових даних у банківських установах

У сучасному світі фінансові дані є одними з найбільш цінних ресурсів. Вони включають інформацію про транзакції, рахунки, кредитну історію та інші важливі аспекти фінансової діяльності банків. З огляду на критичну важливість фінансових даних, конфіденційність та цілісність мають першочергове значення для банківських установ. Порушення цих принципів може призвести до фінансових втрат, юридичних наслідків та втрати довіри клієнтів. В цьому розділі розглянуто важливість захисту конфіденційності та цілісності фінансових даних, загрози та програмно-апаратні засоби, методи та технології, що використовуються банками для захисту цих даних.

Конфіденційність фінансових даних означає захист від несанкціонованого доступу, а саме, що права доступу до інформації мають бути лише в уповноважених осіб. Банки зберігають значну кількість управлінської, фінансової, клієнтської інформації, що складає банківську та комерційну таємницю, яка в свою чергу, може бути використана для шахрайства, крадіжки особистих даних або інших злочинів [11]. Забезпечення конфіденційності фінансових даних є юридичною вимогою, регламентованою державними законами, національними стандартами та нормативними актами галузевого регулятора наприклад Національного банку України.

Цілісність фінансових даних означає, що дані залишаються незмінними та точними протягом усього циклу їх обробки. Порушення цілісності може

призвести до неправильних управлінських рішень, фінансових втрат і серйозних помилок у роботі банків. Втрата цілісності даних може призвести до помилкових, недостовірних фінансових звітів, що може ускладнити прийняття управлінських рішень і може мати серйозні правові наслідки.

Для захисту конфіденційності фінансових даних банківські установи на всіх рівнях оброблення (створення, передавання, зберігання) інформації використовують сучасні технології ІБ.

1) Шифрування.

Шифрування даних є одним з основних методів забезпечення конфіденційності інформації, який полягає в механізмі перетворення даних з метою їх приховування від неавторизованих осіб. Шифрування забезпечує захист конфіденційної інформації від несанкціонованого доступу та крадіжок, що є особливо актуальним в умовах зростання кількості загроз для ІБ.

Шифрування перетворює інформацію в секретний код, який може бути розшифрований лише за допомогою спеціального ключа дешифрування. Це гарантує, що навіть якщо дані будуть перехоплені, зловмисники не зможуть їх використати.

Існує два основних типи шифрування:

Симетричне шифрування: Метод симетричного криптографічного шифрування полягає у використанні одного і того ж ключа для шифрування та дешифрування даних. Цей метод є швидким і ефективним для обробки великих обсягів даних, але вимагає додаткових програмно-технічних засобів безпечної передачі ключа між відправником і одержувачем.

Асиметричне шифрування: За цим методом використовується пара ключів — таємний (закритий) і відкритий, жоден з них не може бути обчислений з іншого за відповідний час. Відкритий ключ призначений для шифрування, а закритий — для дешифрування інформації. Відкритий ключ може бути

опублікованим для використання усіма користувачами системи, для шифрування даних. Розшифровування даних за допомогою відкритого ключа неможливе. Розшифровування повідомлень, що були закодовані відкритим ключем, здійснюється закритим ключем, який є тільки у адресата.

Цей метод забезпечує більш високий рівень безпеки, оскільки закритий ключ залишається конфіденційним.

Алгоритми асиметричного шифрування, також як і симетричного, застосовують для шифрування масивів даних. Ці алгоритми покладено в основу задач автентифікації користувачів банківських інформаційних систем і контролю цілісності даних.

Важливого практичного значення асиметричні криптоалгоритми набули у застосуванні систем електронно-цифрового підпису (ЕЦП), який використовується в автоматизованих системах банківських установ для захисту фінансових, інших конфіденційних даних при виконанні працівниками банку операцій з фінансовими інструментами, дозволеними галузевим регулятором – НБУ.

Банківські установи застосовують шифрування на різних рівнях та для різних цілей:

а) Шифрування даних у стані спокою: Захист даних, які зберігаються на серверах, у базах даних або на резервних носіях, з метою запобігання доступу до інформації у разі фізичного злому чи крадіжки носіїв даних.

б) Шифрування даних під час передачі: Безпека даних, що передається каналами зв’язку між клієнтськими і банківськими програмними додатками, а також між банківськими інформаційними системами, логічно зв’язаними між собою інтеграційними схемами оброблення даних.

Вся інформація від відправника (джерела її створювання/оброблення/збереження) до одержувача (вузла/точки її замовлення

або обробки) передається каналами передачі даних комп’ютерних мереж, які створюються в банківських установах для забезпечення обміну інформації в їх корпоративному середовищі.

В епоху інтенсивного обміну інформацією і активного розвитку інформаційних технологій вся сукупність елементів мережі банківської установи - сервери, мобільні комп'ютери, сайти та бази даних є потенційними цілями зловмисників і всі вони є потенційно уразливі.

Для захисту корпоративних мереж банківських установ та відповідно інформації, що передається з використанням мережевих технологій і відповідного обладнання, використовуються технології шифрування даних, парольного захисту, автентифікація користувачів, антивірусні програми, системи моніторингу та виявлення вторгнень, мережеві файєрволи та транспортні протоколи безпеки, в тому числі протоколи SSL/TLS HTTPS, що створюють захищене з’єднання між веб-сервером та веб-браузером користувача і захищають інформацію під час її передачі через Інтернет.

Важливою складовою СУІБ є також управління криптографічними ключами, що забезпечують захист шифрованих даних. Далі наведено основні підходи та технології, що використовуються для шифрування даних у банківській сфері:

Шифрування даних на рівні програмних додатків: Використовується для захисту конфіденційної інформації, що оброблюється банківськими додатками, такими як інтернет-банкінг чи мобільний банкінг.

Шифрування в апаратних рішеннях: Використовується в банкоматах, платіжних терміналах та інших пристроях для захисту даних на фізичному рівні.

Управління ключами: Відповідно до нормативних актів НБУ та вимог законодавства з метою забезпечення інформаційного захисту банками використовуються сертифіковані НБУ спеціальні системи генерації ключів

шифрування, що мають загальну назву Центр Сертифікації Ключів. Захист і управління криптографічними ключами є критично важливим аспектом СУІБ. Неправильне управління ключами, несвоєчасне їх оновлення може призвести до компрометації шифрованих даних.

Шифрування даних на рівні інтеграції інформаційних систем може використовуватись на рівні обміну, передавання інформації Інтернет та внутрішніми каналами зв'язку на рівні баз даних і програмних застосунків.

З огляду на вищевикладене, шифрування фінансових даних є ключовим аспектом забезпечення інформаційної безпеки у банківській сфері. Воно дозволяє захистити конфіденційну інформацію від несанкціонованого доступу та зменшує ризики кібератак. Впровадження шифрування потребує ретельного планування, ефективного управління криптографічними ключами та дотримання нормативно-правових вимог.

2) Процедури надання доступу до інформаційних систем - аутентифікація та авторизація.

Аутентифікація – це процес перевірки особи користувача, який намагається отримати доступ до системи або даних. Це перший рівень захисту, який підтверджує, що користувач є тим, за кого він себе видає. Без належно встановленої аутентифікації, зловмисники можуть отримати доступ до конфіденційних фінансових даних, що може призвести до фінансових втрат і пошкодження репутації банку.

Паролі найбільш поширений метод аутентифікації, який передбачає введення користувачем унікального паролю для доступу до системи. Однак цей метод має свої недоліки, такі як ризик злому та витоку паролів у випадку їх недостатньої складності.

Багатофакторна аутентифікація (MFA) забезпечує додатковий рівень захисту, вимагаючи від користувачів підтвердження своєї особи за допомогою

декількох незалежних способів. Це може бути комбінація пароля, одноразового коду або паролю (OTP), та одного з біометричних показників - відбитка пальця або розпізнавання обличчя, що значно підвищує рівень безпеки, оскільки біометричні дані важко підробити.

Для забезпечення безпеки платіжних трансакцій і конфіденційних даних в системах дистанційного обслуговування, мобільних додатках тощо банківські установи в своїй діяльності використовують апаратні або програмні пристрої, які генерують одноразові паролі (OTP) для доступу до системи. Вони забезпечують високий рівень безпеки, оскільки навіть якщо пароль перехоплять, його не можна буде використати повторно. Банківськими установами також використовуються апаратно-програмні пристрої e-Token-и, що захищають особисті ключі працівників (менеджерів і операторів) банку від їх копіювання або модифікації зловмисниками.

Вказані заходи безпеки створюють бар’єр для проникнення зловмисних кодів, направлених на викрадення або модифікацію фінансових та інших даних, розміщених та збережених в системах і на інформаційних ресурсах банківської установи.

Наступною процедурою інформаційної безпеки фінансових даних є авторизація. Авторизація- це процес надання прав доступу користувачу після успішної аутентифікації. Авторизація визначає, які ресурси або дані може використовувати користувач і які операції він може виконувати. Навіть якщо користувач пройшов аутентифікацію, авторизація забезпечує, що він має доступ лише до тих даних та функцій, які йому дозволені.

Головне призначення авторизації- керування рівнями та засобами доступу до певного захищеного ресурсу залежно від ідентифікатора і аутентифікатора (наприклад, пароля користувача) та надання певних повноважень (користувачу, програмі) на виконання деяких дій в системі для роботи з даними.

В автоматизованих системах банківських установ використовуються програмні засоби авторизації користувачів за відповідними службовими завданнями і обов’язками, що складає логічну систему виконання операцій за рольовою моделлю.

Загальна рольова модель доступу в інформаційній системі (RBAC) визначає права доступу на основі ролей користувачів. Кожній ролі призначаються певні права, і користувачі, які належать до цієї ролі, отримують відповідний рівень доступу. В інформаційних системах банківських установ використовується вбудований програмний метод логічного розмежування доступу користувачів. На рівні операційних систем та СУБД використовується мандатна модель керування доступом - MAC.

Дискреційний контроль доступу (DAC) дозволяє власникам даних визначати, хто може мати доступ до їхніх даних, до яких саме, і які дії вони можуть з ними виконувати. Це гнучка модель, яка дозволяє точніше налаштовувати права доступу. Метод полягає у вибірковому керуванні (розмежуванні) доступом користувачів до об'єктів на основі списків або матриці доступу.

MAC використовується в середовищах з високими вимогами до безпеки. Права доступу визначаються політиками безпеки, і користувачі не можуть їх змінювати.

Аутентифікація та авторизація є основою інформаційної безпеки в банківських установах, та надає наступні переваги:

- Захист конфіденційних даних: Гарантія, що доступ до фінансових даних мають лише уповноважені особи, що знижує ризик витоку інформації.
- Запобігання шахрайству: Запобігання можливостям реалізації несанкціонованого доступу до банківських систем і зменшення ризиків шахрайських дій.

- Підвищення довіри клієнтів: Забезпечення безпеки фінансових даних клієнтів, що підвищує довіру до банківської установи.

3) Використання VPN.

VPN є важливим інструментом для забезпечення конфіденційності та цілісності фінансових даних у банках. VPN забезпечують безпечний обмін даними, захист від кібератак та можливість безпечного віддаленого доступу.

VPN — технології широко використовуються в банках для захисту даних шляхом створювання VPN-тунелю між двома вузлами, що дозволяє приєднаному пристрою чи користувачу бути повноцінним учасником віддаленої мережі і користуватись її сервісами — внутрішніми сайтами, базами, принтерами, політиками виходу до Всесвітньої мережі Інтернет (World Wide Web — WWW). Безпека передавання інформації через загальнодоступні мережі реалізується за допомогою процедури шифрування, внаслідок чого створюється закритий для сторонніх канал обміну інформацією.

VPN захищають дані, що передаються через Інтернет, створюючи для кожного з'єднання безпечний тунель для передачі інформації. Це означає, що навіть якщо зловмисники перехоплять ці дані, вони не зможуть їх прочитати без відповідного ключа дешифрування. Це особливо важливо при віддаленому доступі до банківських систем, оскільки фінансові транзакції та обмін конфіденційною інформацією повинні бути захищені від несанкціонованого доступу.

Банки часто потребують надання віддаленого доступу до своїх систем для співробітників, партнерів або обслуговуючих організацій. Використання VPN дозволяє безпечно підключатися до внутрішніх мереж банку з будь-якої зовнішньої точки, забезпечуючи при цьому високий рівень безпеки. Це особливо актуально також в умовах зростаючої популярності дистанційної роботи.

VPN допомагають захистити банківські системи від кіберзагроз, таких, як атаки типу "людина посередині" (Man-in-the-Middle), під час яких зловмисники намагаються перехопити та змінити передані дані. Шифрування і захищений тунель, створений VPN, ускладнюють такі атаки та знижують ризики втрати або компрометації даних.

Тож незважаючи на численні переваги, управління VPN може бути складним завданням, оскільки включає налаштування, моніторинг і підтримку VPN-інфраструктури. Банки повинні мати кваліфікований персонал для управління цими системами, що може вимагати додаткових ресурсів і витрат. Безпека VPN повинна постійно підтримуватися на найвищому рівні, що вимагає регулярного оновлення програм ПЗ, виправлення вразливостей і проведення аудиту безпеки.

4) Політики нформаційної безпеки.

Відповідно до законодавства Україні з питань захисту критичної інфраструктури, кіберзахисту та інформаційної безпеки (ст. 73 гл.14 Закону України «Про банки и банківську діяльність») банки розробляють внутрішні політики ІБ та конфіденційності, що регламентують порядок обробки, зберігання конфіденційних даних, та мають забезпечити захист даних від несанкціонованого доступу, втрати або зловживань. Політика конфіденційності має забезпечити захист даних від несанкціонованого доступу, втрати або зловживань.

Системи контролю доступу дозволяють або забороняють доступ до певних типів даних, внесення змін до них для осіб яким ці дані потрібні. Доступ до захищеної інформації повинен бути обмежений, щоб тільки працівники які мають право доступу, могли отримувати цю інформацію. Це запобігає несанкціонованому редагуванню або видаленню інформації.

Системні журнали аудиту дозволяють відслідковувати всі операції з даними, що допомагає виявляти та реагувати на будь-які спроби несанкціонованого втручання.

Засобами захисту фінансових даних є вбудовані в СУБД програмні засоби аудиту доступу до даних, або в операційних системах - до файлів, об’єктів інформаційних мереж. Відповідний модуль аудиту (контролю) за подіями в системі та доступу до її ресурсів реалізовано в операційних системах сімейства MS Server AD, доступ до файлів, об в якій здійснюється за груповими політиками.

5) Хешування даних.

Алгоритм хеш-функцій полягає в програмному перетворенні вхідного масиву даних довільної довжини у вихідний бітовий рядок фіксованої довжини. Для кожного тексту генерується унікальний хеш, що не дозволяє відновлення тексту із хешу в разі перехоплення повідомлення.

Хеш-функції використовуються для кількох важливих завдань:

- Код автентифікації повідомлення: хеш-функції допомагають забезпечити цілісність та автентичність даних, перевіряючи, чи не були вони змінені під час передачі.

- Зберігання паролів: паролі зберігаються у вигляді хешів, що унеможливлює відновлення оригінального пароля навіть при доступі до пам'яті, де вони зберігаються.

- Електронний підпис: при створенні електронного підпису підписується не саме повідомлення, а його хеш-образ, що робить процес швидшим і безпечнішим.

Розроблені криптографічні хеш-функції застосовуються в банках для безпеки цифрового підпису, який за більшістю випадків використовується в програмах дистанційного обслуговування клієнтів у веб-застосунках «Клієнт-Банк» для обміну фінансовими та іншими даними з метою або отримання

інформації за клієнтськими рахунками, або для проведення банком відповідних платежів.

6) Резервне копіювання

Одним з обов'язкових заходів захисту даних і систем банківських установ є процес створення резервних копій баз даних, образів програмного забезпечення, файлів налаштувань мережевого обладнання, міжмережевих екранів, програмних засобів криптографічного захисту та інші.

Резервне копіювання даних забезпечує їх збереження у випадку технічних збоїв або кібератак. Резервні копії зберігаються у захищених місцях і можуть бути використані для відновлення даних.

Резервне копіювання даних є складовою частиною системи забезпечення безперервної діяльності банків. Резервне копіювання використовується для відновлення даних і функціонування роботи інформаційних систем у штатному режимі після аварійного переривання її внаслідок впливу зовнішніх факторів, в тому числі непередбачених катастрофічних подій, що призвели до зупинки банківської виробничої діяльності.

Задля забезпечення безперервного функціонування ІТ-інфраструктури Банку відповідно до правових норм банківськими установами розроблюються Плани відновлення роботи критичних систем автоматизації, які мають постійно тестуватися, актуалізуватися з врахуванням впроваджених змін в ІТ-інфраструктурі установи.

Плановому тестуванню, перевірці цілісності інформації, що зберігається на резервних носіях, також підлягають всі дані, що копіюються по завершенню операційного дня банку на магнітні пристрої за вбудованим в системи графіком, який налаштований з врахуванням часу на коректне закриття в системах автоматизації виробничих завдань.

Конфіденційність та цілісність фінансових даних є критично важливими для банківських установ. Це не тільки забезпечує довіру клієнтів та партнерів, але й запобігає серйозним фінансовим втратам, репутаційним шкодам та правовим наслідкам, пов'язаним з порушенням конфіденційності чи цілісності фінансових даних. Банки повинні постійно вдосконалювати свої системи безпеки, використовуючи новітні технології та методи захисту, щоб протистояти сучасним загрозам.

1.2 Загрози та ризики конфіденційності та цілісності фінансових даних у банківських установах.

Банки постійно стикаються з численними загрозами, що можуть поставити під удар конфіденційність та цілісність фінансових даних. До них належать:

1. Кіберзлочинність. Хакери можуть зламувати системи безпеки банків, красти конфіденційні дані або змінювати фінансові записи.
2. Внутрішні загрози. Співробітники можуть отримувати доступ до конфіденційної інформації, яка не є необхідною для їх роботи, що може призвести до витоку або зміни даних.
3. Шкідливе програмне забезпечення. Віруси, троянські програми та інші види шкідливого програмного забезпечення можуть порушувати конфіденційність та цілісність даних.

Задля забезпечення безпеки фінансових даних відповідними службами банківських установ проводяться заходи з виявлення подій, що можуть загрожувати цілісності банківської інформації [10].

Тому проводиться класифікація кіберзагроз, яка відбувається за наступними критеріями: порушення вимог конфіденційності та доступності, що розглянуто нижче.

1) Порушення вимог конфіденційності інформації, зокрема (не обмежуючись):

- дії через які отримано несанкціонований доступ до інформації або систем;

- втрата носів інформації за межами периметру банку:

- втрата або крадіжка ноутбука, планшета або смартфона, який містить інформацію з обмеженим доступом тощо;

- несанкціоновані спроби працівників отримати доступ вище наявного рівня;

- спроби зсередини або ззовні отримати доступ до інформаційних систем.

2) Порушення вимог цілісності:

- втрата даних або незавершені транзакції;

- шкідливе ПЗ, пошкодження інформації на жорстких дисках, помилки систем.

Основними типами подій, що можуть бути класифіковані, як кіберінциденти, що супроводжують кібератаки є наступні (не обмежуючись):

- компрометація облікових записів привілейованих користувачів;

- компрометація облікових записів зовнішніх сервісів:

- атаки на веб-додатки;

- мережеві атаки;

- зараження зловмисним кодом;

- виявлення збору інформації про інформаційну системи;

- нелегітимне використання привілейованих облікових записів;

- витік інформації з обмеженим доступом;

- порушення правил віддаленого доступу;

- несанкціоновані зміни даних, налаштувань систем/обладнання з вбудованими апаратними засобами захисту;

- незаконний моніторинг інформаційних систем банку (сканування);

- виконання працівником банку операції з інформаційними системами або інформацією, на яку він не має дозволу;

- використання публічних мереж (Інтернет) не за призначенням;

- витік конфіденційної інформації;

-відмова в обслуговуванні та фіксування спроб порушення роботи сервісу чи системи;

- фіксування різкого збільшення мережевого трафіка:

- спроба зламу або злам інформаційних систем Банку:

- фіксування системами виявлення/запобігання вторгнень IDS/IPS подій, що можуть становити загрозу інформаційним активам Банку та мережі Банку в цілому;

- фіксування відповідальними працівниками Банку чи повідомлення користувачів про наявність у своїх поштових скриньках великої кількості повідомлень, що повторюються та мають неслужбовий характер;

-цілеспрямована кібератака комп'ютерних злочинців з метою шантажування тощо.

Опис категорій кіберінцидентів, що трапляються у банківських установах наведено у Додатку А.

З урахуванням вказаних категорій інцидентів відповідними службами банківських установ розробляються превентивні засоби контролю і протидії потенційним загрозам інформаційної безпеки відповідно до вимог Регулятора та Національного законодавства.

Забезпечення конфіденційності та цілісності фінансових даних, забезпечення безперервності функціонування елементів IT-інфраструктури банків, стратегія і політики управління ризиками ІБ регулюється державними законодавчими актами та нормативно-правовими документами. Основними документами, що регулюють діяльність банків у сфері інформаційної безпеки в Україні є (не обмежуючись):

1. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" – визначає основні принципи захисту інформації та вимоги до інформаційної безпеки.
2. Закон України "Про основні засади забезпечення кібербезпеки України" – встановлює правові та організаційні засади забезпечення кібербезпеки.
3. Постанова НБУ № 95 "Про затвердження Положення про захист інформації та кібербезпеку в банківській системі України" – регулює вимоги до забезпечення захисту інформації та кібербезпеки в банківській системі.

Дотримання нормативних вимог є критично важливим для забезпечення належного рівня захисту фінансових даних. Це не лише мінімізує ризики витоку інформації та шахрайства, але й підвищує довіру клієнтів до банку. Крім того, недотримання вимог може призвести до серйозних правових наслідків, включаючи штрафи та втрату ліцензії на здійснення банківської діяльності.

Профільним службам банківської установи необхідно здійснювати постійній моніторинг змін в законодавчій базі та приведення програмних продуктів, які експлуатуються у банківській установі, у відповідність із законами та іншими нормативно-правовими актами, стандартами, нормами і правилами, передбаченими державним законодавством [1].

Незважаючи на існування багатьох методів та засобів захисту, забезпечення конфіденційності та цілісності фінансових даних залишається викликом для розробників і вендорів прикладного програмного забезпечення, призначеного для автоматизації банківських операцій. Нові загрози постійно з'являються, і банки повинні бути готові до запобігання їх реалізації. Це вимагає постійного оновлення систем безпеки, навчання персоналу та впровадження новітніх технологій, в тому числі створення та постійного удосконалення КСЗІ банківських установах.

2 АНАЛІЗ СТАНДАРТІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ФІНАНСОВИХ ДАНИХ У БАНКІВСЬКИХ УСТАНОВАХ

2.1 Підходи до збереження конфіденційності та цілісності фінансових даних у банківських установах

Банківська таємниця

Конфіденційність і цілісність фінансових даних є основоположними принципами роботи банківських установ. Однією з ключових складових цього підходу є поняття банківської таємниці, яке встановлює необхідність захисту інформації про клієнтів і їхні фінансові операції.

Банківська таємниця- це інформація щодо діяльності та фінансового стану клієнта, яка стала відомою банку у процесі обслуговування клієнта та взаємовідносин з ним або стала відомою третім особам при наданні послуг банку або виконанні функцій, визначених чинним законодавством України. В Україні захист банківської таємниці регулюється Законом України "Про банки і банківську діяльність". Згідно з цим законом, банківські установи зобов'язані забезпечувати нерозголошення інформації про своїх клієнтів без їхньої згоди, за винятком випадків, передбачених законодавством. До банківської таємниці, зокрема, відносяться:

1. Відомості стосовно комерційної діяльності клієнтів чи комерційної таємниці, будь-якого проекту, винаходів, зразків продукції та інша комерційна інформація;

2. Інформація щодо звітності по окремому банку, за винятком тієї, що підлягає опублікуванню;

3. Відомості щодо фінансово-економічного стану клієнтів;

4. Інформація про організаційно-правову структуру юридичної особи - клієнта, і керівників, напрями діяльності;

5. Відомості стосовно комерційної діяльності клієнтів чи комерційної таємниці, будь-якого проекту або іншу комерційну інформацію;

6. Інформація щодо звітності по окремому банку, за винятком тієї, що підлягає опублікуванню;

7. Інформація про фізичну особу, яка має намір укласти договір про споживчий кредит, отримана під час оцінки її кредитоспроможності;

8. Інформація про організацію та здійснення інкасації коштів або перевезення валютних цінностей;

9. Інформація про банки чи їх клієнтів, що збирається банками під час здійснення банківського або валютного нагляду, нагляду платіжних систем та систем розрахунків, а також нагляду у сфері запобігання та протидії легалізації доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення;

10. Рішення Національного банку України про застосування заходів впливу, крім рішень про накладення штрафів, про віднесення Банку до категорії неплатоспроможних, про відкликання банківської ліцензії та ліквідацію банку.

Організація роботи із банківською таємницею є критичним аспектом діяльності банківських установ. Дотримання правил роботи із банківською таємницею допомагає зменшити ризики витоку інформації та підтримувати довіру клієнтів.

Основними вимогами до збереження банківської таємниці, запровадженими в банку, що забезпечує збереження банківської таємниці є:

1.) обмеження доступу до конфіденційної інформації виключно для уповноважених осіб, ведення журналів доступу, логування та моніторинг дій користувачів при роботі з даними;

2.) організації спеціального діловодства з документами, що містять банківську таємницю;

3.) використання технічних засобів для запобігання несанкціонованому доступу до електронних та інших носів інформації;

4.) застосування застережень щодо збереження банківської таємниці та відповідальності за її розголошення у договорах і угодах, укладених між Банком і його клієнтами;

5.) регулярне навчання співробітників щодо правил роботи з конфіденційною інформацією, політик безпеки та інформування про нові загрози;

6.) періодичне проведення внутрішніх та зовнішніх аудитів для оцінки ефективності заходів захисту та дотримання політик конфіденційності.

Також працівники Банку при вступі на посаду повинні підписати Зобов'язання щодо збереження банківсько таємниці. Керівники та працівники банківської установи зобов'язані не розголошувати та не використовувати з вигодою для себе чи для третіх осіб інформацію, що становить банківську таємницю, яка стала відома їм під час виконання службових обов'язків.

Якщо банк надає інформацію, що становить банківську таємницю, фізичним та юридичним особам, це здійснюється виключно відповідно до договорів, укладених між такими організаціями та банком. Ці договори містять положення щодо збереження банківської таємниці та передбачають відповідальність за її незаконне розголошення або використання.

Щоб запобігти несанкціонованому доступу до інформації, що становить банківську таємницю, в банку повинен бути визначений особливий порядок

реєстрації, використання, зберігання та доступу до документів, що містять банківську таємницю.

PCI DSS

PCI DSS (Payment Card Industry Data Security Standard) — це глобальний стандарт безпеки, розроблений для захисту інформації про платіжні картки. Він був створений Радою з питань стандартів безпеки платіжних карток (PCI SSC), яка включає такі провідні платіжні системи, як Visa, MasterCard, American Express, Discover та JCB. Основна мета PCI DSS — забезпечити безпеку даних власників платіжних карток шляхом встановлення та підтримання жорстких вимог до обробки, зберігання та передачі даних.

Стандарт PCI DSS є невід'ємною частиною забезпечення інформаційної безпеки у банківських установах. Він встановлює високі вимоги до захисту даних власників карток та забезпечує комплексний підхід до захисту інформації. Впровадження стандарту PCI DSS допомагає банкам захистити себе від кіберзагроз, зберегти довіру клієнтів та відповідати регуляторним вимогам.

Основні вимоги стандарту PCI DSS

PCI DSS включає 12 основних вимог, які згруповані в шість категорій. Кожна з цих вимог спрямована на забезпечення певного аспекту безпеки даних платіжних карток:

1.Створення та підтримка безпечної мережі

Вимога PCI DSS 1: Установка та підтримка конфігурацій брандмауера для захисту даних власника картки.

Брандмауери —це базовий елемент захисту IT-інфраструктури, серверів, додатків та інформації від несанкціонованого доступу та інших зовнішніх загроз. Банківські установи створюють брандмауери у своїй мережі, щоб захистити

особливо конфіденційні дані та обмежити доступ для різних внутрішніх користувачів організації, оскільки не кожному співробітнику потрібен доступ до даних власників карток [4]. Ця вимога PCI DSS також визначає, як налаштовувати маршрутизатори та керувати ними для захисту даних власників карток у внутрішніх мережах. IT-команда банку повинна постійно відстежувати трафік брандмауера, переглядати конфігурації маршрутизатора кожні шість місяців і переналаштовувати їх, якщо необхідно.

Вимога PCI DSS 2: заборона використовувати надані постачальником параметри за замовчуванням для системних паролів та інших параметрів безпеки.

Організації повинні створювати власні унікальні паролі та інші параметри безпеки та не використовувати стандартні параметри, надані постачальником.

Ця вимога має на меті гарантувати, що організації знають і можуть контролювати рівень доступу до свого середовища. Організації також повинні регулярно оновлювати ці паролі та параметри безпеки.

2. Захист даних власників карток

Вимога PCI DSS 3: Захист збережених даних про власника картки.

Організації повинні захищати дані власників карток за допомогою шифрування, паролів і фізичних заходів безпеки, обмежуючи доступ лише для тих працівників, яким вони потрібні для виконання службових обов’язків.

Організації також повинні регулярно контролювати та тестувати безпеку будь-яких систем, які зберігають, обробляють або передають дані власників карток.

Вимога PCI DSS 4: Шифрування передачі даних власника картки через відкриті загальнодоступні мережі.

Ця вимога зобов’язує, що всі дані власника картки мають бути зашифровані під час передачі через відкриті загальнодоступні мережі. Це включає

використання безпечних протоколів шифрування, таких як SSL/TLS або IPsec, для захисту даних власника картки під час їх надсилання з однієї точки в іншу [3]. Ця вимога спрямована на те, щоб дані власників карток не розкривалися неавторизованим третім особам під час їх переміщення з однієї системи в іншу.

3. Підтримка програми керування вразливістю

Вимога PCI DSS 5: захист усіх систем від зловмисного програмного забезпечення та регулярне оновлення антивірусного програмного забезпечення.

Організації повинні підтримувати безпеку програмного забезпечення, що використовується для обробки платіжних транзакцій. Для цього слід вчасно оновлювати та встановлювати нові версії ПЗ, які вмикають вимогам безпеки, а також застосовувати заходи захисту, наприклад, антивірусне програмне забезпечення, перевірку на наявність вразливостей тощо.

Вимога PCI DSS 6: Розробка та обслуговування безпечних систем та додатків.

Ця вимога передбачає, що організації повинні впроваджувати суворі заходи безпеки під час розробки, підтримки та моніторингу всіх програм. Організації повинні переконатися, що всі системи та додатки безпечно налаштовані для захисту даних власників карток, а також регулярно оновлювати системи. Крім того, організації повинні забезпечити усунення всіх вразливостей і регулярно проводити оцінку безпеки третіми сторонами.

4. Впровадження жорстких заходів контролю доступу

Вимога PCI DSS 7: Обмеження доступу до даних власників платіжних карток.

Вимога 7 стандарту PCI DSS спрямована на забезпечення того, щоб доступ до даних власників платіжних карток був обмежений і надавався лише тим користувачам та системам, які мають обґрунтовану необхідність для виконання

своїх робочих обов'язків. Це є критично важливим для запобігання несанкціонованому доступу до конфіденційної інформації та зниження ризику витоку даних.

Вимога PCI DSS 8: Призначення кожній особі, що має доступ до даних або обладнання, унікального ID-ідентифікатора.

Організації повинні гарантувати, що лише авторизовані користувачі мають доступ до даних власників карток, і що лише авторизований персонал має право отримувати доступ до системи та вносити зміни до них. Також компанії повинні використовувати надійні механізми автентифікації, такі як паролі, цифрові сертифікати, біометрія або токени. Доступ до даних власників карток повинен бути обмежений, і видаватись лише для тих, кому доступ потрібен для виконання своїх обов’язків.

Вимога PCI DSS 9: Обмеження фізичного доступу до даних власників платіжних карток.

Вимога наказує організаціям обмежувати фізичний доступ до даних власників карток шляхом впровадження фізичних заходів безпеки для захисту систем, які зберігають дані власників карток. Це включає обмеження доступу для авторизованого персоналу, використання замків, сигналізації та інших заходів фізичної безпеки.

Банки повинні регулярно контролювати та перевіряти заходи фізичної безпеки, а також контролювати та супроводжувати відвідувачів по своїх приміщеннях.

5. Регулярна перевірка та тестування мережі

Вимога PCI DSS 10: Відстеження та контроль доступу до мережі та даних власників карток.

Банківські установи повинні відстежувати та контролювати всі доступи до мережевих ресурсів і даних власників карток. Це включає відстеження особи користувача, типу доступу, а також дати й часу доступу.

Фінансові установи також повинні створювати журнали подій, які фіксують усі системні дії, пов’язані з обробкою, зберіганням і передачею даних власників карток. Журнали подій необхідно регулярно переглядати та контролювати та зберігати щонайменше один рік. Будь-які винятки або підозрювані порушення даних повинні бути негайно розслідувані.

Вимога PCI DSS 11: Регулярне тестування систем та процесів безпеки.

Організації повинні періодично тестувати свої системи та процеси безпеки на вразливість і проблеми безпеки, а також оцінювати здатність персоналу виявляти і реагувати на інциденти безпеки.

Крім того, організації повинні проводити тести на проникнення, сканування зовнішніх і внутрішніх уразливостей та інші тести, пов’язані з безпекою, щоб допомогти виявити будь-які ризики або слабкі місця в їхній системі.

6. Дотримання політики інформаційної безпеки

Вимога PCI DSS 12: Забезпечення виконання політики інформаційної безпеки.

Організації повинні розробляти та впроваджувати політики безпеки, які включають в себе вимоги стандарту PCI DSS, а також внутрішні правила та процедури. Політики безпеки повинні бути доступними для всіх співробітників та регулярно оновлюватись.

ISO/IEC 27002

ISO/IEC 27002 — це міжнародний стандарт, розроблений для надання рекомендацій щодо найкращих практик з управління інформаційною безпекою. Цей стандарт є частиною сімейства стандартів ISO/IEC 27000, які спрямовані на забезпечення захисту інформаційних активів організацій. ISO/IEC 27002 детально описує заходи безпеки, які можуть бути використані для впровадження, моніторингу, підтримки та покращення СУІБ.

На основі цього стандарту розроблено державний стандарт України ДСТУ ISO/IEC 27002:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки (ISO/IEC 27002:2022, IDT).

У банківській установі впровадження цього стандарту є критично важливим, оскільки банки обробляють величезні обсяги чутливої інформації, включаючи персональні дані клієнтів, фінансові транзакції та комерційну інформацію. ISO/IEC 27002 розроблений для підтримки організацій у захисті їхніх інформаційних активів від загроз і забезпеченні конфіденційності, цілісності та доступності інформації. Стандарт складається з таких основних розділів:

- Політики безпеки інформації
- Організація інформаційної безпеки
- Управління активами
- Безпека людських ресурсів
- Фізична та екологічна безпека
- Управління операціями та комунікаціями
- Контроль доступу
- Розробка та впровадження інформаційних систем
- Управління інцидентами інформаційної безпеки
- Управління безперервністю бізнесу
- Відповідність вимогам.

Основні рекомендації та настанови стандарту ISO/IEC 27002:

- Стандарт рекомендує розробку чітких політик інформаційної безпеки, які визначають принципи та напрямки безпеки в організації. Для банків це означає створення документів, що регламентують обробку фінансових даних, правила надання/ контролю доступу, політики управління інцидентами, політики резервного копіювання даних.
- Банки повинні чітко визначити ролі та відповідальність щодо інформаційної безпеки, створити відповідні комітети або групи для координації заходів безпеки та забезпечити підтримку з боку керівництва.
- Навчання та підвищення обізнаності співробітників щодо інформаційної безпеки є необхідними для зниження ризиків людських помилок та зловмисних дій. Банки повинні проводити регулярні тренінги для персоналу, здійснювати перевірку нових працівників та забезпечувати процедури захисту даних під час звільнення.
- Захист фізичних приміщень та обладнання є важливою складовою загальної стратегії безпеки. Банки повинні контролювати доступ до критичних об'єктів, таких як серверні кімнати, та захищати обладнання від фізичних загроз, таких як пожежі або затоплення.
- Ефективне управління операціями включає захист мереж і комунікацій, контроль за шкідливим програмним забезпеченням, управління змінами та регулярне резервне копіювання даних. Банки повинні впровадити чіткі процедури для моніторингу мереж, виявлення та запобігання інцидентам безпеки.
- Контроль доступу до інформаційних активів повинен бути обмежений лише для уповноважених осіб. Це включає управління правами доступу, впровадження багатофакторної аутентифікації та моніторинг доступу до систем. Важливо забезпечити, щоб доступ до фінансових даних був строго контрольованим та регулярно перевірявся.

- Банки повинні впроваджувати безпечні практики розробки програмного забезпечення, включаючи проведення тестувань на безпеку та захист даних на всіх етапах життєвого циклу інформаційних систем. Це включає аналіз вразливостей, тестування на проникнення та регулярне оновлення систем для захисту від нових загроз.
- Ефективне управління інцидентами включає виявлення, реєстрацію, реагування на інциденти безпеки та аналіз наслідків. Банки повинні мати процедури для швидкого реагування на інциденти, мінімізації їх наслідків та вдосконалення заходів безпеки на основі отриманого досвіду.
- Банки повинні мати процедури для швидкого реагування на інциденти, мінімізації їх наслідків та вдосконалення заходів безпеки на основі отриманого досвіду. Необхідно забезпечувати ефективне управління інцидентами, що включає виявлення, реєстрацію, реагування на інциденти безпеки та аналіз ймовірності потенційних загроз та наслідків у випадках їх реалізації.
- Банки повинні дотримуватись законодавчих і регуляторних вимог, проводити внутрішні та зовнішні аудити інформаційної безпеки та управляти ризиками. Це включає відповідність нормативним актам щодо захисту персональних даних та фінансової інформації.
- Банківські установи повинні розробити детальні політики та процедури інформаційної безпеки, які охоплюють всі аспекти захисту даних. Це включає політики щодо контролю доступу, управління інцидентами, резервного копіювання даних та навчання персоналу.
- Банки повинні використовувати передові технології для захисту своїх інформаційних систем. Це включає використання шифрування для захисту даних, брандмауерів для захисту мереж, систем виявлення

вторгнень та інших інструментів для моніторингу та захисту від кіберзагроз.

- Впровадження процесів управління ризиками є критичним для забезпечення безпеки інформації. Банки повинні ідентифікувати, оцінювати та управляти ризиками, пов'язаними з інформаційною безпекою, а також впроваджувати відповідні заходи для їх мінімізації.
- Банківські установи повинні регулярно проводити навчання та тренінги для своїх співробітників з метою підвищення обізнаності щодо загроз інформаційній безпеці та найкращих практик захисту даних. Це допомагає зменшити ризики, пов'язані з людськими помилками та зловмисними діями.
- Регулярні аудити та моніторинг інформаційних систем є важливими для виявлення та запобігання потенційним загрозам. Банки повинні впроваджувати процедури для постійного моніторингу безпеки своїх систем та проведення аудитів для оцінки ефективності заходів безпеки.

ISO/IEC 27002 є ключовим стандартом для управління інформаційною безпекою, надаючи організаціям структуровані рекомендації щодо захисту їхніх інформаційних активів. Впровадження цього стандарту дозволяє банкам та іншим фінансовим установам ефективно управляти ризиками та забезпечувати безпеку даних [5]. Регулярний моніторинг, оцінка ефективності та вдосконалення заходів безпеки, що базуються на ISO/IEC 27002, сприяють підтримці високого рівня інформаційної безпеки та готовності до сучасних викликів у сфері кібербезпеки.

Постанова НБУ №95

Вимоги щодо забезпечення відповідного рівня інформаційної безпеки у банківській системі України розроблені і рекомендовані для впровадження постановою Національного банку України (НБУ) №95 від 14 грудня 2016 року

"Про затвердження Положення про інформаційну безпеку в банківській системі України.

Дане положення визначає обов'язкові мінімальні вимоги щодо організації заходів з інформаційної безпеки та кіберзахисту у банківській інфраструктурі. Особливо важливими є вимоги, які стосуються принципів управління інформаційною безпекою та вимог до інформаційних систем банку, що взаємодіють з інформаційними ресурсами НБУ [6].

Дана постанова не регламентує фізичну безпеку приміщень банку, використання криптографічних засобів захисту інформації НБУ в інформаційних системах НБУ. Вимоги до цих аспектів визначені відповідними нормативно-правовими актами НБУ. До цього переліку також включається використання хмарних технологій та сервісів у сфері автоматизації.

Основні положення постанови №95 включають в себе:

1. Загальні положення: Визначаються терміни та визначення, що використовуються в контексті інформаційної безпеки в банківській системі України.

2. Організація управління інформаційною безпекою в банківській системі: Встановлюється структура та принципи управління інформаційною безпекою, включаючи розподіл обов'язків та відповідальності.

3. Механізми контролю інформаційної безпеки: Визначаються процедури та заходи, спрямовані на забезпечення відповідного рівня захисту інформації в банківській системі.

4. Управління ризиками інформаційної безпеки: Регламентується процес ідентифікації, оцінки та управління ризиками, пов'язаними з інформаційною безпекою.

5. Вимоги до технічних та організаційних засобів захисту інформації: Зазначаються технічні та організаційні заходи, які мають бути впроваджені для забезпечення інформаційної безпеки в банківській системі.

6. Вимоги до забезпечення безперебійності банківської діяльності: Встановлюються вимоги до резервного копіювання даних та відновлення банківської діяльності в разі виникнення непередбачених ситуацій.

7. Вимоги до організації надання інформації з питань інформаційної безпеки: Регламентуються вимоги до організації та надання інформації щодо інформаційної безпеки в банківській системі.

8. Вимоги до організації проведення аудиту інформаційної безпеки: Встановлюються вимоги до проведення аудитів інформаційної безпеки для перевірки відповідності установленим стандартам та вимогам.

До основних заборон для банківських установ згідно з цією постановою є використання незахищених каналів зв'язку. Тобто банкам заборонено передавати конфіденційну інформацію через незахищені канали зв'язку, такі як електронна пошта без шифрування або неконтрольовані месенджери. Також заборонено зберігати конфіденційну інформацію на незахищених носіях, таких як незашифровані жорсткі диски або флеш-накопичувачі.

Заборонено надавати доступ до інформаційних систем та даних банку особам, які не мають відповідних повноважень та потреби в такому доступі.

Згідно з цією постановою постанови банки повинні використовувати лише програмні продукти, які пройшли перевірку на безпеку та відповідають встановленим вимогам інформаційної безпеки. Банки повинні регулярно оновлювати програмне забезпечення та систем безпеки, особливо ті, що виправляють вразливості.

Ця постанова є важливим інструментом для забезпечення високого рівня інформаційної безпеки в українській банківській системі та допомагає уникнути ризиків, пов'язаних з несанкціонованим доступом до конфіденційної інформації.

2.2 Оцінка ефективності використовуваних підходів щодо забезпечення конфіденційності та цілісності фінансових даних у банківських установах відносно наявних загроз та ризиків

Виконання вимог стандарту PCI DSS є обов'язковим для банківських установ, що працюють з платіжними картками. Дотримання цього стандарту сприяє не лише забезпеченню безпеки даних, але й покращенню репутації банку серед клієнтів та партнерів.

Впровадження вимог PCI DSS значно підвищує рівень конфіденційності даних у банківських установах. Використання шифрування при зберіганні та передачі даних мінімізує ризик перехоплення конфіденційної інформації. Обмеження доступу до даних карток лише уповноваженим особам знижує ймовірність внутрішніх загроз та витоків інформації. Завдяки цим заходам, банківські установи можуть ефективно протидіяти несанкціонованому доступу до конфіденційної інформації.

PCI DSS є обов’язковим для забезпечення високого рівня цілісності фінансових даних. Регулярний моніторинг мережевої активності та проведення тестувань на проникнення дозволяє своєчасно виявляти та усувати вразливості, що можуть призвести до модифікації даних. Політики безпеки та заходи контролю доступу гарантують, що лише авторизовані користувачі можуть змінювати або видаляти дані, знижуючи ризик випадкових чи зловмисних змін.

Використання шифрування та багатофакторної аутентифікації зменшує ризик кібератак, спрямованих на викрадення даних карток. Крім того, вимоги

щодо регулярного оновлення програмного забезпечення та проведення аудиту безпеки допомагають банкам виявляти нові загрози та швидко реагувати на них.

Висновок: використання стандарту повинно призвести до значного зниження кількості інцидентів витоку даних. Ефективне використання заходів безпеки, таких як шифрування даних, багатофакторна аутентифікація та регулярний моніторинг мережі, допомагає запобігти несанкціонованому доступу до даних платіжних карток. Банки, що успішно використовують PCI DSS, менше піддаються штрафам та санкціям з боку регуляторів. Відповідність стандарту також допомагає уникнути юридичних проблем, пов'язаних із захистом даних платіжних карток

Стандарт ISO/IEC 27002 спрямований на допомогу організаціям у розробці, впровадженні та підтримці системи управління інформаційною безпекою [12]. Впровадження цього стандарту в банківських установах є ключовим для забезпечення конфіденційності та цілісності фінансових даних, особливо у контексті сучасних загроз та ризиків.

ISO/IEC 27002 сприяє підвищенню рівня конфіденційності даних у банківських установах через розробку чітких політик інформаційної безпеки та процедур контролю доступу. Визначення ролей і відповідальності допомагає уникнути несанкціонованого доступу до конфіденційних даних. Крім того, регулярні тренінги для персоналу підвищують обізнаність про загрози, зменшуючи ризик витоку інформації через людський фактор.

Управління інцидентами дозволяє швидко реагувати на події, що можуть вплинути на цілісність даних, мінімізуючи наслідки атак або технічних збоїв. Також він допомагає ефективно протидіяти сучасним загрозам завдяки своїм рекомендаціям щодо безпечної розробки програмного забезпечення та регулярного оновлення систем. Стандарт вимагає впровадження багатофакторної аутентифікації та інших заходів для захисту від несанкціонованого доступу та

кібератак, а постійний моніторинг мережевої активності дозволяє своєчасно виявляти та усувати вразливості.

ISO/IEC 27002 передбачає системний підхід до управління ризиками, що включає ідентифікацію, оцінку та управління ризиками, пов'язаними з інформаційною безпекою. Це дозволяє банкам постійно впроваджувати заходи для мінімізації потенційних загроз, що сприяє підвищенню загального рівня безпеки фінансових даних.

Висновок: дотримання вимог стандарту ISO/IEC 27002 у банках є ефективним для забезпечення конфіденційності та цілісності фінансових даних у банківських установах. Він допомагає захистити дані від несанкціонованого доступу та модифікації, протидіяти сучасним загрозам та управлінню ризиками. Банки, що дотримуються рекомендацій ISO/IEC 27002, можуть значно підвищити свій рівень безпеки. Однак, ефективність стандарту залежить від постійного дотримання вимог та регулярного оновлення заходів безпеки у відповідь на нові загрози.

Постанова НБУ №95 спрямована на встановлення мінімальних вимог для організації заходів із забезпечення інформаційної безпеки та кіберзахисту в банківській інфраструктурі України. Вона регулює принципи управління інформаційною безпекою та вимоги до інформаційних систем банків, що взаємодіють з інформаційними ресурсами Національного банку України.

Постанова НБУ №95 підтримує конфіденційність фінансових даних через впровадження чітких політик управління доступом та контролю. Встановлення обмежень на доступ до конфіденційних даних для уповноважених осіб допомагає запобігти несанкціонованому доступу. Регулярні навчання та підвищення обізнаності співробітників сприяють зменшенню ризику людських помилок та зловмисних дій, що можуть призвести до витоку інформації. Впровадження механізмів контролю та моніторингу змін у інформаційних системах дозволяє вчасно виявляти та виправляти порушення цілісності даних. Процедури

управління інцидентами забезпечують швидке реагування на загрози, мінімізуючи потенційні втрати даних. Вимоги постанови щодо захисту інформаційних систем та управління інцидентами допомагають банкам ефективно протидіяти сучасним кіберзагрозам. Регулярні оцінки ризиків та впровадження новітніх технологій захисту дозволяють банкам своєчасно оновлювати свої системи безпеки, зменшуючи вразливість до нових атак.

Висновок: постанова НБУ №95 є ефективним інструментом для забезпечення конфіденційності та цілісності фінансових даних у банківських установах. Ця постанова надає чіткі вимоги та рекомендації щодо організації заходів інформаційної безпеки, що допомагають банкам протидіяти сучасним загрозам та управляти ризиками. Дотримання вимог постанови підвищує рівень безпеки інформаційних систем банків та сприяє підтримці довіри з боку клієнтів та регуляторів.

Впровадження та дотримання стандартів ISO/IEC 27002, PCI DSS та постанови НБУ №95 значно підвищують рівень захищеності фінансових даних у банківських установах, забезпечуючи їх конфіденційність та цілісність. Це створює надійне середовище для обробки та зберігання інформації, сприяючи підвищенню довіри клієнтів до банківської системи.

3 РОЗРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО ПІДВИЩЕННЯ БЕЗПЕКИ ФІНАНСОВИХ ДАНИХ У БАНКІВСЬКИХ УСТАНОВАХ

3.1 Рекомендації щодо підвищення рівня забезпечення конфіденційності та цілісності фінансових даних у банківських установах.

З огляду на стрімкий розвиток сучасних інформаційних технологій, включаючи програмування шкідливих кодів для злому та викрадення даних, а також супутні ризики інформаційної безпеки, питання вдосконалення існуючих форм і засобів захисту інформації в банківських установах залишається актуальним.

За результатами проведеного аналізу програмно-технічних засобів інформаційного захисту даних в інформаційно-комунікаційних системах для підвищення рівня захищеності фінансових даних банківських установ зроблено наступні рекомендації.

1. Провести організаційні заходи у напрямку реєстрації, моніторингу, вивченню і аналізу інцидентів та подій ризику ІБ з метою запобігання втрати даних там, де це відбувається найчастіше.

Необхідно враховувати, що причиною втрати фінансових даних можуть бути не тільки кібератаки, здійснені досвідченими фахівцями. Більшість витоків даних виникає через людські помилки, а не зловмисні дії. Основними причинами цього є злом і поганий рівень безпеки. Погана безпека часто проявляється у випадках, коли дані доступні користувачам у незашифрованому вигляді та зберігаються в незахищеній базі даних без необхідної автентифікації.

Деяка частина даних втрачається через збої, яких можна уникнути за допомогою автоматизованих засобів захисту, що запобігають необдуманим діям

обслуговуючого персоналу, відповідального за технічну підтримку інформаційних та комунікаційних систем.

При розробці стратегії безпеки важливо включити організаційні заходи, що запобігають несанкціонованому доступу, а також забезпечити програмно-апаратний захист даних від навмисного несанкціонованого доступу.

2. Банку необхідно враховувати всі можливі джерела витоку даних

Необхідно встановлювати сучасні антивірусні, захисні від шкідливих програм рішення на кінцевих точках елементів IT-інфраструктури та проводити своєчасно процедури оновлення баз сигнатур антивірусного програмного забезпечення.

Враховувати всі потенційні джерела витоку даних, в тому числі такі, як веб-інтерфейси та типові дії на кінцевих точках з'єднання - спілкування в чатах, засобами електронної пошти, в тому числі під час публікації інформації в соціальних мережах або використання USB-накопичувача для переміщення даних.

Необхідно застосовувати превентивні заходи захисту інформації та суворі правила доступу до інформації, використовувати спеціалізовані апаратні та програмні засоби контролю вхідного та вихідних трафіків даних, в тому числі переданих мережею Інтернет, аналізувати та відфільтровувати дані, що передаються через програми обміну повідомленнями, електронну пошту та підключені пристрої. Банківська установа повинна забезпечити придбання і впровадження сучасних технологій захисту IT-інфраструктури від витоку даних через фішинг, відкриті мережеві порти, незахищені IP-адреси, від вірусів та зловмисних програмних кодів (трояни).

3. Впровадити моніторинг усіх потенційних джерел конфіденційної інформації

Моніторинг усіх потенційних джерел конфіденційної інформації є критично важливою складовою стратегії забезпечення інформаційної безпеки в банківських установах, що конфіденційна інформація не завжди зосереджена в одному джерелі.

Для моніторингу захищеності мережі, банківським установам необхідно використовувати рішення, яке називається SIEM (Security Information and Event Management), воно буде збирати в собі всі отримані дані, від систем безпеки. Розглянемо SIEM систему QRadar від компанії IBM.

Використання QRadar в банківській інфраструктурі може допомогти забезпечити безпеку та моніторинг подій. Він допомагає збирати та аналізувати дані з різних джерел, включаючи системні журнали, мережеві пристрої та додатки, це дозволить банку мати централізований огляд та контроль над подіями безпеки в реальному часі. QRadar використовує розуміння загроз та аналіз поведінки для виявлення підозрілої або відхиленої активності, він використовує алгоритми машинного навчання та правила для виявлення аномальних подій, таких як кібератаки, вторгнення або незвичайні зміни в системі [9].

QRadar інтегрується зі системами сканування вразливостей для отримання актуальної інформації про потенційні слабкі місця в інфраструктурі банківської установи. Такий метод допомагає ідентифікувати вразливості та приймати заходи для їх усунення, зменшуючи ризик вторгнень.

SIEM система допомагає банкам автоматизувати процес реагування на події безпеки. Вона може генерувати автоматичні сповіщення, запускати реакції на певні події та спрямовувати їх на відповідні команди або системи для подальшого розслідування та реагування на інциденти.

IBM QRadar допомагає банкам виконувати різні нормативні вимоги щодо безпеки, такі як вимоги PCI DSS або вимоги регуляторних органів. Він надає

засоби для моніторингу та звітності, що полегшує аудит та документування відповідності. Система інтегрується з іншими безпековими системами та інструментами, такими як системи управління інцидентами, системи управління подіями, системи виявлення вторгнень та інші. Це дозволяє банку отримати цілісну систему безпеки зі збільшеною ефективністю та розширеними можливостями [8]. Використання QRadar у банківській інфраструктурі допомагає забезпечити раннє виявлення та моніторинг загроз.

4. Банки повинні впровадити засоби шифрування скрізь, де це технічно можливо реалізувати

Якщо 20 років тому шифрування інформації вважалося рідкісним явищем і асоціювалося лише з передачею секретів, то настала епоха переносимості даних (data portability), коли майже кожна передача даних шифрується. Наприклад, більшість веб-сторінок, які сьогодні відвідують користувачі, використовують з'єднання SSL/TLS (HTTPS), які гарантують, що ніхто не зможе прослуховувати зв'язок між браузером і веб-сайтом або веб-додатком [16]. Сервери електронної пошти взаємодіють один з одним, і багато платформ обміну миттєвими повідомленнями застосовують шифрування і навіть дозволяють надсилати повідомлення з обмеженим терміном зберігання, надаючи можливість автоматичного стирання після вибраного проміжку часу. Проте, хоча і всі ці механізми доступні, багато хто їх не застосовує. Не кожен веб-сайт дозволяє лише безпечні з'єднання, багато хто все ж таки дозволяє використовувати незашифровану передачу даних. Вміст електронної пошти майже ніколи не шифрується, і є відомі платформи обміну повідомленнями, які довіряють стороннім каналам зв'язку для обробки шифрування. Тому слід застосовувати шифрування скрізь, де це можливо, особливо якщо є підозра, що будь-яка конфіденційна інформація може бути включена до збору даних.

5. Впровадити систему централізованого управління обліковими даними

Впровадження системи централізованого управління обліковими даними наприклад, на базі технології Oracle Identity Manager дозволить підвищити ефективність управління та контролю доступу користувачів до основних інформаційних систем банку.

Oracle Identity Manager (OIM) - це інтегрована система управління ідентифікацією та доступом (IAM), розроблена корпорацією Oracle. OIM дозволить банкам та іншим організаціям ефективно керувати ідентифікацією користувачів, їх доступом до різних ресурсів і даних, а також автоматизувати процеси управління цими ідентифікаціями та доступом.

OIM дозволить автоматизувати процеси створення, зміни та видалення облікових записів користувачів. Це дозволяє банкам ефективно керувати доступом співробітників до систем та додатків на різних етапах їхньої кар'єри. Також він дозволяє організаціям встановлювати ролі та привілеї для користувачів на основі їхніх обов'язків та функціональної області, що допоможе забезпечити принцип найменшого можливого доступу і уникнути надмірного доступу до чутливих даних [14].

Впровадження системи OIM надасть можливість автоматизувати багато рутинних завдань, пов'язаних з управлінням ідентифікацією та доступом, що допоможе підвищити ефективність та знизити ризики людських помилок.

У загальному, Oracle Identity Manager допомагає банкам забезпечити безпеку, ефективність та відповідність в управлінні ідентифікацією та доступом, що стає все важливішим у сучасному цифровому світі.

5. Налаштувати брандмауери

NGFW (Next-Generation Firewall)- це є тип мережевого пристрою, який використовується для захисту комп'ютерних мереж від різних кіберзагроз. Він проводить глибокий аналіз мережевого трафіку на рівні сесій, додатків і

протоколів та використовує розуміння контексту додатків для виявлення та блокування небезпечних дій, включаючи використання шкідливих програм та передачу конфіденційної інформації.

NGFW дозволяє налаштовувати правила доступу на основі різних параметрів, таких як IP-адреси, порти, протоколи, а також ідентифікує користувачів та їхні ролі для забезпечення відповідності політиці безпеки [15]. Фаерволл використовує різноманітні методи для виявлення та блокування загроз у реальному часі, такі як антивірусні програми, інтелектуальні системи виявлення вторгнень (IPS), захист від шкідливих URL-адрес .

Брандмауер може бути легко інтегрований з іншими системами безпеки, такими як SIEM, що дозволяє організаціям забезпечити централізоване управління та моніторинг безпеки мережі. Також NGFW може аналізувати мережевий трафік та створювати звіти про потенційні загрози та вразливості.

Для захищеності банківських web-застосунків потрібно використовувати рішення класу WAF (Web application firewall). F5 WAF є одним з високопродуктивних рішень для захисту веб-додатків в банківських установах.

F5 WAF- це рішення, розроблене компанією F5 Networks, яке призначене для захисту веб-додатків від різноманітних кіберзагроз. Основна мета F5 WAF полягає в запобіганні та виявленні атак на веб-додатки, таких як SQL-ін'єкції, перехоплення сесій, XSS (Cross-Site Scripting) та інші, які можуть призвести до компрометації інформації або порушення їх цілісності [7].

Основні функції F5 WAF включають:

1. Виявлення та блокування небезпечних запитів, що надходять до веб-додатків, перед тим як вони досягнуть сервера;
2. Моніторинг веб-трафіку для виявлення підозрілих або відхилення запитів;

3. Впровадження заходів для запобігання та пом'якшення DDoS-атак, які можуть спричинити відмову в обслуговуванні;
4. Виявлення та блокування атак на рівні додатків, таких як SQL-ін'єкції та XSS;
5. Можливість створювати та налаштовувати правила відповідно до конкретних потреб та характеристик веб-додатків.

Використання F5 WAF дозволяє організаціям захистити свої веб-додатки від різноманітних загроз, забезпечуючи надійний рівень безпеки та захист від потенційних кібератак.

7.Ввести обов’язкове резервне копіювання

Резервне копіювання - це процес створення копій важливих даних з метою їх подальшого відновлення в разі втрати, пошкодження або видалення оригінальних даних. Основна мета резервного копіювання полягає в забезпеченні безпеки і надійності інформації, зменшенні ризику втрати даних та можливості їх відновлення в разі потреби. Далі ми розглянемо рішення IBM Backup, що дозволить банківським установам робити резервне копіювання даних.

IBM Backup - це набір продуктів та послуг компанії IBM, спрямованих на забезпечення резервного копіювання і відновлення даних для підприємств будь-якого розміру. Основні компоненти IBM Backup включають у себе різноманітні програмні рішення, апаратне забезпечення, облікові записи для хмарних та гібридних рішень резервного копіювання[13].

IBM Backup надає можливість регулярного та автоматизованого резервного копіювання даних з різних джерел, таких як сервери, робочі станції, бази даних тощо. Платформа дозволяє швидко і ефективно відновлювати дані в разі випадків аварійного знищення, випадкового видалення або інших негативних сценаріїв.

Крім традиційного резервного копіювання на місці, IBM Backup також пропонує рішення для зберігання резервних копій в хмарних сервісах, що дозволить зменшити витрати на обладнання та підвищити доступність даних.

Резервне копіювання може бути реалізоване як локально на пристрої для зберігання даних, так і в хмарних сервісах. Використання ефективних стратегій резервного копіювання дозволяє організаціям забезпечити безпеку та доступність їх важливих інформаційних ресурсів.

3.2 Побудова стратегії та опис практичних кроків з впровадження розроблених рекомендацій.

Побудова стратегії та опис практичних кроків з впровадження розроблених рекомендацій є критично важливими для забезпечення ефективної інформаційної безпеки в банківських установах. Стратегія має базуватися на всебічному аналізі поточних загроз і ризиків, враховувати сучасні стандарти та нормативні вимоги. Практичні кроки впровадження включають розробку та оновлення політик безпеки, впровадження передових технологічних рішень та навчання персоналу. Такий підхід забезпечить захист конфіденційності та цілісності фінансових даних, знизить ризики несанкціонованого доступу та підвищить загальний рівень кібербезпеки установи.

Першим кроком у розробці стратегії інформаційної безпеки є проведення детального аналізу поточних загроз і ризиків. Це включає ідентифікацію потенційних векторів атак, оцінку ймовірності їх реалізації та визначення можливих наслідків для банківських установ. Використання таких методологій, як оцінка ризиків та аналіз вразливостей, дозволяє створити надійну основу для подальших дій.

Також для забезпечення високого рівня захисту фінансових даних банкам необхідно впроваджувати сучасні технологічні рішення. Це включає використання багатофакторної автентифікації, IDS, засоби шифрування даних на різних рівнях, а також технології для захисту мережевої інфраструктури. Важливо також регулярно оновлювати програмне забезпечення та системи безпеки для запобігання експлуатації нових вразливостей.

Одним з організаційних заходів з впровадження і дотримання норм інформаційної безпеки є оперативне і планове навчання фахівців служб безпеки банківської установи. В Банку на постійній основі повинно проводиться тренування щодо відпрацювання заходів Плану реагування на кіберзагрози під час перевірки ефективності заходів щодо захисту периметра мережі Банку шляхом виконання періодичних тестів на проникнення та захищеності мереж і систем, перегляд налаштувань параметрів безпеки.

З метою попередження кіберінцидентів підрозділи УІБ та ДІС на постійній основі повинні здійснювати наступні превентивні заходи:

- оновлення баз системи захисту від зловмисного коду;

- оновлення спеціалізованого програмного забезпечення;

- налаштування політики доступу до мережі Інтернет та до інформаційних систем банку;

- моніторинг подій ІБ;

- навчання працівників.

Всі працівники банку мають бути відповідальними за своєчасне повідомлення про інциденти ІБ до служби управління інформаційної безпеки, а також, у разі потреби, за допомогу у визначенні та впровадженні рішення щодо обробки таких подій. Бажано внутрішніми політиками з ІБ передбачити, щоб усі

відповідальні працівники Банку мали змогу і відповідні програмні інструменти для :

-фіксації подробиць подій та належним чином зберігати матеріали, інформацію та носії інформації, що можуть вказувати на кіберінцидент;

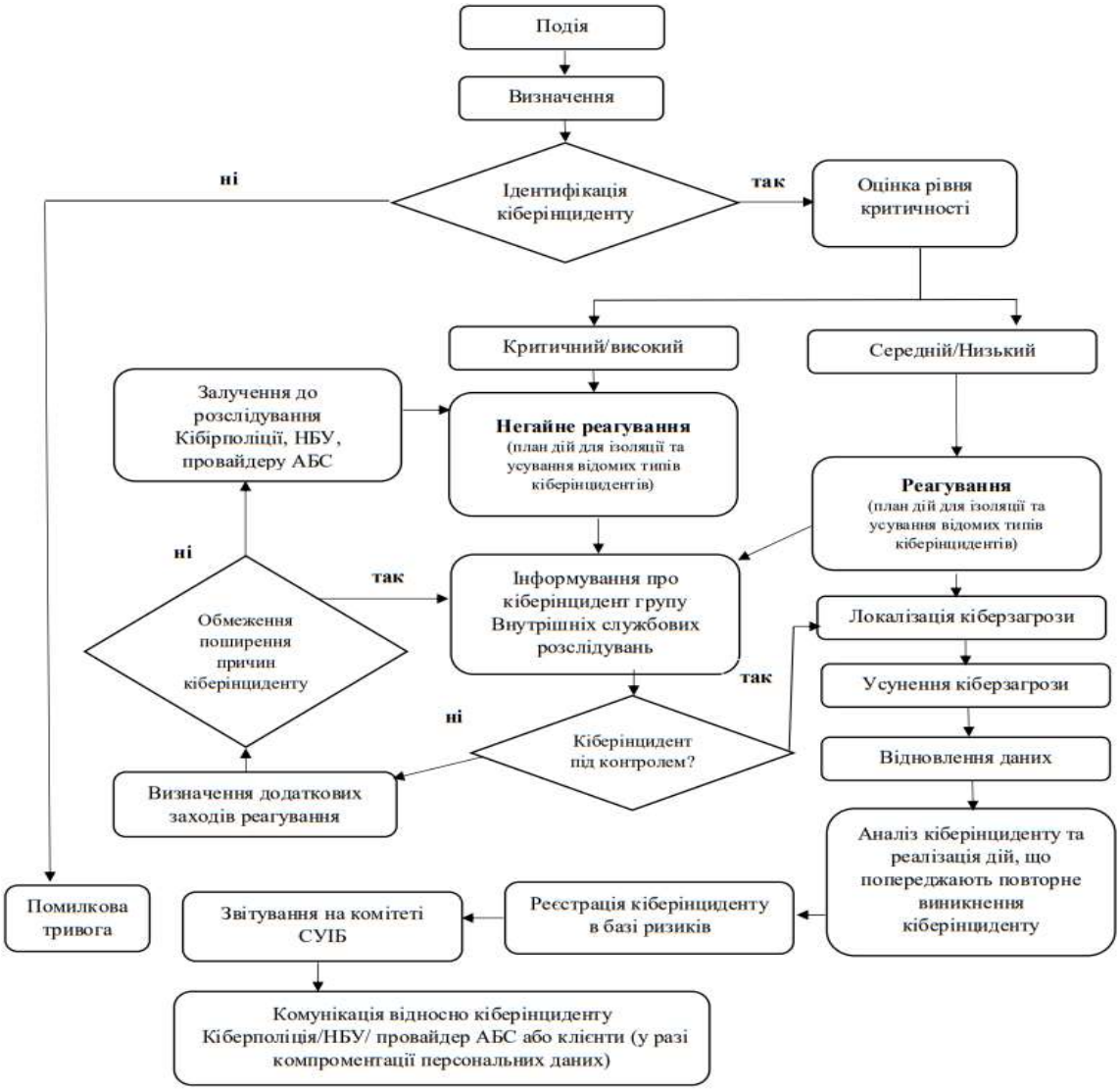
-повідомлення про всі виявлені кіберінциденти своєму безпосередньому керівнику та Управлінню інформаційної безпеки та Управління ризик-менеджменту;

-вживання усіх можливих заходів безпеки з метою запобігання Банку від кіберінцидентів.

План реагування на кіберзагрози дозволяє організації бути підготовленою до можливих інцидентів, це допоможе зменшити час реагування та мінімізувати наслідки. Оперативне реагування на загрози допоможе захистити конфіденційну інформацію, запобігаючи її втраті або несанкціонованому доступу. План реагування на кіберзагрози є критично важливим інструментом для будь-якої організації, яка прагне захистити свої інформаційні активи, зберегти фінансову стабільність та підтримувати репутацію на ринку. Він забезпечує структурований підхід до управління інцидентами, допомагаючи швидко виявляти, реагувати та відновлюватися після кіберзагроз, з мінімальними втратами та максимальним збереженням безпеки даних.

Основна відповідальність за написання плану лежить на команді ІБ, вона повинні мати глибокі знання у сфері кіберзагроз, засобів захисту та реагування. Контроль та перевірку стану виконання вимог Плану реагування на кіберзагрози має здійснювати управління інформаційної безпеки та Керівний орган СУІБ. Докладний план реагування наведений у схемі 1.

Схема 1.- План реагування на кіберзагрози, кібератаки та кіберінциденти



Кожен з цих етапів є критичним для забезпечення ефективного реагування на кіберінциденти і мінімізації їх впливу на організацію. Регулярний перегляд і вдосконалення плану реагування на інциденти допомагає організаціям бути краще підготовленими до можливих кіберзагроз.

Реагування на кіберзагрози, кібератаки та кіберінциденти, а також визначення відповідальних працівників банку за заходи реагування здійснюються в послідовності вказаній у Додатку Б .

Відповідно до виявлених загроз і ризиків, банківським установам необхідно розробити або оновити існуючі політики безпеки. Ці політики мають чітко визначати процедури та правила щодо захисту інформації, включаючи управління доступом, використання криптографічних засобів, моніторинг та реагування на інциденти. Політики безпеки повинні бути зрозумілими та доступними для всього персоналу.

Впровадження системи моніторингу у банківську інфраструктуру для виявлення та швидкого реагування на інциденти безпеки буде невід'ємною частиною стратегії. Це включає впровадження SIEM системи, яка збирає і аналізує дані з різних джерел для виявлення підозрілої активності. Департаментам ІБ також важливо також розробити чіткий план дій на випадок інциденту, включаючи процедури інформування, ізоляції загроз та відновлення роботи систем.

Реалізація цих стратегій та практичних кроків дозволить банківським установам значно підвищити рівень інформаційної безпеки, знизити ризики витоку конфіденційної інформації та забезпечити стабільну та надійну роботу своїх інформаційних систем.

ВИСНОВКИ

У даній дипломній роботі було проведено детальне дослідження шляхів забезпечення конфіденційності та цілісності фінансових даних у банківських установах. В процесі дослідження було виявлено важливість забезпечення конфіденційності та цілісності фінансових даних у банківських установах для забезпечення довіри клієнтів та ефективного функціонування фінансової системи.

Було проаналізовано сучасні методи та засоби, які використовуються для захисту фінансових даних. Зокрема, досліджено криптографічні алгоритми, методи автентифікації та шифрування даних, а також програмно-апаратні засоби захисту.

Вивчено поняття банківської таємниці, та які банківські операцій, категорії і групи інформації відносяться до банківської таємниці.

Проаналізовано існуючі загрози для конфіденційності та цілісності фінансових даних у банківських установах. Виявлено основні види загроз, включаючи внутрішні та зовнішні атаки, людські помилки, технічні збої та зловмисні дії.

Було розглянуто основні міжнародні та національні стандарти і нормативні документи, такі як PCI DSS, ISO/IEC 27021 та постанова НБУ №95.

Проаналізувавши вимоги та рекомендації стандартів PCI DSS та ISO/IEC 27002, було визначено основні напрями, які мають бути враховані для побудови ефективної системи захисту фінансових даних.

Стандарти PCI DSS та ISO/IEC 27002 охоплюють різні аспекти інформаційної безпеки, такі як управління доступом, захист мережевої інфраструктури, моніторинг та реагування на інциденти. PCI DSS надає чіткі інструкції щодо захисту даних власників платіжних карток, що є критично важливим для банківських установ, які обробляють такі дані. Впровадження цього стандарту допомагає мінімізувати ризики, пов'язані з фінансовими шахрайствами.

Виконання вимог цих стандартів дозволяє банківським установам суттєво знизити ризики витоку конфіденційної інформації та підвищити загальний рівень захищеності фінансових даних.

Постанова НБУ №95 регламентує обов'язкові мінімальні вимоги щодо організації заходів із забезпечення інформаційної безпеки та кіберзахисту в банківській інфраструктурі України. Вона акцентує увагу на необхідності створення ефективних механізмів управління інформаційною безпекою, забезпечення відповідного рівня захищеності інформаційних систем та дотримання нормативних вимог. Виконання положень цієї постанови допоможе підвищити стійкість банківських установ до кіберзагроз та забезпечить відповідність національним регуляторним вимогам.

На основі проведеного аналізу, у роботі розроблено рекомендації для банківських установ щодо підвищення рівня захищеності конфіденційності та цілісності фінансових даних. Запропоновано заходи для підвищення рівня безпеки, включаючи впровадження нових технологій, підвищення обізнаності персоналу та вдосконалення організаційних заходів. Основні рекомендації включають в себе розробку та впровадження чітких політик і процедур, що регулюють обробку та захист фінансових даних, встановлення захисту для кожного типу активів, включаючи бази даних клієнтів та системи обробки платежів.

Регулярні тренінги та підвищення обізнаності співробітників щодо інформаційної безпеки, впровадження багатофакторної аутентифікації та моніторингу для систем з обмеженим доступом також допоможе підвисити рівень захищеності банківської установи.

Було розроблено рекомендації щодо підвищення захищеності конфіденційності та цілісності фінансових даних у банківських установах. Завдяки сучасним технологіям захисту інформації, таким як шифрування, брандмауери, системи виявлення вторгнень, інструменти для моніторингу та

захисту від кіберзагроз були надані надійні рекомендації для збереження даних у банківських установах.

Впровадження цих рекомендацій допоможе банківським установам значно підвищити рівень захищеності конфіденційної та цілісної інформації, зменшити ризики кіберзагроз і ризики витоків інформації та забезпечити відповідність нормативним вимогам. Це, у свою чергу, сприятиме зміцненню довіри клієнтів до банківських послуг та підвищенню загальної стійкості фінансової системи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" (№ 80/94-ВР від 5 липня 1994 року)/ URL: https://ips.ligazakon.net/document/z008000?an=4711&ed=2020_06_04
2. Закон України «Про банки та банківську діяльність» URL: https://zakon.rada.gov.ua/laws/show/2121-14#Text
3. What Are the 12 Requirements of PCI DSS? URL: https://reciprocity.com/blog/what-are-the-12-requirements-of-pci-dss/
4. What are the 12 requirements of PCI DSS compliance? URL: https://www.itgovernanceusa.com/the-12-requirements-of-the-pci-dss
5. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту системи управління інформаційною безпекою. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66910
6. Постанова НБУ № 95 "Про затвердження Положення про захист інформації та кібербезпеку в банківській системі України" (від 28 серпня 2018 року). URL:: https://zakon.rada.gov.ua/laws/show/v0095500-17#Text
7. Що таке WAF наступного покоління? URL: https://www.megatrade.ua/news/reviews/shcho-take-waf-nastupnogo-pokolinnya/
8. IBM documentation. URL: https://www.ibm.com/products/qradar-siem
9. IBM QRadar Security Intelligence Platform URL: https://spro.com.ua/desitions/siem/ibm-qradar-security-intelligence-platform
10. Стаття 60 Закону України “Про банки та банківську діяльність” URL: https://zakon.rada.gov.ua/laws/show/2121-14#Text
11. Інформаційна безпека банків: шляхи розв’язання проблеми. URL: https://journal.bank.gov.ua/archive/2010/5.pdf#page=3
12. ЗВІД ПРАВИЛ ДЛЯ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ (ISO/IEC 27002:2005, MOD. URL: https://s-byte.com/useful/27002.pdf
13. IBM Backup Solutions URL: https://www.cloudfirst.host/ibm-backup-solution/

14. Oracle Identity Manager. URL: https://erc.ua/erc-reviews/17792/oracle-identity-management
15. NGFW: What is a next-generation firewall URL: https://www.cloudflare.com/learning/security/what-is-next-generation-firewall-ngfw/
16. 5 рекомендацій щодо захисту та конфіденційності даних користувачів URL:https://corewin.ua/blog/recommendations-for-user-data-protection-and-data-privacy/

ДОДАТКИ

Додаток А: Таблиця 1- Перелік категорій кіберінцидентів

№ №	Категорія інциденту	Тип інциденту	Опис типу інциденту
11	Шкідливий вміст	Спам	Надсилання небажаних повідомлень або великої кількості повідомлень
22	Шкідливий програмний код	Зараження зловмисним кодом (Malware)	У системі виявлено шкідливе програмне забезпечення
		Розповсюдження шкідливого ПЗ	Розповсюдження шкідливого програмного забезпечення, наприклад шляхом розсилки повідомлень електронної пошти, що містять вкладення з зловмисний кодом або посилання на його завантаження
33	Збір інформації зловмисником	Сканування	Збір інформації про системи або мережі
		Фішинг (Phishing)	Спроба збору інформації про користувача чи систему за допомогою масової розсилки електронною поштою спрямованою на збір даних, що може містити посилання на фішингові сайти
44	Спроби втручання	Спроба авторизації в систему(Login	Спроба входу до служб доступу. Невдала спроба підбору

		attempts)	автентифікаційних даних чи використання вже не актуальних даних
55	Втручання	Компрометація облікового запису (Account compromise)	Фактичне вторгнення в систему або мережу шляхом компрометації облікового систему шляхом запису користувача
		Компроментація системи (System compromise)	Фактичне вторгнення в систему чи її сервіс або застосунок через використання вразливості в мережі. Несанкціонований доступ до системи в обхід системи контролю доступу
66	Порушення доступності (Availability)	DoS/DDoS	Вплив на нормальне функціонування системи, що досягається направленням з одного чи багатьох джерел до цільового ресурсу запитів для перенасичення пропускної здатності чи системних ресурсів
		Шкідливі дії	Дії, спрямовані на пошкодження системи, переривання процесів, зміну або видалення інформації тощо
		Збій	Збій в роботі системи без зловмисного втручання
77	Порушення властивостей	Несанкціонований доступ до інформації	Несанкціонований доступ до інформації. Несанкціонований

	інформації		обмін конкретним набором інформації
		Несанкціонована модифікація	Несанкціонована зміна або видалення певного набору інформації
88	Шахрайство	Шахрайський сайт	Створення фішингових сайтів для збору автентифікаційних чи інших даних користувачів

Додаток Б: Таблиця 2- Етапи реагування на кіберінциденти

№№	**Етапи реагування**	**Заходи реагування**	**Відповідальний**
11	Виявлення та ідентифікація кіберінциденту	● ідентифікація порушених кіберінцидентом ресурсів та систем	Підрозділ ІБ
		● визначення можливих наслідків від кіберінциденту	Підрозділ ІБ
		● повідомлення підрозділу ІБ та підрозділу ризик-менеджменту про кіберінцидент	Підрозділ, що виявив
22	Початкове реагування	● фіксування основних деталей подій, які супроводжують інцидент;	Підрозділ ІБ

		● збір інформації; ● аналіз log-файлів в інформаційній системі; ● вибір стратегії реагування; ● попередня оцінка кіберінциденту	
33	Визначення заходів реагування	● з урахуванням попередньої оцінки кіберінциденту, визначення конкретних дій реагування, які повинні базуватися на всіх відомих фактах інциденту	Підрозділ ІБ Правління Банку (у разі критичного рівня)
44	Обмеження поширення, усунення причин і наслідків кіберінциденту	● відключення інфікованої системи або ресурсів від локально-обчислювальної мережі; ● видалення будь-яких прихованих зловмисних програм або каталогів, доданих зловмисником, чи розгорнутого зловмисного програмного коду, включаючи повне видалення всіх програм і файлів системи, якщо це необхідно; ● оновлення вірусних сигнатур засобів захисту від	Підрозділ ІБ Служба відповідальна за інформаційні системи

		шкідливого коду; ● усунення уразливості, що спричинила кіберінцидент; ● забезпечення відновлення системи з оптимальною конфігурацією безпеки	
55	Розслідування кіберінциденту	● збір та аналіз усіх даних щодо кіберінциденту; ● за необхідності ініціювання питання щодо залучення до розслідування правоохоронних органів	Підрозділ ІБ Служба відповідальна за інформаційні системи
66	Звітування про кіберінцидент	● складання детального звіту про розслідування кіберінциденту: причини, наслідки, пропозиції щодо уникнення в майбутньому	Підрозділ ІБ
77	Аналіз кіберінциденту та реалізація дій що попереджають повторне виникнення кіберінциденту	● визначення джерела зловмисного коду або атаки; ● оцінка витрачених затрат на усунення кіберінциденту (час та кошти); перегляд та удосконалення системи захисту банку	Підрозділ ІБ
88	Повідомлення про	● для реєстрації кіберінциденту працівник	Працівник Підрозділу ІБ

	кіберінцидент	підрозділу ІБ, у найкоротший термін, повинен надати інформацію щодо кіберінциденту службу операційних ризиків банку	
09	Реєстрація кіберінциденту	● внесення інформації про кіберінцидент до Бази подій операційного ризику	Служба банку з операційних ризиків

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)