Міністерство освіти і науки України

«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій

Кафедра кібербезпеки та захисту інформації

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційна робота магістра

галузь знань	*12 Інформаційні технології*
	(шифр і назва галузі знань)
спеціальність	*125 Кібербезпека*
	(код і назва спеціальності)
освітній ступень	*магістр*
	(назва освітньої програми)
освітньо-наукова програма	*Кібербезпека*

на тему: «Методи забезпечення безпеки у банківській інфраструктурі»

Виконавець: студент ІІ курсу, групи КБм-21

Максим ЖАРОНКІН

(підпис) (Ім'я, ПРІЗВИЩЕ)

	Ім'я, ПРІЗВИЩЕ	**Підпис**
Науковий керівник	Сергій ТОЛЮПА	
Нормоконтроль	Юрій ЩЕБЛАНІН	

Київ 2023

Міністерство освіти і науки України

«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій

Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____ Сергій ТОЛЮПА
«24» жовтня 2022 р.

ЗАВДАННЯ

на виконання кваліфікаційної роботи

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

освітній ступень *магістр*

Здобувача КБм-21 (група) Жаронкін Максим Юрійович (прізвище ім'я по-батькові)

Тема дипломної роботи Методи забезпечення безпеки у банківській інфраструктурі

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол № 3 від 20.10.2022

2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень	Процес забезпечення безпеки у банківській інфраструктурі
Предмет досліджень	Процес захисту об'єктів банківської інфраструктури.
Мета	Досягнення підвищення ефективності систем безпеки у банківській інфраструктурі шлях розробки методів захисту інформаційного простору банку.
Вихідні дані для проведення роботи	Методи захисту інформаційної безпеки банківських установ.

3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна	Формування комплексної рекомендації для банківських установ у сфері інформаційної безпеки.
Практична цінність	Покращення ефективності роботи інформаційної безпеки банку.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Робота виконана у повному обсязі відповідно до теми.

5. ЕТАПИ ВИКОНАННЯ РОБОТИ

Найменування етапів робіт	**Строки виконання робіт (початок-кінець)**
Розробка плану для досягнення мети роботи	24.10.2022 – 22.01.2023
Аналіз літературних джерел	23.01.2023 – 15.02.2023
Розробка пропозицій для покращення ефективності систем інформаційної безпеки	16.02.2023 – 23.04.2023
Оформлення і друк пояснювальної записки	24.04.2023 – 19.05.2023

6. РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект	Оптимізація витрат на побудову інформаційної безпеки
Соціальний ефект	Підвищення ефективності систем інформаційної безпеки для банків різного розміру.

7. ДОДАТКОВІ ВИМОГИ

Завдання видав _____ Сергій ТОЛЮПА

(підпис) (Ім'я, ПРІЗВИЩЕ)

Завдання прийняв

до виконання _____ Максим ЖАРОНКІН

(підпис) (Ім'я, ПРІЗВИЩЕ)

Дата видачі завдання: 24.10.2022 р.

Термін подання кваліфікаційної роботи до ЕК 19.05.2023 р.

УДК. 004.432.16

РЕФЕРАТ

Пояснювальна записка до дипломної роботи «Методи забезпечення безпеки у банківській інфраструктурі»: 70 сторінок загального тексту, 2 рисунки та 24 літературних джерела.

Об’єктом дослідження є процес забезпечення безпеки у банківській інфраструктурі.

Предметом дослідження в даній роботі є процес захисту об’єктів банківської інфраструктури.

Метою даної роботи є досягнення підвищення ефективності систем безпеки у банківській інфраструктурі шлях розробки методів захисту інформаційного простору банку.

Наукова новизна: запропоновано метод побудови безпеки гібридної системи банківської інфраструктури.

Результати роботи можуть використовуватися для побудови ефективної системи безпеки у банках різних масштабів.

У роботі проаналізована існуюча література та нормативно-правова база, що регламентує інформаційну безпеку банківської інфраструктури.

Ключові слова: безпека банківської інфраструктури, PCI DSS, ISO/IEC 27002, Постанова НБУ №95, кібербезпека.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

СУІБ	Система управління інформаційною безпекою
ІБ	Інформаційна безпека
НБУ	Національний Банк України
ІзОД	Інформація з обмеженим доступом
ІТ	Information Technology
КСВ	Корпоративна соціальна відповідальність
ОС	Операційна система
БД	База даних
ПЗ	Програмне забезпечення
VoIP	voice over IP
NTP	Network Time Protocol
DNS	Domain Name System
ПК	Персональний комп’ютер
ІС	Інформаційна система
WAF	Web application firewall
ЦСК	Центр сертифікації ключів
DLP	Data loss prevention
IDM	Identity and access management
HR	Human research

ЗМІСТ

ВСТУП

Актуальність даної роботи визначається тією обставиною, що масштабні атаки на банківський сектор мають місце ледве не кожного тижня з початку 2022 року з метою кібернетичної боротьби з Україною, аби взяти під контроль системи управління банківської інфраструктури країни або зупинити її роботи на довгий час.

Росія розпочала найбільш активні військові проти України 24 лютого 2022 року, але, нажаль, російські кібератаки проти України тривають із моменту незаконної анексії Росією автономної республіки Крим у 2014 році, посилившись безпосередньо перед повномасштабним вторгненням у 2022 році. За інформацією з відкритих джерел в цей період найбільше постраждали державно-адміністративний, енергетичний, медійний, фінансовий, бізнес та некомерційний сектори України. Починаючи з 24 лютого поодинокі та групові російські кібератаки значно ускладнили розподіл медикаментів першої необхідності , харчових продуктів та надзвичайної допомоги серед населення країни. Організації та уряди в усьому світі не залишилися байдужими до ризиків, що пов'язані з цією зловмисною активністю. За лідерством країн Європейського Союзу, США та НАТО реалізуються ініціативи, спрямовані на нейтралізацію кіберзагроз та захист життєво важливої інфраструктури України. У рамах цих ініціатив ЄС активізував роботу своїх команд швидкого реагування на кіберінциденти для посилення кібероборони нашої країни. Різні неурядові та приватні структури підтримують Україну та в якості допомоги проводять різні заходи для досягнення більшого рівня кіберстійкості. Незалежні хакерські групи (наприклад, Anonymous) від початку вторгнення здійснили значну кількість контратак, які вразили державно-управлінську, фінансову та медійну системи російської федерації. Європейський парламент на початку вторгнення виступив із закликом посилити допомогу Україні у сфері кібербезпеки та в повній мірі використовувати усі наявні важелі для введення ще більш жорстких кіберсанкцій ЄС проти осіб, організацій та установ, відповідальних за різні кібератаки

на Україну або причетних до них. Одним з проявів підтримки України стало приєднання до Центру НАТО з питань співробітництва в галузі кіберзахисту (CCDCOE) 16 травня 2023 року.

Метою даної роботи є досягнення підвищення ефективності систем безпеки у банківській інфраструктурі шлях розробки методів захисту інформаційного простору банку.

Для досягнення поставленої мети необхідно вирішити такі *завдання*:

- проаналізувати існуючу вітчизняну та міжнародну нормативно-правову базу що регламентую банківську безпеку;
- проаналізувати наявні методи забезпечення безпеки у банківській інфраструктурі;
- розробити рекомендації, щодо побудови гібридної, відмовостійкої та захищеної системи у банківській установі.

Об'єктом дослідження є процес забезпечення безпеки у банківській інфраструктурі.

Предметом дослідження в даній роботі є процес захисту об'єктів банківської інфраструктури.

Наукова новизна: запропоновано метод побудови безпеки гібридної системи банківської інфраструктури.

Методи дослідження у кваліфікаційній магістерській роботі:

- аналіз літератури;
- аналіз методів, що застосовуються в банківських установах;
- порівняння існуючих методів;
- вивчення та узагальнення вітчизняної і зарубіжної практики.

Апробація результатів роботи та публікації за темою кваліфікаційної роботи:

Толюпа С.В, Жаронкін М.Ю. Захист кіберпростору у банківській сфері. Матеріали V Міжнародної науково-практичної конференції "Проблеми кібербезпеки інформаційно-телекомунікаційних систем (PCSITS)" (Київ, 2023).

РОЗДІЛ 1
ІНФОРМАЦІЙНА БЕЗПЕКА У БАНКІВСЬКІЙ ІНФРАСТРУКТУРІ

1.1 Структура та система інформаційної безпеки банку

На сучасному етапі розпитку світової економіки, банки відіграють вкрай важливу роль, оскільки вони виконують різноманітні функції, такі як залучення вкладів, надання кредитів, обслуговування платежів, управління ризиками та фінансовими активами. Банки своєю діяльністю підтримують функціонування різних секторів економіки, таких як промисловість, сільське господарство, торгівля, інфраструктура тощо.

Для того, аби глибше зрозуміти сутність банківської діяльності потрібно звернутись до наявних науково-теоретичних підходів. Оксфордський тлумачний словник розглядає банківську діяльність як діяльність, що здійснюється банками і включає: особисте обслуговування (фізичних осіб), комерційні послуги (обслуговування невеликих і середніх підприємств) та обслуговування корпорацій [1]. Вітчизняні науковці мають наступні думки щодо ролі банківської діяльності, з якими ми погоджуємось. Так, В. Ортинський наголошує, що ступінь розвитку банківської діяльності визначає фінансово-економічну спроможність і потенціал держави. На думку науковця, банківська діяльність є певним різновидом підприємницької діяльності, яка здійснюється на власний розсуд і ризик з метою отримання прибутку. Також банківська діяльність включає в себе діяльність банків як самостійних суб’єктів господарювання та владно-організаційну діяльність НБУ [7, с. 62]. А. Мороз у своїй праці стверджує, що банківська діяльність визначається як сукупність правових дій, що здійснюються певними суб’єктами у формі, яка вимагається законом або договором [8]. Відповідно до законодавства України банківська діяльність – це залучення у вклади грошових коштів фізичних і юридичних осіб та розміщення зазначених коштів від свого імені, на власних умовах та на власний ризик, відкриття і ведення банківських рахунків фізичних та

юридичних осіб [9].

Увесь процес банківської діяльності є важливим компонентом сучасної економіки і має декілька ключових аспектів, які пропонуємо розглянути далі. По-перше, банки допомагають у залученні та мобілізації фінансових ресурсів від фізичних та юридичних осіб. Далі залучені ресурси можуть бути використані для розміщення кредитів та інших інвестицій. По-друге, банки виконують функцію надання кредитів та фінансового посередництва, що сприяє розвитку бізнесу, стимулює виробництво та споживання, а також забезпечує фінансову підтримку населення. По-третє, банки забезпечують обслуговування платежів: можливість здійснення грошових переказів, оплати рахунків, використання платіжних карток та інших фінансових інструментів. Крім цього, банки активно займаються оцінкою, управлінням та розподілом ризиків, пов'язаних зі здійсненням фінансових операцій. Вони також управляють своїми фінансовими активами, забезпечуючи максимальну дохідність та ефективне використання ресурсів.

З позиції фахівця із кібербезпеки, банківська діяльність неможлива без політики безпеки. Політика інформаційної безпеки банківської установи – це система поглядів на визначення основних сфер, умов та процедур практичного вирішення інформаційного захисту банку від протиправних дій. Домарєв В. В. зазначає, що під політикою інформаційної безпеки слід розуміти набір законів, правил, обмежень, рекомендацій тощо, які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз [10, с. 102]. Ми погоджуємось з вищенаведеною думкою та підкреслимо, що політика представляє з себе комплекс заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації, що належить банку та його клієнтам. Головне завдання політики полягає у тому, щоб визначити стратегію, мету та принципи захисту інформації, які відображають ставлення банку до інформаційної безпеки та допомагають забезпечити безпеку даних, що обробляються банком.

З огляду на сучасну практику, до складу політики інформаційної безпеки можуть входити наступні елементи:

- Створення та використання захисних технологій, що забезпечують захист від несанкціонованого доступу до інформації;
- проведення регулярних аудитів та оцінка ризиків щодо інформаційної безпеки;
- розробка та реалізація процедур забезпечення захисту даних під час їх передачі, зберігання та обробки;
- підготовка та навчання співробітників банку з питань інформаційної безпеки;
- встановлення процедур реагування на випадки порушення інформаційної безпеки та розробка планів дій в разі кібератак або інших загроз інформаційній безпеці.

За допомогою політики інформаційної безпеки банк може забезпечити високий рівень захисту даних та знизити ризик виникнення витоків інформації, що може завдати шкоди його діяльності та репутації.

До об’єктів політики інформаційної безпеки відноситься:

- Інформація щодо технічного забезпечення банку;
- інформація про ІзОД;
- інформація про працівників банку;
- інформація про клієнтів банку;
- інформація про фінансові операція;
- конфіденційні електронні мережі банку.

Слід підкреслити, що банк зберігає у своєму інформаційному просторі велику кількість різноманітних даних, втрата або компрометація яких може призвести до значних репутаційних та фінансових втрат:

- Інформація про рахунки, депозити та операції клієнтів;
- інформація про клієнтів банку (паспортні дані, ІНН, мобільні номери);
- інформація про інформаційні технології і засоби безпеки, що використовуються в банку.

Важливим і необхідним інструментом для забезпечення захисту конфіденційної інформації, забезпечення цілісності та доступності банківських даних є план інформаційної безпеки банку. План визначає мету та частину системи інформаційної безпеки, принципи правової бази для її організації та функціонування, типи загроз безпеці та джерела, які слід зберігати, а також основні компоненти стандартів та захисту для розвитку систем безпеки. При цьому важливо розуміти, що захист інформаційної безпеки банку має забезпечувати стійку та неперервну роботи інформаційних та банківських систем, зберегти від загроз інформаційного характеру, захистити від несанкціонованого втручання, порушення цілісності, втрати.

Отож задачами систем забезпечення інформаційної безпеки є:

- Категоризація інформації (комерційна та банківська таємниця);
- протидія витоку та знищенню даної інформації;
- прогнозування та своєчасне реагування на загрози інформаційної безпеки;
- впровадження механізмів для своєчасного і оперативного реагування на інциденти інформаційної безпеки банку;
- ефективне усунення загроз, на основі правових, інженерно-технічних і організаційних мір і засобів забезпечення безпеки.

При побудові ефективної системи інформаційної безпеки банку, треба керуватись такими принципами: стійкість, надійність, повнота, своєчасність, активність, законність, ефективність та раціональність. Дотримання цих принципів допоможе банку створити надійну і ефективну систему інформаційної безпеки, яка захистить конфіденційні дані та забезпечить безперебійну роботу банківської системи.

Успішне та ефективне розгортання інформаційної безпеки банку досягається шляхом формування систем правил, інструкцій, положень та політик. Структуровані функціональні обов’язки працівників та служб, включаючи службу економічної безпеки. Необхідними передумовами забезпечення безпеки є правила розгалуженого доступу до будівлі та окремих кабінетів і серверних кімнат та впровадження правил використання електронних та паперових носіїв інформації.

При побудові банківської інформаційної система, треба розуміти, що один з основних напрямків – це інформаційна безпека, яка націлена на збереження конфіденційності, цілісності та доступності інформації. Складові інформаційної безпеки зображені на рис. 1.1.

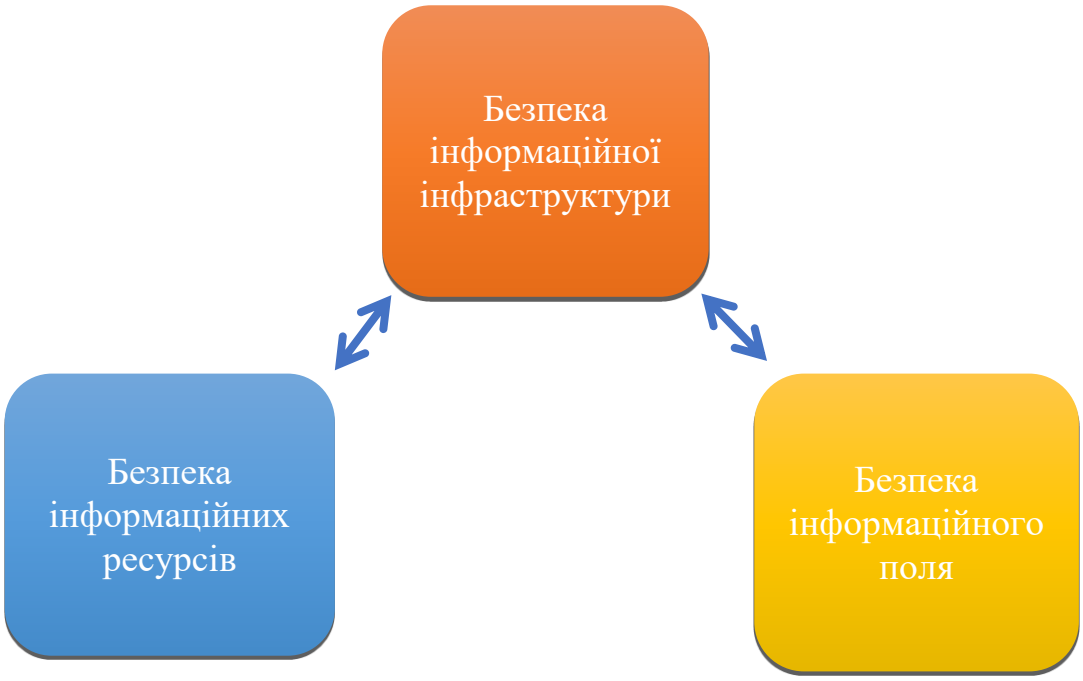

Рисунок 1.1. - Складові інформаційної безпеки банку

Першим важливим елементом є безпека інформаційних ресурсів. Безпека інформаційних ресурсів – це процес захисту інформації від порушень її цілісності та конфіденційності, та протидія її несанкціонованому витоку та пошкодженню. Друга складова інформаційної безпеки банку – це безпека інформаційної інфраструктури, тобто процес захисту технічних компонентів (комп'ютерів, серверів, мережевого обладнання), та забезпечення їх цілісності, доступності та відмовостійкості. І третім важливим елементом є безпека інформаційного поля – це процес захисту несистематичних потоків інформації, яка розповсюджується ЗМІ, конкурентами, оргонами влади, тощо.

Аналіз джерел СУІБ та бізнес-процесів, або банківських продуктів базується на існуючих заходах безпеки та інформації, яка загальнодоступна та систематизована на

етапі опису інформації в інфраструктурі. На цьому етапі ми розглянемо найважливіші банківські продукти, визначені та описані раніше, програмні та апаратні можливості захисту інформації, збитки в разі порушення. Даний аналіз дозволить більш детально оцінити загрози інформаційної безпеки у майбутньому та визначити план управління ризиками. Важливо враховувати, наскільки ефективні перераховані вище комплекси є у процесі захисту інформації.

Серед характеристик захищеної інформації слід виділити такі основні її властивості:

- Конфіденційність – ця властивість гарантує, що інформація не буде розголошена або доступна тим, хто не має на це права. Застосування шифрування, контролю доступу та інших технологій дозволяє забезпечити конфіденційність інформації. Таким чином, це суб'єктивно визначена характеристика інформації, яка вказує на необхідність введення обмежень на коло суб'єктів, які можуть отримати доступ до цієї інформації, і забезпечується здатністю системи зберігати цю інформацію в таємниці від недоступних суб'єктів.
- Цілісність – вказує на те, що інформація має бути збережена у незмінному та правильному стані. Іншими словами, вона не повинна бути втручена, змінена або пошкоджена неправомірними діями. Фактично, це існування інформації в неушкодженому стані.
- Доступність – ця властивість означає, що інформація повинна бути доступною та використовуватися за необхідності. Інформація повинна бути доступною для авторизованих користувачів в потрібний момент часу, щоб вони могли здійснювати свої робочі функції. Захист доступності включає резервне копіювання, масштабування систем, захист від вірусів та інших загроз. На практиці, доступність полягає у забезпеченні своєчасного і безперешкодного доступу до інформації, що становить інтерес для предметної області, а також готовністю відповідних автоматизованих сервісів відповідати на запити.
- Спостережність – відноситься до здатності системи моніторити та реагувати

на події, які відбуваються в ній. Це означає, що система має механізми виявлення та відстеження подій, що стосуються безпеки, таких як спроби несанкціонованого доступу, вторгнення або зміни даних. Забезпечення спостережності включає використання систем моніторингу мережі, виявлення інцидентів та систем аналізу безпеки.

Усі описані вище ознаки не залежать одна від одної, конфігуруються, можуть бути багаторазово відтворені з використанням різних механізмів і заходів захисту, можуть враховувати конкретні загрози інформації, а т акож визначати сервіси, які забезпечують кожну властивість залежно від важливості інформації, очікуваних загроз інформації, а також цілей і завдань захисту. Характеристики інформації завжди включають можливість її порушення або збою, тобто можливість виникнення загроз. Загрози інформації оцінюються з точки зору небажаного впливу на будь-яку з цих характеристик та ймовірності їх порушення. Іншими словами, загроза може розцінюватись як потенційний негативний вплив на інформацію.

Згідно з сучасними підходами до інформаційної безпеки банку, слід зазначити, що інформаційна безпека часто розглядається як один із ключових аспектів корпоративної соціальної відповідальності банків. Корпоративна соціальна відповідальність (Corporate Social Responsibility, CSR) - це концепція, за якою підприємства приймають на себе додаткові соціальні та екологічні зобов'язання. Компанії, які приділяють увагу КСВ, роблять акцент на позитивному впливі своєї діяльності на суспільство, співробітників та навколишнє середовище. Так інформаційна безпека вважається досягнутою в КСВ, якщо для всіх інформаційних ресурсів системи забезпечується певний рівень конфіденційності, цілісності, доступності та спостережуваності [6].

1.2 Загрози інформаційної безпеки банку

Часто неполадки та прогалини в інформаційній системі банку свідчать про те, що певні питання інформаційної безпеки ігноруються або їм не приділяють необхідної уваги. У разі виникнення кризової ситуації (для прикладу, коли на різних бізнес-

процесах або банківських продуктах може бути виявлено ризик втрати основних сервісів безпеки) рекомендується впровадження процесу по зменшенню ризику на всіх системах банку, без виключень. Однак, маємо наголосити, що у більшості випадків існують різні рівні ризиків у різних бізнес-процесах та банківських продуктах, що вимагає від співробітників відділу ІБ спеціальних методів і заходів безпеки для кожного банківського продукту та бізнес-процесу окремо. Саме тому детальна оцінка ризиків повинна враховувати як загально банківські проблеми, так і проблеми, характерні для окремих бізнес-процесів та банківських продуктів. Крім того, особливу увагу слід приділити врахуванню обміну інформацією між різними бізнес-процесами та програмно-апаратними комплексами.

Після детального аналізу впливу порушення інформаційної безпеки на бізнес-процеси можна провести більш глитбоку оцінку ризиків інформаційної безпеки. Загрози можуть завдати шкоди таким ресурсам СУІБ, як інформація, персонал, клієнти, обладнання, процеси та програмно-апаратні засоби, бізнес-процеси, банківські продукти та діяльність банку. Загрози можуть бути природними або штучними, випадковими або навмисними. У бідь-якому разі, необхідно ідентифікувати джерело загроз: як випадкових, так і навмисних. Загрози можна визначити відповідно до їх загальної форми або типу.

Існування вразливості в інформаційному просторі банківської діяльності не може впливати лише на ресурси, бізнес-процеси або банківські продукти, оскільки повинна існувати загроза її використання. Вразливості, що не становлять загрози, не потребують заходів безпеки, але зміни в СУІБ повинні бути ідентифіковані та керовані. Це стосується як ресурсів СУІБ, так і бізнес-процесів або банківських продуктів. Адже неправильно впроваджені або неефективні заходи безпеки є різновидом вразливостей.

У багатьох випадкох вразливості можуть бути пов'язані з характеристиками ресурсів СУІБ. Залежно від важливості даних, робочих процесів, банківських продуктів та інформаційно-комунікаційних технологій, для виявлення вразливостей можна використовувати різні методи проактивного тестування. До таких методів тестування

відносяться:

- Сканери вразливостей;
- тестування захищеності інфраструктури;
- тест на проникнення в середину мережі;
- перегляд та аналіз коду програмно-технічних комплексів;
- аналіз відомих порушень безпеки;
- аналіз відомих вразливостей програмно-технічних компонентів (ОС, БД, веб-застосунки, мобільні застосунки).

Такий комплекс заходів дозволить своєчасно ідентифікувати вразливості. Але слід зазначити, що подібні методи можуть надавати інформацію про вразливості, які не несуть загрози. Тому необхідно коректно та чітко задавати параметри програмно-технічних комплексів та їх конфігурацію і проводити тестування. Наслідки загроз можуть включати втрату продуктивності, бізнес-процесів, репутації тощо. Якщо виявлена загроза призводить до інциденту інформаційної безпеки шляхом використання пов'язаної з нею вразливості або набору вразливостей, необхідно проаналізувати потенційні негативні наслідки для банку. Такий інцидент інформаційної безпеки може вплинути на один або декілька ресурсів СУІБ, бізнес-процесів або банківських продуктів. Отож ресурсам СУІБ та бізнес-наслідкам пошкодження або компрометації цих ресурсів може бути присвоєна грошова оцінка.

Найбільшу загрозу безпеці інформаційних ресурсів становить розголошення або втрата таких ресурсів, особливо інформації, що становить банківську таємницю. Загрози інформаційним ресурсам можуть бути реалізовані шляхом:

- підкуп осіб, які мають прямий доступ до конфіденційної банківської та іншої інформації, до якої банківські установи мають обмежений доступ;
- необережне, недбале поводження з конфіденційною та іншою інформацією Банку з обмеженим доступом;
- недостатня правова та психологічна підготовленість відповідальних працівників банківської установи, наприклад, недотримання банківською установою

встановлених вимог щодо збереження інформації з обмеженим доступом у відносинах з регулюючими та наглядовими органами.

Протидія таким загрозам має полягати, насамперед, у наступних діях:

- визначення благонадійності працівників підприємства, які працюють з конфіденційною та іншою інформацією з обмеженим доступом
- регулювання спеціальних рахунків банківських установ, що містять банківську таємницю та іншу інформацію з обмеженим доступом
- встановлення та закріплення диференційованих прав доступу працівників до банківської таємниці та іншої інформації з обмеженим доступом (наприклад, працівники можуть знати банківську таємницю та вчиняти певні дії лише у зв'язку з виконанням своїх службових обов'язків)
- визначення персональної відповідальності працівника за збереження документів та інших матеріальних носіїв інформації, що містять інформацію з обмеженим доступом банківської організації, наданих йому або розроблених ним.
- обмеження доступу працівників та сторонніх осіб до приміщень, де обробляється (зберігається) інформація з обмеженим доступом банківської організації.
- заходи щодо контролю за діяльністю працівників, які обробляють носії інформації, що містять інформацію з обмеженим доступом банківської організації, та впровадження ефективних систем виявлення та фіксації незаконних дій з такою інформацією;
- впровадження надійних та ефективних систем зберігання носіїв інформації для запобігання несанкціонованому доступу, знищенню та підробці носіїв інформації.

Суттєвими загрозами безпеці інформаційної інфраструктури є:

- Несанкціонований доступ до інформації, що захищається, та знищення такої інформації за допомогою технічних засобів;
- підслуховування з використанням технічних засобів з метою негласного отримання інформації, що циркулює в системах зв'язку та комп'ютерній техніці;

несанкціонований доступ до інформації та навмисний технічний вплив під час її обробки та зберігання;

- використання технічних засобів для підслуховування конфіденційних розмов, що відбуваються в офісних приміщеннях або в транспортних засобах.
- Заходи протидії таким загрозам ґрунтуються насамперед на широкому і, головне, економічно ефективному використанні технічних засобів захисту інформаційних інфраструктур.
- Конкретні заходи щодо протидії загрозам безпеці інформаційної інфраструктури банківських організацій включають
- Забезпечення цілісності засобів захисту, апаратного та програмного середовища. Це означає фізичне зберігання засобів інформаційних технологій, незмінність програмного середовища, виконання функцій, передбачених засобами безпеки, а також розділення засобів безпеки та користувачів;
- Захист від витоку інформації через наявність фізичних полів акустичного та непрямого електромагнітного випромінювання, взаємодію з комунікаційними мережами та будівельними конструкціями;
- Шифрування та захист найбільш цінної інформації при роботі з комп'ютерами, системами, комп'ютерними мережами та корпоративними мережами зв'язку;
- Надання дискримінаційного доступу до даних в комп'ютерах, системах, комп'ютерних мережах та телекомунікаційних мережах банківських установ різного рівня та з різною метою, а також використання працівниками програмно-технічних засобів для виконання певних операцій (створення, перегляд, зберігання, модифікація, видалення), забезпечуючи при цьому: розмежування доступу користувачів до даних; розмежування доступу користувачів до комп'ютерів, систем, комп'ютерних мереж та телекомунікаційних мереж
- ідентифікацію користувачів в електронно-обчислювальних машинах (комп'ютерах), системах, комп'ютерних мережах та телекомунікаційних мережах

організацій на основі використання паролів, ключів, магнітних карток, електронних цифрових підписів та особистих біометричних характеристик при доступі до інформаційно-телекомунікаційних систем користувачів та користувачів

- фіксування (із зазначенням дати і часу) дій користувачів (у тому числі спроб несанкціонованого доступу) до інформаційних і програмних ресурсів на комп'ютерах, в системах та комп'ютерних мережах
- запобігання передачі інформації з обмеженим доступом незахищеними телекомунікаційними лініями зв'язку
- запобігання проникненню вірусів в інформаційно-комунікаційні системи;
- Регулярно перевіряти технічні засоби та приміщення на предмет наявності пристроїв несанкціонованого доступу;
- Виділення спеціальних приміщень для захисту голосової інформації, в тому числі конфіденційних розмов.

Найбільш серйозними загрозами безпеці "інформаційного сектору" є шкода комерційному іміджу банківської установи, проблеми у відносинах з реальними та потенційними клієнтами, конкурентами, регуляторами та правоохоронними органами, зокрема вплив поширення дезінформації та існуючої дезінформації про банківську установу, а також вплив негативної інформації.

Конкретні заходи щодо протидії загрозам безпеці "інформаційного сектору" банківських установ повинні включати

- Широкий збір та аналіз інформації;
- негайні дії у разі поширення неправдивої інформації про банківську установу;
- скоординовану та цілеспрямовану рекламну, маркетингову та іншу інформацію для покращення іміджу та сприйняття банківської організації серед клієнтів.
- Обмін інформацією з державними органами та органами місцевого самоврядування в межах чинного законодавства.

Виходячи з цих численних загроз та шляхів їх подолання, система інформаційної безпеки банківської організації повинна захищати інформацію з обмеженим доступом банківської організації від несанкціонованого поширення, використання та порушення конфіденційності (приватності), а також цілісність і доступність інформації, що обробляється, зберігається та циркулює в електронно-обчислювальних машинах (комп'ютерах), системах та засобах зв'язку Цілісність і доступність інформації, що обробляється, зберігається та циркулює в електронно-обчислювальних машинах, системах та засобах зв'язку, повинна бути забезпечена.

Це можна визначити як комплекс організаційних, технічних, програмних та криптографічних заходів і засобів захисту, спрямованих на забезпечення цілісності та доступності інформації, що обробляється, зберігається та розповсюджується електронно-обчислювальними машинами, системами та засобами зв'язку.

1.3 Захист інформації у банківській інфраструктурі

Основним методом захисту інформації є так званий метод захисту. AAA або 3A (автентифікація, авторизація та контроль) вважається основним методом захисту інформації. Важливе місце у світі займають апаратні та програмні системи ідентифікації та автентифікації (CIA) до комп’ютеру.

При використанні CIA співробітники отримують дозвіл на доступ до ПК і мереж для спільної роботи. При використанні SIA доступ співробітників до ПК і мереж для спільної роботи дозволяється тільки після успішної ідентифікації та автентифікації. Під час використання SIA доступ до ПК і мереж для спільної роботи дозволяється тільки після успішної ідентифікації та автентифікації. Засоби ідентифікаціїВизнання особи людини. Розпізнавання користувача за допомогою або через функцію ідентифікації, видану особі. Перевірка автентичності особи користувача здійснюється в процесі автентифікації. Аутентифікація перевіряється в процесі автентифікації.

Сучасні IAC можна поділити на такі типи засобів ідентифікації електронні паролі,

біометричні паролі, уніфіковані паролі та одноразові паролі (рис. 1.2).

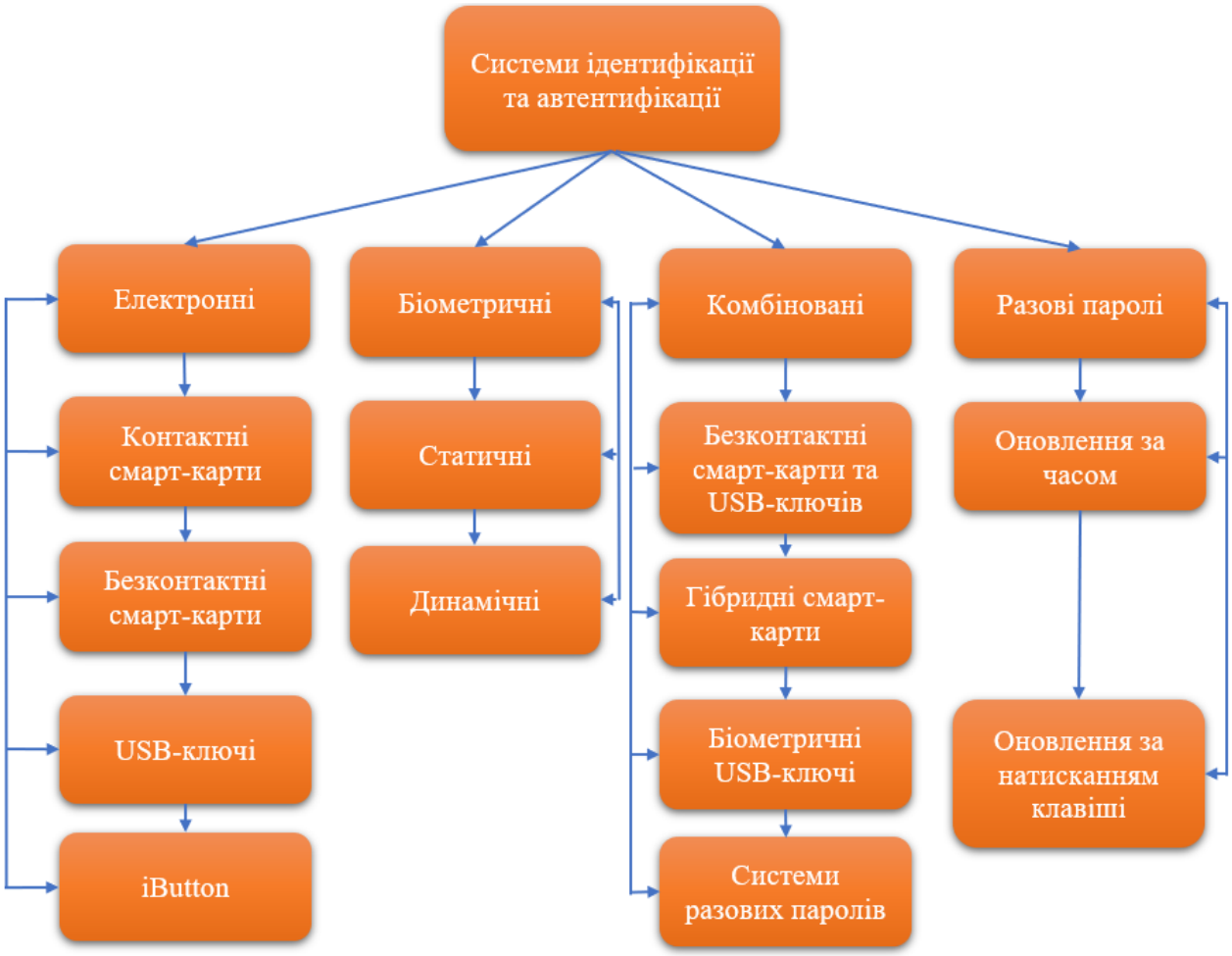

Рисунок 1.2 – Класифікація систем ідентифікації та автентифікації

Численні дослідження показали, що віруси, трояни, шпигунські та інші шкідливі програми є найбільш поширеною і шкідливою інформаційною загрозою. Крім того, всі комп'ютери, незалежно від того, підключені вони до Інтернету чи ні, повинні бути оснащені цим інструментом безпеки.

Всесвітньо визнана антивірусна технологія захищає ваш комп'ютер від сучасних інформаційних загроз, таких як Віруси, трояни, хробаки, шпигунські програми, рекламне ПЗ тощо.

Нові, невідомі загрози, які швидко поширюються. Руткіти, буткіти та інші сучасні загрози. Ботнети та інші шкідливі методи. Ця підсистема повинна виявляти всі атаки

(всіх рівнів) проти даного вузла мережі. Підсистема також повинна вміти виконувати аналіз безпеки та виявляти вразливості у вузлах, що контролюються; стежити за журналами операційної системи та журналами додатків, що працюють під управлінням операційної системи. Вона також повинна виявляти атаки на мережі TCP, IP та SMB/NetBios, побудовані на основі мережевої архітектури, що підтримується комп'ютерами, за якими ведеться спостереження.

Підсистема інформаційної безпеки в локальній мережі повинна включати наступні механізми захисту:

- Розширена ідентифікація та аутентифікація
- Дозволений вибірковий контроль доступу
- Закрите програмне середовище
- Захист зашифрованих даних
- Інші механізми безпеки

Адміністратор безпеки повинен мати можливість централізовано керувати всіма механізмами безпеки, а також централізовано контролювати та відслідковувати дотримання політики безпеки. Вся інформація про події, пов'язані з безпекою в ІС, повинна реєструватися в єдиному файлі журналу. Забезпечити негайне інформування адміністратора безпеки, якщо користувач намагається вчинити протиправну дію.

Також повинні бути доступні інструменти для створення звітів, попередньої обробки журналів та управління віддаленими робочими станціями. Підсистема може мати клієнт-серверну архітектуру, де серверна частина централізовано зберігає і обробляє дані системи безпеки, а клієнтська частина захищає ресурси робочих станцій і сервера і зберігає управлінську інформацію у власній базі даних.

У цьому випадку сервер безпеки встановлюється на виділеному комп'ютері або контролері домену і забезпечує виконання наступних завдань. Ведення центральної бази даних системи безпеки, що містить інформацію, необхідну для роботи системи безпеки.

Збір інформації про події від усіх клієнтів в єдиний лог-файл і передача обробленої інформації в підсистему управління. Взаємодія з підсистемою управління та надсилання

адміністративних команд управління клієнтським частинам системи безпеки.

Завдяки таким схемам управління, управління інформаційною безпекою можна керувати за допомогою розподілу повноважень між мережевим адміністратором та адміністратором безпеки може бути суворо дотриманий.

Цілісність інформаційної бази даних будь-якої організації зазвичай забезпечується механізмами, вбудованими в систему управління базами даних, що використовується цією організацією.

Підсистема реєстрації та обліку - ця підсистема повинна дозволяти користувачеві переглядати список активних користувачів, тобто список користувачів, які в даний момент працюють в інформаційній базі даних. Крім того, необхідно проаналізувати журнали дій, виконаних користувачами за будь-який період (історія користувача). Також необхідно, щоб такі журнали можна було архівувати для подальшого використання.

На цьому найвищому рівні процедури безпеки та контролю починаються з політики безпеки. Політика безпеки - це комплексний план захисту компанії від внутрішніх і зовнішніх загроз, який повинен відповідати ISO 17799, міжнародному стандарту інформаційної безпеки, що визначає найкращі практики безпеки. Стандарт складається з десяти основних розділів:

Політика безпеки, Контроль доступу до системи, Управління комп'ютерами, Розробка та обслуговування, Фізична та екологічна безпека, Відповідність вимогам, Особиста безпека, Організація безпеки, Класифікація та контроль, Управління безперервністю бізнесу. Сучасна тенденція в практиці безпеки полягає в поєднанні фізичної та логічної безпеки в організації.

Фізична безпека - це всі заходи, які організація використовує для захисту своїх об'єктів, ресурсів і приватних даних, що зберігаються у фізичному середовищі, в той час як логічна безпека - це методи, які обмежують доступ до систем та інформації організації лише для уповноважених осіб. На додаток до цих заходів безпеки, керівництво також повинно контролювати людські та інформаційні ресурси компанії.

Ці заходи контролю на рівні підприємства є дуже важливими, оскільки вони часто мають широкий вплив на багато інших заходів контролю, таких як загальний контроль IT та контроль на рівні додатків. У зв'язку зі збільшенням частоти природних і техногенних катастроф, компаніям і організаціям будь-якого розміру необхідно свідомо розробляти і тестувати плани аварійного відновлення для підтримки своїх загальних засобів контролю. Крім того, на думку Rainer & Cegielski, надійні плани резервного копіювання є критично важливими для інформаційної безпеки, і це ще більш важливо для МСП, оскільки втрата даних означає втрату клієнтів. У багатьох випадках така інтеграція вирішує дві основні проблеми [2].

По-перше, об'єднуються географічно розподілені підсистеми. По-друге, це дозволяє користувачам Інтернету отримати доступ до даних LSI. Зазвичай ці два завдання реалізуються за допомогою веб-сайту.

Практика показує, що функціонування веб-сайту має значний вплив на загальну ефективність IOMC: Основою веб-сайту є веб-сервер, який надає клієнтам доступ до веб-сторінок через мережу. Цей підроблений веб-сайт точно такий же, як і оригінальний, і може легко передати дані про безпеку хакерам і шахраям. Ось кілька способів уникнути фішингу. Жоден банк не надішле вам електронного листа з проханням повідомити свій номер безпеки та пароль. Якщо ви отримали електронного листа від вашого банку, не відповідайте на нього, незалежно від того, наскільки важливою є інформація про безпеку.

Завжди телефонуйте за номером телефону банку і запитуйте, чи дійсно ця інформація необхідна. Потім, якщо ви підозрюєте шахрайство, надішліть до банку електронного листа з повідомленням про шахрайство. Перевірте веб-сайт банку, присвячений безпеці: ніколи не переходьте за гіперпосиланнями в Інтернеті та не переходьте за посиланнями на домашню адресу банку. Завжди вводьте повну URL-адресу веб-сайту банку у своєму браузері. Перевірте, чи починається веб-сайт банку з "https" і чи є внизу браузера значок замка. Двічі клацніть на піктограму замка, щоб побачити інформацію про замок і перевірити, чи є сайт справжнім. Якщо замок

недійсний або виданий сайту, якого ви не впізнаєте, не вводьте жодної інформації про безпеку.

Вхід і вихід щоб запобігти шахрайству, не повідомляйте нікому свій ідентифікатор безпеки та пароль. Не залишайте комп'ютер або ноутбук без нагляду, коли ви ввійшли до свого облікового запису в інтернет-банкінгу. Завжди виходьте зі свого облікового запису в кінці сеансу роботи. Не зберігайте свій ідентифікатор безпеки та пароль на комп'ютері і завжди тримайте їх у безпечному місці. Також не змінюйте свої облікові дані безпеки, коли користуєтесь комп'ютером у громадських місцях. Значна частина проблеми забезпечення інформаційної безпеки в ІС може бути вирішена організаційними заходами. Так, на минулій лабораторній роботі були надані інструкції та положення щодо чіткого розмежування обов'язків та прав сторін, задіяних у компанії, правил поведінки на обладнанні для забезпечення конфіденційності та цілісності даних, а також визначення особистої таємниці.

Висновки за розділом 1

Банківська діяльність – це комплекс фінансових операцій, які здійснюються комерційними банками з метою збереження, розмноження та розподілу грошових коштів у межах економічної системи. Актуальність банківської діяльності пояснюється її ключовою роллю у фінансовій системі та економіці загалом.

У першому розділі ми розібрали інформацію про інформаційну безпеку банку, систему та загрози ІС. Існує загальна потреба у подальшому вивченні та розробці чіткої концепції "загрози", і слід зосередитись на створенні ефективної та реалістичної системи моніторингу та управління та інші інформаційних загроз Стратегічною місією банку є запобігання існуючим та потенційним загрозам інформаційній безпеці та забезпечення інформації безпеки забезпечити механізм для.

В інформаційній галузі забезпечує послідовну систематичну діяльність, низку заходів та державні та правоохоронні органи, які забезпечують належну реалізацію

національних інтересів держави. пов’язані людські інтереси та суспільство, запобігання недолікам інформації та їх швидке вирішення. З огляду на активну глобалізацію інформаційно-комунікаційних мереж, співпраця важлива не лише для банку, держави, але й для міжнародних організацій у боротьбі з агресією різних держав.

РОЗДІЛ 2
ДОСЛІДЖЕННЯ ДОКУМЕНТІВ РЕГЛАМЕНТУЮЧИХ БАНКІВСЬКУ БЕЗПЕКУ

2.1 Дослідження стандарту PCI DSS

Зростання шахрайства з платіжними картками є однією з основних причин, чому міжнародні платіжні системи співпрацюють, щоб вжити додаткових заходів для захисту своїх клієнтів. Тому в 2004 році було розроблено єдиний набір вимог до безпеки даних - Стандарт безпеки даних індустрії платіжних карток (Payment Card Industry Data Security Standard).

Пізніше, у вересні 2006 року, була створена спеціальна рада з безпеки - Рада зі стандартів безпеки PCI, яка займається розробкою та просуванням стандарту PCI DSS. Основними функціями Ради зі стандартів безпеки є розробка та публікація стандарту PCI DSS та всіх пов'язаних з ним документів, визначення вимог до майбутніх акредитованих компаній, що проводять аудит (QSA) та сканування PCI DSS, проведення самої акредитації, навчання майбутніх QSA та забезпечення якості роботи, що виконується аудиторами. Моніторинг. Тим часом міжнародні платіжні системи приймають аудиторські звіти та оцінюють роботу QSA.

Усі організації, які зберігають, обробляють або передають інформацію про платіжні картки, уповноважені платіжними системами VISA, MasterCard, American Express, Discover та JCB, повинні відповідати стандартам безпеки PCI DSS. Це стосується банків, постачальників платіжних послуг, інтернет-магазинів і традиційних торговців.

Відповідність - це не одноразова вимога. Торговці зобов'язані перевіряти свою відповідність раз на рік, але очікується, що вони будуть дотримуватися її постійно.

PCI DSS (Payment Card Industry Data Security Standard) - це набір стандартів безпеки даних платіжних карт, який розробляється та підтримується Консорціумом

платіжних систем (PCI SSC). Цей стандарт встановлює вимоги до захисту конфіденційної інформації, пов'язаної з платіжними картами, та включає такі області, як захист мережевої інфраструктури, захист даних карток та захист даних в процесі обробки платіжних транзакцій.

PCI DSS є обов'язковим для всіх організацій, які займаються обробкою, зберіганням або передачею інформації про платіжні картки. Дотримання цього стандарту допомагає запобігти витоку конфіденційної інформації, зменшити ризик шахрайства з використанням платіжних карток та збільшити довіру клієнтів до організації, що обробляє їхні платежі.

PCI DSS складається з 12 вимог, які охоплюють такі аспекти, як захист мережевої інфраструктури, захист даних карток, захист даних в процесі обробки платіжних транзакцій, управління ризиками та інші. Для виконання цих вимог організація повинна розробити та впровадити політики, процедури та технічні заходи безпеки, а також періодично проводити оцінку відповідності стандарту та аудити безпеки даних.

Отже, стандарт PCI DSS складається з 12 вимог, які охоплюють різні аспекти безпеки даних. Ось короткий опис кожної з цих вимог:

1) Захист мережевої інфраструктури: організації повинні підтримувати безпечну мережеву інфраструктуру шляхом встановлення технічних заходів захисту, наприклад, фаєрволів, роутерів, віртуальних приватних мереж тощо.

2) Захист даних про платіжні картки: організації повинні забезпечувати захист даних про платіжні картки, зокрема, номерів карток, строків дії тощо. Для цього слід використовувати криптографічні методи та забезпечити контроль доступу до цих даних.

3) Захист даних в процесі обробки платіжних транзакцій: організації повинні забезпечити безпеку даних під час обробки платіжних транзакцій. Наприклад, вони повинні захищати даних під час їх передачі в мережі та забезпечувати захист даних, що зберігаються на пристроях для обробки платіжних транзакцій.

4) Використання безпеки за замовчуванням: організації повинні застосовувати безпеку за замовчуванням, тобто, всі системи та додатки повинні бути налаштовані

таким чином, щоб вони були захищені за допомогою стандартних налаштувань безпеки.

5) Оновлення та захист ПЗ: 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.

6) Обмеження доступу до даних: організації повинні забезпечувати контроль доступу до даних про платіжні картки, наприклад, обмежувати доступ до цих даних тільки тим співробітникам, які це потребують у зв'язку зі своїми обов'язками.

7) Моніторинг та відстеження: організації повинні підтримувати моніторинг та відстеження дій, що виконуються в мережі та на пристроях для обробки платіжних транзакцій. Наприклад, слід вести журнали подій, які дозволять виявити можливі загрози та напади на систему.

8) Впровадження заходів захисту згідно з принципом "потрібно знати лише необхідне": організації повинні забезпечувати захист даних про платіжні картки лише за необхідності. Наприклад, у випадку зберігання даних, слід зберігати лише необхідну мінімальну кількість даних про картки, які потрібні для обробки платіжних транзакцій.

9) Регулярне тестування захисту: організації повинні регулярно проводити тестування захисту, щоб виявляти можливі вразливості та ризики безпеки. Тестування можуть включати сканування вразливостей, перевірку на наявність шкідливого програмного забезпечення, перевірку на стійкість до атак тощо.

10) Захист фізичного середовища: організації повинні забезпечувати безпеку фізичного середовища, де знаходяться пристрої для обробки платіжних транзакцій, наприклад, сервери, термінали тощо. Наприклад, слід забезпечити безпеку приміщень, контроль доступу до них, захист від змін підключення обладнання тощо.

11) Управління ризиками: організації повинні визначати та оцінювати ризики безпеки і вживати заходів для зниження цих ризиків до прийнятного рівня. Наприклад, слід проводити оцінку ризиків та планувати заходи захисту відповідно до виявлених

загроз та ризиків.

12) Впровадження та зберігання політик 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.

Всі ці вимоги повинні виконуватись організаціями, які приймають платіжні картки, для забезпечення безпеки обробки платіжних транзакцій та захисту даних про платіжні картки від несанкціонованого доступу.

Далі ми описуємо сферу застосування стандарту PCI DSS, що зазначено у самому стандарті.

Вимоги PCI DSS застосовуються до:

- Середовище даних власників карток (CDE), яке складається з:
- Системні компоненти, люди та процеси, які зберігають, обробляють та передають дані власників карток та/або конфіденційні дані автентифікації;
- системні компоненти, які не можуть зберігати, обробляти або передавати CHD/SAD, але мають необмежене підключення до компонентів системи що зберігати, обробляти або передавати CHD/SAD.
- Системні компоненти, люди та процеси, які можуть вплинути на безпеку CDE.

«Системні компоненти» включають мережеві пристрої, сервери, обчислювальні пристрої, віртуальні компоненти, хмарні компоненти та програмне забезпечення. Приклади системних компонентів включають, але не обмежуються:

- Системи, які зберігають, обробляють або передають дані облікового запису (наприклад, платіжні термінали, системи авторизації, системи клірингу, системи проміжного програмного забезпечення для платежів, системи бек-офісів платежів, системи переднього ходу кошика та магазину, системи платіжного шлюзу/комутатора, системи моніторингу шахрайства).
- Системи, які надають послуги безпеки (наприклад, сервери аутентифікації,

сервери контролю доступу, інформація про безпеку та події системи управління (SIEM), системи фізичної безпеки (наприклад, доступ до бейджів або CCTV), багатофакторні системи аутентифікації, антивірусні системи).

- Системи, які полегшують сегментацію (наприклад, внутрішні елементи контролю безпеки мережі).
- Системи, які можуть вплинути на безпеку даних облікового запису або CDE (наприклад, дозвіл імен або перенаправлення електронної комерції (веб) сервери).
- Компоненти віртуалізації, такі як віртуальні машини, віртуальні комутатори/маршрутизатори, віртуальна техніка, віртуальні додатки/настільні комп'ютери, і гіпервізори.
- Хмарна інфраструктура і компоненти, як зовнішні, так і локальні, і в тому числі установки контейнерів або зображень, віртуальні приватні хмари, хмарна ідентифікація та управління доступом, CDE, що проживають у приміщеннях або в хмарі, сервісні сітки з контейнерами додатки та інструменти оркестрування контейнерів.
- Мережеві компоненти, включаючи, але не обмежуючись, мережевий контроль безпеки, комутатори, маршрутизатори, мережеві пристрої VoIP, бездротовий доступ точки, мережеві прилади та інші прилади безпеки.
- Типи серверів, включаючи, але не обмежуючись, веб, додаток, базу даних, аутентифікацію, пошту, проксі, протокол мережевого часу (NTP), іСистема доменних імен (DNS).
- Пристрої кінцевого користувача, такі як комп'ютери, ноутбуки, робочі станції, адміністративні робочі станції, планшети та мобільні пристрої.
- Принтери та багатофункціональні пристрої, які сканують, друкують та факсять.
- Зберігання даних облікового запису в будь-якому форматі (наприклад, папір, файли даних, аудіо-файли, зображення та відеозаписи).
- Додатки, програмне забезпечення та програмні компоненти, без серверні програми, включаючи всі придбані, підписані (наприклад, Softwareas-a-Service),

спеціальні та користувальницькі програми, включаючи внутрішні та зовнішні (наприклад, Інтернет) програми.

- Інструменти, репозиторії коду та системи, які реалізують управління конфігурацією програмного забезпечення або для розгортання об'єктів у CDE або в системи, які можуть впливати на CDE[3].

2.2 Дослідження постанови НБУ №95

Це Положення розроблено відповідно до Законів України “Про Національний банк України”, “Про банки і банківську діяльність”, “Про захист інформації в інформаційно-телекомунікаційних системах”, “Про основи національної безпеки України”, указів Президента України від 13 лютого 2017 року № 32/2017 “Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року “Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації” та від 15 березня 2016 року № 96/2016 “Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року “Про Стратегію кібербезпеки України”, національних стандартів України з питань інформаційної безпеки ДСТУ ISO/IEC 27000:2015 “Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник” (далі – ДСТУ ISO/IEC 27000:2015), ДСТУ ISO/IEC 27001:2015 “Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги” (далі – ДСТУ ISO/IEC 27001:2015), ДСТУ ISO/IEC 27002:2015 “Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки” (далі – ДСТУ ISO/IEC 27002:2015), які прийняті наказом Державного підприємства “Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості” від 18 грудня 2015 року № 193, та з урахуванням міжнародних стандартів з питань інформаційної безпеки, загальноприйнятих у міжнародній практиці принципів забезпечення інформаційної безпеки і кіберзахисту з метою підвищення рівня інформаційної безпеки в банківській системі України [4].

Дане положення регламентує обов’язкові мінімальні вимого щодо організації заходів із забезпечення інформаційної безпеки та кіберзахисту у банківській інфраструктурі. Не мало важливим, є вимоги, що описані у постанові, які стосуються принципів управління інформаційною безпекою і вимоги до інформаційних систем банку, що взаємодіють з інформаційними ресурсами НБУ.

Важливо розуміти, що ця постанова не регламентує фізичну безпеку приміщень банку, використання криптографічних засобів захисту інформації Національного банку в інформаційних системах Національного банку, вимоги до яких визначені відповідними нормативно-правовими актами НБУ. До цього списку також входить використання хмарних технологій\сервісів у сфері автоматизації.

Далі ми розберемо принципи забезпечення інформаційної безпеки у банках, які описані у постанові. Першочерговим є те, що підхід до побудови інформаційної безпеки у банку має бути структурованим та комплексним, а процес по удосконаленню та розвитку цих систем має вестись неперервно і мати обґрунтування і використання раціональних заходів з дослідженням і використанням найкращих практик міжнародного досвіду. Своєчасними й адекватними мають бути заходи захисту від реальних і потенційних загроз у мережі банку. Має бути постійний контроль і підтримка зі сторони керівництва банку, за для забезпечення належного рівня захищеності інформаційної мережі банку.

Криптографічний захист інформації в інформаційній системі Національного банку під час обміну даними між учасниками інформаційної системи Національного банку та Національним банком забезпечується шляхом застосування багаторівневого (ієрархічного) підходу з використанням незалежної системи криптографічного захисту.

Для захисту сеансового рівня моделі взаємодії відкритих систем інформаційних систем Національного банку використовуються криптографічні протоколи Transport Layer Security (TLS), що гарантує контроль за цілісністю та конфіденційністю інформації. На прикладному рівні механізми захисту використовуються для ідентифікації/автентифікації підписувача та контролю цілісності й конфіденційності на

всіх етапах обробки інформації. Залежно від категорії інформації, пов'язаної з критеріями конфіденційності, транспортний рівень використовує односторонній (криптографічні ключі на стороні клієнта і сервера, надійна криптографічна автентифікація по обидва боки з'єднання) або двосторонній довірений захист (криптографічні ключі тільки на стороні сервера, надійна криптографічна автентифікація на стороні сервера) для забезпечення ідентифікації та автентифікації каналу.

Інформаційна система Національного банку підтримує останню версію протоколу криптографічного захисту інформації на транспортному рівні, але не нижче версії 1.2 Інформаційна система Національного банку використовує виключно криптографічний пакет криптографічного захисту інформації на транспортному рівні з довжиною ключа не менше 128 біт та симетричним шифруванням Департамент безпеки Національного банку надає криптографічну бібліотеку засобів криптографічного захисту інформації, рекомендації щодо їх використання та програмне забезпечення для генерації ключів.

Банк зобов’язаний упровадити СУІБ згідно з ДСТУ ISO/IEC 27001:2015 для визначеної сфери застосування з урахуванням обов’язкових вимог щодо впровадження СУІБ, викладених у цьому положенні [3].

Ця постанова чітко регламентує вимоги до реалізації СУІБ у структурі банку. Мова іде про те, що банк зобов’язаний мати орган СУІБ, який буде мати потрібні повноваження і регламентуватися положенням про СУІБ, в якому буде чітко викладено його завдання, функції та відповідальності.

Банк повинен впровадити в орган СУІБ голову правління чи\або його заступника, який відповідає за інфомраційну безпеку банку, керівника підрозділу банку - власник ключових бізнес-процесів банку та керівник підрозділу управління ризиками банку. Банки мають право включати до операційної структури СУІБ інших працівників банку залежно від потреб, що випливають із специфіки діяльності банку.

Банки зобов'язані покласти на орган управління СУІБ такі завдання виконувати такі обов'язки:

- затвердження та перегляд політики інформаційної безпеки, заходів щодо її реалізації та стратегії розвитку інформаційної безпеки банку
- затвердження нових проектів, керівних документів, стратегічних питань та впровадження заходів з інформаційної безпеки для забезпечення інформаційної безпеки банку; та
- розгляд, затвердження та управління реалізацією проектів, пов'язаних з розробкою, впровадженням, функціонуванням, моніторингом, переглядом, підтримкою та вдосконаленням СУІБ банку; та
- визначення найбільш доцільних ресурсів, необхідних для реалізації заходів з інформаційної безпеки; та
- організація практичних засобів підвищення обізнаності та навчання персоналу банку з питань інформаційної безпеки; та
- своєчасний моніторинг впровадження та ефективності СУІБ Банку та подальша оцінка можливостей для вдосконалення і необхідності коригувальних заходів.

Окрім цього, банк повинен розробити та впровадити загальну політику інформаційної безпеки банку, яка має включати в себе наступні об’єкти:

- Напрямки та цілі розвитку та функціонування інформаційної безпеки;
- регламентування сфер застосування цієї політики;
- правила, принципи та вимоги що описують інформаційну безпеку банку;
- описати відповідальних за сектор інформаційної безпеки та чітко розгалужити ролі та їх функції.

Банк зобов’язаний розробити та затвердити стратегію розвитку інформаційної безпеки, політику інформаційної безпеки, та забезпечити їх підтримкою в актуальному стані на регулярній основі.

Окрім вищеописаного, банк повинен впровадити в себе криптографічний захист інформації в інформаційних системах НБУ.

Учасники інформаційних систем НБУ встановлюють системи криптографічного захисту інформації в інформаційних системах НБУ відповідно до вимог, установлених

у відповідних експлуатаційних документах кожної інформаційної системи НБУ. Банк забезпечує захист інформаційних систем банку від несанкціонованого доступу та дій, спрямованих на відмову в обслуговуванні, відповідно до вимог розділу 4 цього положення.

Банки зобов'язані призначити керівника служби інформаційної безпеки (CISO) з достатніми повноваженнями для прийняття управлінських рішень (посада нижче заступника голови правління банку).

У банківських інформаційних системах, що безпосередньо забезпечують автоматизацію банківських операцій, забороняється об'єднання в одній функції (ролі) таких компетенцій: розробка та супроводження (експлуатація), супроводження (адміністрування), розроблення та (управління) та експлуатацію, виконання операцій у відповідній системі та здійснення контролю за їх виконанням.

Банки зобов'язані використовувати механізми багатофакторної автентифікації при наданні доступу до виконання функцій з управління або обслуговування САБ.

Банк блокує або перейменовує обліковий запис користувача операційної системи за замовчуванням та забезпечує відключення гостьового облікового запису. Банк блокує обліковий запис резидента локального адміністратора операційної системи або (якщо це технічно неможливо на функціональному рівні операційної системи) перейменовує обліковий запис резидента та змінює його пароль не рідше ніж один раз на 30 днів.

Банк зобов'язаний автоматично блокувати робочий стіл операційної системи після 15 хвилин бездіяльності користувача на робочій станції або сервері, а потім повторно аутентифікувати користувача при розблокуванні (за винятком робочих станцій або серверів, де блокування неможливе або вимагає більшого часу бездіяльності через використовувану технологію).

Банки повинні забезпечити постійне оновлення мережевої документації банку (в електронній та/або паперовій формі), документування всіх змін у конфігурації мережі банку та зберігання попередніх версій мережевої документації протягом щонайменше одного року.

Банк забезпечує використання режиму захисту WPA2-Enterprise (корпоративний режим у наборі алгоритмів і протоколів Wireless Protected Access версії 2) у своїй бездротовій мережі, а для реалізації гостьових підключень - WPA2-Personal (персональний режим у наборі алгоритмів і протоколів Wireless Protected Access версії 2).

Також банки забов’язані впровадити в себе структуру ЦСК, яка буде займатись акредитованими власними сертифікатами ключів.

Банк зобов'язаний використовувати проміжний сервер для виконання адміністративних функцій або функцій підтримки інформаційних систем, мережевого обладнання та серверів Банку. Підключення до таких серверів здійснюється з непривілейованого облікового запису, а підключення з проміжного сервера до інформаційних систем, мережевого обладнання та серверів Банку здійснюється з привілейованого облікового запису. Банк може використовувати альтернативні методи управління та контролю доступу, які не дозволяють привілейованим користувачам (адміністраторам) мати прямий доступ до інформаційних систем, мережевого обладнання та серверів Банку.

Банки зобов'язані вживати заходів безпеки для захисту від DoS/DDoS-атак у периметрі мережі банку. Методи та засоби (технології) захисту від таких атак визначаються банком самостійно.

2.3 Дослідження стандарту ISO/IEC 27002

Цей міжнародний стандарт призначений для використання організаціями як довідник для вибору засобів контролю в рамках процесу впровадження системи управління інформаційною безпекою (СУІБ) на основі ISO/IEC 27001 або як керівний документ для організацій, які впроваджують загальноприйняті засоби контролю інформаційної безпеки. Цей стандарт також призначений для використання в промисловості, що розвивається керівні принципи управління інформаційною безпекою

для конкретної організації, враховуючи їх специфічне середовище ризику інформаційної безпеки.

Організації всіх типів і розмірів (включаючи державний і приватний сектори, комерційні та некомерційні) збирати, обробляти, зберігати та передавати інформацію в багатьох формах, включаючи електронну, фізичну та вербальну (наприклад, бесіди та презентації).

Цінність інформації виходить за рамки написаних слів, цифр і зображень: знання, поняття, ідеї і бренди є прикладами нематеріальних форм інформації. У взаємопов’язаному світі інформація та пов'язані процеси, системи, мережі та персонал, залучений до їх експлуатації, обробки та захисту це активи, які, як і інші важливі бізнес-активи, є цінними для бізнесу організації отже, заслуговують або вимагають захисту від різних небезпек.

Активи піддаються як навмисним, так і випадковим загрозам, тоді як пов’язані процеси, системи, мережі та люди мають невід’ємну вразливість. Зміни в бізнес-процесах і системах або інші зовнішні зміни (наприклад, нові закони та нормативні акти) можуть створити нові ризики для інформаційної безпеки. Таким чином, враховуючи безліч способів, якими загрози можуть скористатися вразливістю, щоб завдати шкоди організації завжди присутні ризики інформаційної безпеки. Ефективна інформаційна безпека знижує ці ризики, захищаючи організацію від загроз і вразливостей, а потім зменшуючи вплив до своїх активів.

Інформаційна безпека досягається впровадженням відповідного набору засобів контролю, включаючи політики, процеси, процедури, організаційні структури та функції програмного та апаратного забезпечення. Ці засоби контролю потрібні створювати, впроваджувати, контролювати, переглядати та покращувати, де це необхідно, щоб гарантувати, що конкретні цілі безпеки та бізнес-цілі організації досягнуті. СУІБ, як зазначено в ISO/IEC 27001 містить цілісний, скоординований погляд на ризики інформаційної безпеки організації в щоб реалізувати комплексний набір засобів контролю інформаційної безпеки в рамках загальної структури цілісної системи

управління.

Багато інформаційних систем не розроблено таким чином, щоб бути безпечними в розумінні ISO/IEC 27001 і цього стандарт. Безпека, яку можна досягти за допомогою технічних засобів, обмежена, і її слід підтримувати відповідним управлінням і процедурами. Визначення того, які засоби контролю повинні бути на місці, вимагає ретельне планування та увага до деталей. Успішна СУІБ потребує підтримки з боку всіх співробітників організації. Це також може вимагати участі акціонерів, постачальників або інших зовнішніх сторін. Також можуть знадобитися консультації спеціалістів від зовнішніх сторін.

У більш загальному сенсі ефективна інформаційна безпека також забезпечує керівництво та інші зацікавлені сторони що активи організації є достатньо безпечними та захищеними від шкоди, таким чином діючи як а стимулятор бізнесу.

Вимоги до інформаційної безпеки, що описує цей стандарт, важливо, щоб організація визначила свої вимоги безпеки. Існує три основних джерела вимоги безпеки:

- оцінка ризиків для організації, беручи до уваги загальний бізнес організації стратегія та цілі. За допомогою оцінки ризиків визначаються загрози для активів, вразливість до оцінюється ймовірність виникнення та оцінюється потенційний вплив;
- правові, статутні, регулятивні та договірні вимоги до організації, її торгівлі партнери, підрядники та постачальники послуг мають задовольнити своє соціокультурне середовище;
- набір принципів, цілей і бізнес-вимог до обробки, обробки інформації, зберігання, передача та архівування, які організація розробила для підтримки своїх операцій.

Ресурси, задіяні для впровадження заходів контролю, мають бути збалансовані з ймовірною шкодою для бізнесу бути результатом проблем безпеки за відсутності цих елементів керування. Результати оцінки ризиків будуть допомогти скерувати та визначити відповідні управлінські дії та пріоритети для управління інформацією ризики безпеки та для впровадження засобів контролю, вибраних для захисту від цих ризиків.

ISO/IEC 27005 надає вказівки щодо управління ризиками інформаційної безпеки, включаючи поради щодо ризиків оцінка, обробка ризику, прийняття ризику, комунікація ризику, моніторинг ризику та огляд ризику.

Елементи керування можна вибрати з цього стандарту або з інших наборів елементів керування, або можна створити нові елементи керування для задоволення конкретних потреб у відповідних випадках. Вибір засобів контролю залежить від організаційних рішень на основі критеріїв ризику прийняття, варіанти обробки ризиків і загальний підхід до управління ризиками, застосований до організації, а також має підпадати під дію всіх відповідних національних і міжнародних законів і правил. Вибір елементів також залежить від того, як елементи керування взаємодіють для забезпечення глибокого захисту.

Деякі елементи керування в цьому стандарті можна розглядати як керівні принципи інформаційної безпеки управління та застосовні для більшості організацій. Елементи керування пояснюються більш детально нижче разом із керівництвом із впровадження. Додаткова інформація про вибір елементів керування та інше лікування ризиків параметри можна знайти в ISO/IEC 27005.

Інформація має природний життєвий цикл, від створення та виникнення до зберігання, обробки, використання та передачі до його остаточного знищення або розпаду. Вартість активів і ризики для них можуть змінюватися протягом їх (наприклад, несанкціоноване розкриття або викрадення фінансових рахунків компанії є набагато менш значущим після вони були офіційно опубліковані), але інформаційна безпека залишається певною мірою важливою на всіх етапах. Інформаційні системи мають життєвий цикл, у межах якого вони задумуються, конкретизуються, проектуються, розробляються, перевірено, впроваджено, використано, обслуговувано та зрештою знято з експлуатації та утилізовано. Інформація безпека повинна враховуватися на кожному етапі. Нові розробки системи та зміни існуючої системи надають організаціям можливості для оновлення та вдосконалення засобів контролю безпеки, приймаючи фактичні інцидентів, поточних і прогнозованих ризиків інформаційної безпеки.

Цей міжнародний стандарт дає настанови щодо стандартів організаційної безпеки інформації та практики управління інформаційною безпекою, включаючи вибір, впровадження та управління засобів контролю з урахуванням середовища(ів) ризику інформаційної безпеки організації. Цей міжнародний стандарт розроблено для використання організаціями, які мають намір:

- вибрати елементи керування в процесі впровадження системи управління інформаційною безпекою на основі ISO/IEC 27001;
- запроваджувати загальноприйняті засоби контролю інформаційної безпеки;
- розробити власні керівні принципи управління інформаційною безпекою

Користуючись мобільними пристроями, слід особливо уважно стежити за тим, щоб бізнес-інформація не була скомпрометована. Політика щодо мобільних пристроїв повинна враховувати ризики роботи з мобільними пристроями в незахищеному середовищі.

У політиці щодо мобільних пристроїв слід враховувати:

- реєстрація мобільних пристроїв;
- вимоги до фізичного захисту;
- обмеження встановлення програмного забезпечення;
- вимоги до версій програмного забезпечення мобільних пристроїв і до застосування патчів;
- обмеження підключення до інформаційних послуг;
- контроль доступу;
- криптографічні методи;
- захист від шкідливих програм;
- дистанційне вимкнення, стирання або блокування;
- резервні копії;
- використання веб-сервісів і веб-додатків.

Слід бути обережним, користуючись мобільними пристроями в громадських

місцях, кімнатах для переговорів та інших незахищених місцях. Необхідно забезпечити захист, щоб уникнути несанкціонованого доступу до інформації, що зберігається та обробляється цими пристроями, або розголошення інформації, напр. використання криптографічних методів і забезпечення використання секретної інформації для автентифікації. Мобільні пристрої також мають бути фізично захищені від крадіжки, особливо коли вони залишаються, наприклад, у автомобілях та інших видах транспорту, готельних номерах, конференц-центрах і місцях зустрічей.

Специфічна процедура з урахуванням правових, страхових та інших вимог безпеки організації повинні бути встановлені на випадки крадіжки або втрати мобільних пристроїв. Пристрої, що містять важливу, конфіденційну або критичну бізнес-інформацію, не можна залишати без нагляду та, де можливо, їх потрібно фізично заблокувати або використовувати спеціальні замки для захисту пристроїв.

Необхідно організувати навчання для персоналу, який використовує мобільні пристрої, щоб підвищити його обізнаність про додаткові ризики, пов’язані з таким способом роботи, і засоби контролю, які слід запровадити.

Усі працівники організації та, у відповідних випадках, підрядники повинні проходити відповідну освіту та навчання, а також регулярно оновлювати політику та процедури організації відповідно до їх робочих функцій.

Програма підвищення обізнаності щодо інформаційної безпеки має бути спрямована на те, щоб працівники та, де це доцільно, підрядники були обізнані про їхню відповідальність за інформаційну безпеку та засоби, за допомогою яких ці обов’язки виконуються.

Програма підвищення обізнаності щодо інформаційної безпеки повинна бути створена відповідно до політики інформаційної безпеки організації та відповідних процедур, беручи до уваги інформацію організації, яку необхідно захистити, і засоби контролю, які були впроваджені для захисту інформації. Програма інформування повинна включати низку заходів з підвищення обізнаності, таких як кампанії (наприклад, «день інформаційної безпеки») та випуск буклетів чи інформаційних

бюлетенів.

Програма підвищення обізнаності повинна бути спланована з урахуванням ролей працівників в організації та, де це доречно, очікувань організації щодо обізнаності підрядників. Діяльність у програмі підвищення обізнаності має бути запланована на час, бажано регулярно, щоб заходи повторювалися та охоплювали нових працівників і підрядників. Програму підвищення обізнаності також слід регулярно оновлювати, щоб вона відповідала організаційним політикам і процедурам, і повинна базуватися на уроках, отриманих з інцидентів інформаційної безпеки.

Навчання з підвищення обізнаності має проводитися відповідно до вимог програми організації з підвищення обізнаності щодо інформаційної безпеки. Навчання з підвищення обізнаності може використовувати різні засоби доставки, включаючи навчання в аудиторії, дистанційне навчання, веб-інтерфейс, самостійне навчання та інші.

Навчання та тренінги з інформаційної безпеки мають відбуватися періодично. Початкове навчання та навчання стосується тих, хто переходить на нові посади чи ролі з суттєво іншими вимогами до інформаційної безпеки, а не лише новачків, і має проходити до того, як ця роль стане активною.

Організація повинна розробити програму навчання та навчання для ефективного проведення навчання та навчання. Програма повинна відповідати інформації організації політику безпеки та відповідні процедури, беручи до уваги інформацію організації, яку потрібно захистити, і засоби контролю, які були впроваджені для захисту інформації. Програма слід розглянути різні форми освіти та навчання, напр. лекції або самостійна робота.

Класифікації та пов’язані з ними засоби захисту інформації повинні враховувати потреби бізнесу щодо обміну інформацією чи її обмеження, а також вимоги законодавства. Інші активи, окрім інформації, також можна класифікувати відповідно до класифікації інформації, яка зберігається в активі, обробляється або іншим чином обробляється чи захищається цим активом. Власники інформаційних активів повинні нести відповідальність за їх класифікацію.

Схема класифікації повинна містити умовності для класифікації та критерії перегляду класифікації з часом. Рівень захисту в схемі слід оцінювати шляхом аналізу конфіденційності, цілісності та доступності та будь-яких інших вимог до інформації, що розглядається. Схема повинна бути узгоджена з політикою контролю доступу. Кожному рівню слід присвоїти назву, яка має сенс у контексті застосування схеми класифікації.

Схема має бути узгодженою для всієї організації, щоб кожен однаково класифікував інформацію та пов’язані з нею активи, мав спільне розуміння вимог захисту та застосовував належний захист.

Класифікація повинна бути включена в процеси організації та бути послідовною та узгодженою в усій організації. Результати класифікації повинні вказувати на вартість активів залежно від їх чутливості та критичності для організації, напр. з точки зору конфіденційності, цілісності та доступності. Результати класифікація повинна оновлюватися відповідно до змін їх значення, чутливості та критичності через їхній життєвий цикл.

Висновки за розділом 2

У другому розділі ми розібрали інформацію про нормативні документи, які регламентують інформаційну безпеку банку. Був досліджений міжнародний стандарт PCI DSS, який регламентує набір вимог, розроблених Консорціумом індустрії платіжних карт (PCI SSC), з метою забезпечення безпеки обробки, зберігання та передачі даних платіжних карт.

У другому підрозділі було розібрано постанову Національного Банку України під номером 95, яка регламентую безпеку банківської інфраструктури у банках України.

У третьому підрозділі був детально розібраний міжнародний стандарт ISO/IEC 27002. Цей міжнародний стандарт призначений для використання організаціями як довідник для вибору засобів контролю в рамках процесу впровадження системи управління інформаційною безпекою на основі ISO/IEC 27001 або як керівний документ

для організацій, які впроваджують загальноприйняті засоби контролю інформаційної безпеки.

Ці документи є ключовими опорами, на які слід спиратись, при побудові налагодженої і ефективної системи інформаційної безпеку банку. Вони висувають універсальні рекомендації, які необхідно впроваджувати в системи банку, щоб забезпечити високий рівень захисту інформації, включаючи дані платіжних карт та банківську інфраструктуру.

Застосування вимог PCI DSS дозволяє банкам створити та підтримувати безпечне середовище для обробки платіжних карт, включаючи встановлення захищених мереж, шифрування даних, контроль доступу та моніторинг інцидентів. Цей стандарт є важливим для запобігання крадіжок карткових даних, зменшення ризику шахрайства та підвищення довіри клієнтів до банку.

Стандарт ISO/IEC 27002, у свою чергу, надає широкий набір рекомендацій щодо контролю інформаційної безпеки. Цей стандарт може використовуватися як основа для впровадження системи управління інформаційною безпекою в банку, де розглядаються аспекти, такі як фізична безпека, доступ до інформації, криптографічний захист, управління інцидентами та багато інших.

У побудові ефективної системи інформаційної безпеки банку важливо враховувати індивідуальні потреби та характеристики організації, використовувати передові технології та практики, а також забезпечувати постійний моніторинг, аналіз та оновлення системи безпеки. Рекомендується залучати кваліфікованих фахівців з інформаційної безпеки та використовувати сертифіковані рішення та послуги для забезпечення найвищого рівня захисту.

Всі ці заходи сприятимуть збереженню конфіденційності, цілісності та доступності інформації в банку, а також зниженню ризику втрати даних, порушення безпеки та фінансових втрат. Окрім вимог стандартів PCI DSS та ISO/IEC 27002, також важливо враховувати регулятивні вимоги та законодавство, що стосуються безпеки інформації в банківській сфері. Кожна країна може мати свої власні правила та

нормативи, які банк повинен дотримуватися.

При побудові налагодженої і ефективної системи інформаційної безпеки банку важливо забезпечити належне навчання та свідомість персоналу щодо важливості безпеки інформації, впровадити процеси моніторингу та аудиту для постійного виявлення та виправлення потенційних проблем, а також розробити і регулярно оновлювати плани реагування на інциденти безпеки.

РОЗДІЛ 3.
РЕКОМЕНДАЦІЙНІ МЕТОДИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ У БАНКІВСЬКІЙ ІНФРАСТРУКТУРІ

3.1 Рекомендації щодо методів забезпечення кібербезпеки в банківській інфраструктурі

При побудові захищеної мережі, ми маємо розуміти, що нам загрожує і які методи протидії будуть най ефективнішими. Для початку нам потрібно захистити наш периметр, найкращим рішенням буде використання NGFW. Одним із лідерів на ринку по всьому світу є рішення від Ізраїльської компанії CheckPoint, яке має дуже потужні рішення інформаційної безпеки.

Родина мережевих екранів («шлюзів безпеки») ізраїльської компанії Check Point входить до архітектури безпеки Infinity, яка також включає в себе пісочниці SandBlast, пристрої захисту від DDoS-атак DDoS Protector і систему оркестрування Quantum Maestro для кластеризації NGFW. Самі мережеві екрани складають оновлену родину Quantum Security Gateways, яку було представлено рік тому. Мережеві екрани (за визначенням Check Point) призначені для захисту від «кібератак п’ятого покоління», тобто складних багатовекторних атак типу WannaCry і NotPetya, у яких використовуються високорозвинені зловмисні програми. Функціональність мережевих екранів включає функцію перевірки у хмарній пісочниці SandBlast Threat Emulation, яка, за твердженням виробника, виявляє зловмисне ПО на етапі експлойту (використання вразливості) ще до того, як воно встигне застосувати технології ухилення для обману пісочниці. Інший інструмент, SandBlast Threat Extraction, вилучає з файлів потенційно вразливі елементи і надає користувачам вже знешкоджений контент [11].

Це рішення дозволить нам перекрити периметр внутрішньої мережі і контролювати пакети даних як із зовні, так і всередині мережі. Перевагою цього рішення буде наявність захисту від атак типу Dos\DDos, різноманітних зловмисних програм (при

спробі потрапити в мережу), захист від шифрувальників і іншого. Позитивною стороною буде те, що рішення від компанії CheckPoint може ефективно масштабуватись, відштовхуючись від потреб банку і задовольнити як невелику мережу, так і масштабну, гібридну інфраструктуру. Це рішення ефективно показує себе з рішеннями інших виробників, наприклад мережевим обладнанням від компанії CISCO. Підтримується можливість об'єднання декількох гейтвеїв у кластер, для підвищення рівня відмовостійкості всієї інфраструктури. Також є можливість розміщення агентів, на кінцевих точках, для моніторингу і регулюванню їх захищеності.

Критичним об'єктом банківської інфраструктури є бази даних. Дуже важливо забезпечити їх конфіденційність, цілісність та доступність, бо вони зберігають як фінансові дані, так і повну інформацію про клієнтів банку.

Для початку треба розробити і впровадити суворі політики безпеки для БД, які включають комплексні паролі, регулярну їх зміну, виділення обмеженого кола необхідних користувачів та контроль доступу на рівні ролей і привілеїв. Необхідно використовувати криптографічні методи захисту інформації, такі як шифрування даних, що знаходяться в БД, для цієї задачі добре підійде прогремне рішення Microsoft SQL Server transparent Data Encryption, це рішення в SQL Server надає можливість шифрування баз даних на рівні файлів, що дозволяє захистити дані в спокійний період і під час передачі на диски з резервними копіями.

Прозоре шифрування даних (TDE) шифрує файли даних SQL Server, Azure SQL Database і Azure Synapse Analytics. Це шифрування відомо як шифрування даних у стані спокою. Щоб захистити базу даних користувачів, ви можете вжити таких заходів:

- Проектування безпечної системи.
- Шифрування конфіденційних активів.
- Побудова брандмауера навколо серверів баз даних.

Однак зловмисник, який викрадає фізичні носії, такі як накопичувачі або резервні стрічки, може відновити або прикріпити базу даних і переглянути її дані.

Одним з рішень є шифрування конфіденційних даних у базі даних і використання

сертифіката для захисту ключів, які шифрують дані. Це рішення запобігає використанню даних будь-ким, хто не має ключів. Але планувати цей вид захисту потрібно заздалегідь.

TDE здійснює шифрування та розшифровку даних і файлів журналу в реальному часі. Для шифрування використовується ключ шифрування бази даних (DEK). Завантажувальний запис бази даних зберігає ключ доступності під час відновлення. DEK є симетричним ключем. Це захищено сертифікатом, який зберігає головна база даних сервера, або асиметричним ключем, який захищає модуль EKM. TDE захищає дані в стані спокою, тобто файли даних і журнали. Це дає змогу дотримуватися багатьох законів, постанов і вказівок, прийнятих у різних галузях. Ця можливість дозволяє розробникам програмного забезпечення шифрувати дані за допомогою алгоритмів шифрування AES і 3DES, не змінюючи існуючі програми [12].

Наступним кроком, для забезпечення безпеки даних, буде впровадження системи DLP.

Прикладом даної системи буде виступати рішення від компанії Symantec, під назвою Symantec DLP. Це розширена платформа DLP, яка надає можливості виявлення, моніторингу та запобігання витоку даних через електронну пошту, веб-сайти, зовнішні пристрої та інші канали комунікації. Вона підтримує широкий спектр регуляторних вимог і володіє розширеними функціями аналізу контенту та контексту даних.

- Захист конфіденційної інформації: Банки мають обов'язок забезпечити конфіденційність даних своїх клієнтів. DLP система дозволяє виявляти та запобігати витоку чутливої інформації, такої як персональні дані, банківські реквізити або фінансові транзакції. Це допомагає запобігти фінансовим втратам, порушенням довіри клієнтів та репутаційним проблемам.
- Виконання регуляторних вимог: Банківська галузь підлягає строгим регуляторним вимогам щодо захисту даних. DLP система допомагає виконувати ці вимоги, сприяючи виявленню та запобіганню витоку даних, які можуть призвести до порушення законодавства, такого як GDPR, PCI DSS або HIPAA.
- Виявлення внутрішніх загроз: Велика кількість витоків даних стається через

недбалість або зловживання співробітниками. DLP система дозволяє виявляти підозрілу активність, яка може свідчити про намірену або ненавмисну передачу конфіденційної інформації. Це допомагає попереджати внутрішні загрози та зменшувати ризик витоку даних.

- Запобігання кібератакам: DLP система допомагає виявляти незвичайну активність, що може свідчити про кібератаку або вторгнення. Вона сприяє вчасному виявленню та реагуванню на такі загрози, що дозволяє банку захистити свою інфраструктуру та дані від різних видів кіберзлочинів, включаючи крадіжку фінансової інформації, шахрайство, фішингові атаки та викрадення даних.
- Забезпечення дотримання внутрішніх політик: DLP система дозволяє банкам встановлювати та здійснювати контроль над використанням та передачею даних відповідно до їхніх внутрішніх політик безпеки. Вона дозволяє налаштувати правила та політики, які визначають, які дані можуть бути передані, кому і через які канали, забезпечуючи дотримання внутрішніх стандартів та процедур [13].

Всі ці фактори роблять DLP систему важливим компонентом банківської інфраструктури, допомагаючи забезпечити безпеку та конфіденційність даних, виконати регуляторні вимоги та запобігти витоку інформації, що може мати серйозні наслідки для банку і його клієнтів.

Для розуміння статусу захищеності внутрішньої мережі банку, необхідно на регулярній основі проводити сканування на виявлення вразливостей. З цією задачею допоможе рішення класу сканер вразливостей, як приклад ми преведемо рішення під назвою Qualys, від однойменної компанії, воно відмінно себе зарекомендувало серед конкурентів і тримає головні позиції в цьому сегменті рішень. Воно виконує задачі по оцінці, моніторингу та захисту безпеки інформаційних систем.

Qualys пропонує широкий спектр продуктів та сервісів, включаючи:

- Qualys Vulnerability Management: Це рішення надає засоби для виявлення, аналізу та усунення уразливостей в інформаційних системах. Воно допомагає організаціям виявляти потенційні вразливості та приймати заходи для їх усунення.

- Qualys Policy Compliance: Цей продукт дозволяє перевіряти виконання безпекових політик та стандартів у всій інфраструктурі. Він надає можливості автоматичного аудиту та репортування, що допомагає забезпечити дотримання внутрішніх та регуляторних вимог.
- Qualys Threat Protection: Ця послуга забезпечує раннє виявлення та захист від загроз кібербезпеки. Вона використовує технології машинного навчання та штучного інтелекту для аналізу потоку даних та ідентифікації підозрілої активності.
- Qualys Cloud Security: Цей продукт дозволяє контролювати безпеку хмарних сервісів, таких як AWS, Azure, GCP та інші. Він надає можливості моніторингу, аналізу конфігурації та ідентифікації потенційних проблем безпеки в хмарному середовищі [14].

Для централізованого контролю та моніторингу захищеності нашої мережі, нам необхідно рішення, яке буде збирати в собі всі отримані дані, від систем безпеки. Даний тип рішень називається SIEM. Достойним претендентом у цьому сегменті буде рішення від компанії IBM, під назвою QRadar.

- Це є популярним рішенням SIEM (Security Information and Event Management), яке використовується в банківській інфраструктурі для забезпечення безпеки та моніторингу подій. Ось кілька ключових аспектів та переваги використання QRadar у банківському секторі:
- Централізований моніторинг: QRadar збирає, агрегує та аналізує дані з різних джерел, включаючи системні журнали, мережеві пристрої, додатки та інші. Це дозволяє банку мати централізований огляд та контроль над подіями безпеки в реальному часі.
- Виявлення загроз: 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.
- Кореляція подій: QRadar використовує технологію кореляції подій для з'єднання пов'язаних подій і виявлення складних атак, що можуть проявлятися у вигляді

послідовності звичайних подій. Це дозволяє банку отримати більш повну картину щодо потенційних загроз та вчасно реагувати на них.

- Відстеження вразливостей: QRadar може інтегруватися з системами сканування вразливостей для отримання актуальної інформації про потенційні слабкі місця в інфраструктурі банку. Це допомагає ідентифікувати вразливості та приймати заходи для їх усунення, зменшуючи ризик вторгнень.
- Розширені можливості аналітики: QRadar пропонує розширені можливості аналізу та візуалізації даних безпеки. Він дозволяє створювати звіти, графіки та інші візуальні засоби для моніторингу та аналізу подій безпеки. Це допомагає аналітикам та безпековим фахівцям зрозуміти загальну картину загроз та приймати відповідні заходи.
- Реагування та інцидентний менеджмент: QRadar допомагає автоматизувати процес реагування на події безпеки. Він може генерувати автоматичні сповіщення, запускати реакції на певні події та спрямовувати їх на відповідні команди або системи для подальшого розслідування та реагування на інциденти.
- Дотримання нормативних вимог: QRadar допомагає банкам виконувати різні нормативні вимоги щодо безпеки, такі як вимоги PCI DSS (Payment Card Industry Data Security Standard) або вимоги регуляторних органів. Він надає засоби для моніторингу та звітності, що полегшує аудит та документування відповідності.

Інтеграція з іншими системами безпеки: QRadar може інтегруватися з іншими системами безпеки 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 [15]. Використання QRadar у банківській інфраструктурі допомагає забезпечити раннє виявлення загроз.

Наступним важливим кроком, при побудові інформаційної мережі банку є впровадження системи ЦСК, що необхідно, для підвищення рівня захищеності банку. При впроваджені цієї системи потрібно проаналізувати вимоги: першим кроком є аналіз вимог щодо безпеки та керування ключами в банківській мережі. Це включає визначення

потреб у сертифікатах, рівнях доступу, перевірку ідентичності тощо.

Планування і архітектура: Наступним кроком є розробка детального плану впровадження ЦСК. Це включає визначення архітектури системи, вибір відповідних технологій та інфраструктури, а також установлення бюджету та графіку реалізації.

Вибір технології: Наступним кроком є вибір відповідної технології ЦСК. Це може включати використання комерційних рішень, відкритих стандартів або розробку власних рішень, залежно від потреб і можливостей банку. Розгортання і налаштування: Після вибору технології ЦСК виконується її розгортання та налаштування в мережі банку. Це включає встановлення серверів ЦСК, налаштування параметрів безпеки та інтеграцію з існуючими системами. Генерація та розповсюдження сертифікатів: Наступним кроком є генерація та розповсюдження сертифікатів. Це включає створення сертифікатів для користувачів, серверів, пристроїв та інших об'єктів, а також їх розповсюдження та установку на відповідні системи.

Управління ключами та сертифікатами: Після впровадження ЦСК важливим етапом є надання доступу до ключів та сертифікатів в мережі банку. Це включає установлення політик керування ключами, розподіл прав доступу, регулярну зміну та оновлення ключів та сертифікатів.

Моніторинг та аудит: Для забезпечення безпеки системи ЦСК важливо здійснювати моніторинг та аудит активності ключів та сертифікатів. Це включає виявлення та відстеження незвичайної або підозрілої активності, а також аналіз журналів подій для виявлення потенційних загроз або вразливостей. Навчання та свідомість персоналу: Важливим аспектом впровадження ЦСК є навчання та підвищення свідомості персоналу банку. Це включає навчання щодо безпеки ключів та сертифікатів, процедур використання, розповсюдження та зміни ключів, а також ідентифікації та реагування на підозрілу активність. Оновлення та підтримка: Після впровадження ЦСК важливо забезпечити його оновлення та підтримку. Це включає встановлення оновлень, виправлення помилок, моніторинг та вдосконалення системи з метою забезпечення найвищого рівня безпеки [16].

Весь процес впровадження ЦСК у мережі банку повинен бути виконаний з урахуванням вимог безпеки та нормативних вимог, з метою забезпечення надійного та безпечного керування ключами та сертифікатами в банківському середовищі.

Для контролю і розгалуженню прав доступу користувачів потрібно впровадити систему IDM, яка дозволить ефективно керувати на адмініструвати цей процес.

Впровадження системи централізованого управління обліковими даними на базі технології Oracle Identity Manager. Нова система підвищить ефективність управління та контролю доступу користувачів до основних інформаційних систем банку. Впровадження системи IDM стало логічним продовженням загального тренду на оптимізацію та підвищення рівня інформаційної безпеки в банку. Фахівці системного інтегратора провели дослідження IT-інфраструктури банку і процесів авторизації доступу, в результаті якого були сформульовані системні вимоги, успішно реалізовані в проекті на базі Oracle Identity Manager.

На першому етапі проекту було встановлено інфраструктуру Oracle Identity Manager в головному офісі банку та проведено інтеграцію рішення з основними IT-системами замовника. Першочерговим завданням була інтеграція рішення Oracle з системою управління персоналом SAP в головному офісі материнського банку в Угорщині.

HR-системи були з'єднані між собою за допомогою коннектора через веб-сервіси. Це дозволило завантажувати інформацію про співробітників і структуру персоналу в Oracle Identity Manager. На основі даних з HR-системи рішення Oracle використовувалося для управління правами доступу до основних інформаційних систем банку. Особливості проекту включали реалізацію сервісів самообслуговування користувачів для управління паролями та автоматизацію синхронізації конфігурацій персоналу і груп Active Directory [17].

Для підвищення відмовостійкості всієї мережі необхідно впроваджувати систему резервного копіювання та відновлення даних.

Основні функції систем резервного копіювання та відновлення включають в себе

наступні пункти:

- Регулярне резервне копіювання: Системи автоматично або за заданим графіком створюють резервні копії даних та систем. Це може включати копіювання файлів, баз даних, налаштувань систем та інших важливих компонентів.
- Інкрементальне та диференційне копіювання: За допомогою цих методів системи резервного копіювання зберігають тільки змінені або нові файли, що дозволяє економити простір на сховищі та скоротити час відновлення [18].
- Зберігання та архівування: Резервні копії зазвичай зберігаються на віддалених серверах або на зовнішніх носіях, таких як локальні дисків, мережеві сховища або хмарні платформи. Деякі системи також надають можливість архівування даних для довготривалого зберігання.
- Відновлення даних: У разі втрати або пошкодження даних, системи резервного копіювання дозволяють відновити ці дані до попереднього стану. Це може включати відновлення окремих файлів, баз даних або повних систем.

Рекомендованим рішенням буде IBM Backup and Restore Manager. Ця система резервного копіювання та відновлення дозволяє забезпечити захист даних у різних середовищах, включаючи фізичні сервери, віртуальні машини та хмарні сервіси. Вона має можливості дедуплікації, шифрування та централізованого управління [19].

Для захищеності банківських web-застосунків потрібно використовувати рішення класу WAF (Web application firewall). Лідером на ринку є рішення під назвою F5 WAF, воно себе зарекомендувало як ефективний та надійний інструмент у цій сфері.

F5 WAF є одним з високопродуктивних рішень для захисту веб-додатків в банках та інших секторах. Він забезпечує захист від широкого спектру кібератак, спрямованих на вразливості веб-додатків, таких як SQL-ін'єкції, XSS (міжсайтові скриптінги) та інші.

Він використовує різноманітні механізми для виявлення та блокування потенційно шкідливих запитів до веб-додатків. Він аналізує трафік, що проходить через нього, виявляючи аномальні патерни та поведінку, які можуть свідчити про атаку. Застосовуються методи евристичного аналізу, сигнатурного пошуку, а також аналізу

контексту для виявлення нових та невідомих загроз.

У банківській сфері F5 WAF дозволяє захищати клієнтські облікові записи, фінансові транзакції та конфіденційні дані від кіберзлочинців. Він може блокувати спроби злому, використовуючи різноманітні методи атак, такі як внедрення зловмисних скриптів у форми вводу, маніпуляції параметрами URL або спроби виконання зловмисного коду на сервері.

F5 WAF також забезпечує можливість налаштування політик безпеки та різні механізми перевірки ідентичності користувачів, що дозволяє банкам контролювати доступ до веб-додатків та виконувати аутентифікацію та авторизацію. Це особливо важливо для дотримання нормативних вимог щодо безпеки даних, таких як PCI DSS (Payment Card Industry Data Security Standard).

Структурно, департамент інформаційної безпеки, має включати в себе п’ять підрозділів, які будуть відповідати за свій сектор обов’язків, підрозділ СУІБ, підрозділ кібербезпеки та протидії кіберзагрозам, підрозділ SOC, підрозділ управління правами та підрозділ криптографії.

Кожен з цих підрозділів виконує невід’ємно важливу роль, в системній, продуктивній та ефективній роботі всього департаменту. Підрозділ СУІБ займається розробкою і підтримкою в актуальному стані внутрішніх регулятивних документів. Також цей підрозділ має співпрацювати з аудиторськими компаніями, за для контролю цього процесу і має з ними домовлятись на регулярній основі, про проведення різноманітних перевірок. Розробка і контроль програм навчання інформаційній грамотності і захищеності теж лежить на цьому секторі. Підрозділ SOC займається відстежуванням статусу захищеності мережі і реагує на інциденти, за допомогою SIEM системи [20].

Підрозділ кібербезпеки та протидії кіберзагрозам виконує багато різноманітних завдань, пов’язаних із захистом інформації. Цей сектор має плідно співпрацювати з усіма підрозділами департаменту ІБ та ІТ. Цей підрозділ займається технічним супроводом і впровадження систем безпеки, відслідковуванням та усуненням

вразливостей на системах, та багато іншого.

Підрозділ управління правами доступу займається веденням ПЗ IDM, видає та контролює права доступу для окремих і груп співробітників. На плечах цього підрозділу лежить розробка повноцінної моделі розмежування прав доступу в мережі банку [21].

Підрозділ криптографії займається всім, що стосується криптографічного захисту інформації. Процес впровадження і адміністрування ЦСК є дуже важливим для банку. Також цей сектор відповідає за криптографічні токени, для доступу до ПК, захистом платежів і відслідковує повний цикл життя різноманітних сертифікатів у мережі банку.

3.2 Рекомендації щодо забезпечення безпеки хмарної інфраструктури

Забезпечення безпеки хмарної інфраструктури банку є критично важливим завданням для банку, при побудові гібридної інфраструктури. Побудова гібридної мережі з використанням хмарних технологій Azure є прогресивним рішенням і включає інтеграцію локальної інфраструктури з хмарним середовищем для створення розширеної і більш гнучкої мережевої інфраструктури. Спеціалістам з інформаційної безпеки потрібно виконати наступні дії, для побудови гібридної мережі з використанням сервісів Azure:

Оцінити потреби банку і визначити, які частини інфраструктури потрібно розмістити в хмарі та які залишити на місцевих серверах. Потрібно визначити вимоги до мережевого з'єднання між локальною мережею і системою Azure. Першочерговим є розробка плану міграції, визначивши послідовність перенесення додатків і даних в хмару.

Важливим етапом є налаштування VPN-з'єднання між локальною мережею і Azure за допомогою Azure Virtual Network Gateway або Azure ExpressRoute. Це дозволить підключити локальну мережу до віртуальної мережі Azure. Необхідно встановити локальний мережевий пристрій (наприклад, VPN-шлюз) для забезпечення з'єднання з Azure. Це може включати налаштування IPsec-тунелей та маршрутизації.

Наступною задачею буде створення і налаштування віртуальної мережі в Azure,

яка буде використовуватися для підключення до локальної мережі. Далі іде налаштування підмережі (subnet) віртуальної мережі і визначення IP-діапазони для кожної підмережі. Налаштуйте маршрутизацію віртуальної мережі для забезпечення потрібного маршрутування трафіку між локальною мережею і Azure.

Міграція додатків та даних до Azure є важливим етапом. Розгляньте можливості міграції додатків, такі як підняття віртуальних машин, контейнеризація або використання хмарних сервісів Azure, наприклад, Azure App Service або Azure Functions. Далі іде перенос даних до хмари, використовуючи рішення для резервного копіювання та відновлення, або синхронізуйте дані між локальними серверами і Azure.

Налаштування безпеки та моніторингу: Встановіть необхідні заходи безпеки, такі як файрволи, системи виявлення вторгнень та моніторингу безпеки, як для локальної мережі, так і для хмарної інфраструктури Azure. Налаштуйте систему моніторингу, щоб відслідковувати активності, аномалії та потенційні загрози в гібридній мережі.

Керування та автоматизація: Використовуйте інструменти керування ресурсами Azure, такі як Azure Resource Manager, для створення і управління інфраструктурою хмари. Розгляньте можливості автоматизації за допомогою інструментів, таких як Azure Automation або Azure Logic Apps, для автоматичного налаштування, моніторингу та виконання завдань у гібридному середовищі.

Резервне копіювання та відновлення: Використовуйте рішення для резервного копіювання та відновлення, такі як Azure Backup, для захисту важливих даних і додатків в хмарі. Налаштуйте регулярне резервне копіювання і тестування відновлення для забезпечення надійності та доступності даних.

Масштабування та оптимізація: Використовуйте можливості масштабування Azure, такі як автоматичне масштабування віртуальних машин або використання контейнерних рішень, для ефективного розподілу ресурсів в залежності від потреб вашого банку. Аналізуйте моніторингові дані та використовуйте інструменти для оптимізації витрат та ефективного використання ресурсів Azure.

Безпека та захист даних: Забезпечте безпеку мережі та даних за допомогою

інструментів і сервісів Azure, таких як Azure Security Center, Azure Firewall, Azure DDoS Protection і Azure Active Directory. Налаштуйте доступ до ресурсів в хмарі, використовуючи управління ролей та політики доступу. Використовуйте шифрування для захисту даних під час передачі та зберігання, наприклад, шифрування дисків або використання Azure Key Vault для керування ключами шифрування.

Моніторинг та аналітика: Використовуйте Azure Monitor для моніторингу стану ресурсів, метрик продуктивності та виявлення аномалій. Встановіть централізовані системи логування та аналізу логів, такі як Azure Log Analytics або Azure Sentinel, для виявлення і реагування на події безпеки та виявлення вторгнень.

Дислокація резервних копій та географічна реплікація: озгляньте можливість дислокації резервних копій та реплікації даних в різних регіонах Azure для забезпечення високої доступності та захисту від збоїв. Використовуйте Azure Site Recovery для реплікації і відновлення віртуальних машин і додатків між різними регіонами Azure.

Супровід та підтримка: Оцініть можливості підтримки, які пропонуються Azure або партнерами Azure, для надання технічної підтримки та консультацій щодо гібридної мережі.

Віртуальні мережі Azure схожі на локальну мережу. Ідея віртуальної мережі Azure полягає в тому, що ви створюєте мережу на основі єдиного приватного простору IP-адрес, у якому можна розмістити всі свої віртуальні машини Azure. Доступні простори приватних IP-адрес знаходяться в діапазонах класу A (10.0.0.0/8), класу B (172.16.0.0/12) і класу C (192.168.0.0/16). Не призначайте правила дозволу з широкими діапазонами (наприклад, дозвольте від 0.0.0.0 до 255.255.255.255).

Потрібно переконатись, що процедури усунення несправностей перешкоджають або забороняють встановлення таких типів правил. Ці правила дозволу створюють помилкове відчуття безпеки, і часто їх знаходять і використовують червоні команди.

Найкраща практика: сегментуйте більший адресний простір на підмережі. Використовуйте принципи підмереж на основі CIDR для створення підмереж. Створіть елементи керування доступом до мережі між підмережами. Маршрутизація між

підмережами відбувається автоматично, і вам не потрібно вручну налаштовувати таблиці маршрутизації. За замовчуванням між підмережами, які ви створюєте у віртуальній мережі Azure, немає елементів керування доступом до мережі.

Використовуйте групу безпеки мережі для захисту від небажаного трафіку до підмереж Azure. Групи безпеки мережі (NSG) — це прості пристрої перевірки пакетів із збереженням стану. NSG використовують підхід із 5 кортежів (вихідний IP-адреса, вихідний порт, цільова IP-адреса, цільовий порт і протокол рівня 4), щоб створити правила дозволу/заборони для мережевого трафіку. Ви дозволяєте або забороняєте трафік до та з однієї IP-адреси, до та з кількох IP-адрес або до та з цілих підмереж.

Коли ви використовуєте групи безпеки мережі для контролю доступу до мережі між підмережами, ви можете розмістити ресурси, які належать до тієї самої зони безпеки або ролі, у їхніх власних підмережах.

Уникайте невеликих віртуальних мереж і підмереж, щоб забезпечити простоту та гнучкість. Більшість організацій додають більше ресурсів, ніж спочатку планувалося, і перерозподіл адрес є трудомістким. Використання невеликих підмереж додає обмежену цінність безпеки, а зіставлення групи безпеки мережі для кожної підмережі додає додаткових витрат. Визначте підмережі широко, щоб забезпечити гнучкість для зростання.

Спростіть керування правилами груп безпеки мережі, визначивши групи безпеки додатків. Визначте групу безпеки програми для списків IP-адрес, які, на вашу думку, можуть змінитися в майбутньому або використовуватимуться в багатьох групах безпеки мережі. Обов’язково чітко назвіть групи безпеки програми, щоб інші могли зрозуміти їхній вміст і призначення [22].

Коли ви розміщуєте віртуальну машину у віртуальній мережі Azure, віртуальна машина може підключатися до будь-якої іншої віртуальної машини в тій же віртуальній мережі, навіть якщо інші віртуальні машини знаходяться в різних підмережах [23]. Це можливо, оскільки набір системних маршрутів, увімкнених за замовчуванням, дозволяє цей тип зв’язку. Ці маршрути за замовчуванням дозволяють віртуальним машинам в тій

самій віртуальній мережі ініціювати з’єднання одна з одною та з Інтернетом (лише для вихідного зв’язку з Інтернетом). Хоча системні маршрути за замовчуванням корисні для багатьох сценаріїв розгортання, бувають випадки, коли потрібно налаштувати конфігурацію маршрутизації для своїх розгортань. Ви можете налаштувати адресу наступного стрибка для досягнення певних пунктів призначення [24].

Ми рекомендуємо вам налаштувати маршрути, визначені користувачем, під час розгортання пристрою безпеки для віртуальної мережі.

Висновки за розділом 3

У третьому розділі було розроблено конкретні рекомендації та методики для побудови гібридної, відмовостійкої інфраструктури банку з метою забезпечення високого рівня безпеки. Враховуючи різноманітні сфери банківської структури, були надані рішення та засоби для ефективного захисту інформаційного периметру.

Одним з ключових аспектів було використання технічно-апаратних комплексів, таких як Next-Generation Firewall (NGFW), для забезпечення безпеки мережі та захисту від різних видів загроз. Для захисту чутливої інформації були рекомендовані рішення, такі як системи резервного копіювання даних (Backup), системи запобігання витоку даних (Data Loss Prevention - DLP) та механізми розмежування прав доступу працівників.

У контексті захисту WEB-застосунків, було рекомендовано використовувати рішення Web Application Firewall (WAF), що забезпечують виявлення та захист від вразливостей та атак на веб-додатки.

Для побудови гібридної інфраструктури, було запропоновано використання хмарного рішення Azure, яке забезпечує гнучкість, масштабованість та безпеку для банківських операцій.

Ці рекомендації та методики є важливими для забезпечення безпеки банківської інформації, запобігання вразливостям та зловживанням, а також для збереження довіри

клієнтів та стабільності банківських операцій. Важливо впроваджувати ці рекомендації на рівні організації та забезпечувати постійний моніторинг та оновлення системи за потреби. Крім того, рекомендації стандартів та методики забезпечення безпеки повинні бути постійно оновлювані, оскільки загрози та технології швидко змінюються.

Побудова гібридної, відмовостійкої інфраструктури, застосування технічно-апаратних комплексів, резервного копіювання даних, систем DLP, розмежування прав доступу та захист WEB-застосунків є лише деякими аспектами комплексного підходу до забезпечення безпеки банку. Варто зазначити, що безпека інформації - це неперервний процес, який потребує уваги та регулярного оновлення.

ВИСНОВКИ

В роботі виконано поставлені перед її початком задачі, проаналізовано різноманітні методи забезпечення безпеки банківської інфраструктури.

Банківська діяльність – це комплекс фінансових операцій, які здійснюються комерційними банками з метою збереження, розмноження та розподілу грошових коштів у межах економічної системи. Актуальність банківської діяльності пояснюється її ключовою роллю у фінансовій системі та економіці загалом.

Був досліджений міжнародний стандарт PCI DSS, який регламентує набір вимог, розроблених Консорціумом індустрії платіжних карт (PCI SSC), з метою забезпечення безпеки обробки, зберігання та передачі даних платіжних карт.

У другому підрозділі було розібрано постанову Національного Банку України під номером 95, яка регламентую безпеку банківської інфраструктури у банках України.

У третьому підрозділі був детально розібраний міжнародний стандарт ISO/IEC 27002.

Було розроблено конкретні рекомендації та методики для побудови гібридної, відмовостійкої інфраструктури банку з метою забезпечення високого рівня безпеки. Враховуючи різноманітні сфери банківської структури, були надані рішення та засоби для ефективного захисту інформаційного периметру.

Для захисту чутливої інформації були запропоновані рішення з резервного копіювання даних, система DLP (Data Loss Prevention), яка дозволяє виявляти, контролювати та запобігати витоку конфіденційної інформації, а також розмежування прав доступу працівників, що дозволяє обмежувати доступ до конкретних ресурсів залежно від ролі та потреб користувача. Для захисту WEB-застосунків запропоновано використання рішень класу WAF (Web Application Firewall), які дозволяють виявляти та захищати веб-додатки від різноманітних атак.

Окрім того, було висвітлено важливість використання хмарних технологій,

зокрема хмарного рішення Azure, для побудови гібридної інфраструктури банку. Це дозволяє поєднувати локальні та хмарні ресурси, забезпечуючи гнучкість, масштабованість та високу доступність системи. Хмарні технології також надають широкий спектр інструментів для забезпечення безпеки, включаючи механізми шифрування, моніторингу, ідентифікації та автентифікації.

Застосування цих рекомендацій і методик забезпечує банкам можливість створити надійну та безпечну інфраструктуру, що забезпечує захист конфіденційної інформації, запобігає кібератакам та забезпечує довіру клієнтів. Однак варто пам'ятати, що безпека - це постійний процес, і банки повинні постійно оновлювати та вдосконалювати свої заходи безпеки, враховуючи постійні зміни загроз та технологій.

Забезпечення інформаційної безпеки є невід'ємною частиною діяльності будь-якого банку. У цій роботі ми проаналізували різноманітні методи та нормативні документи, що регламентують безпеку банківської інфраструктури. Система інформаційної безпеки має бути належно налагодженою та ефективною, щоб забезпечувати захист банку від кіберзагроз та зберігання конфіденційної інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Батлер Б., Джонсон Б., Сідуел Е. Оксфордський тлумачний словник. 2003. Режим доступу до ресурсу: http://vocable.com/dictionary/533/word/banking-bankovskaja-dejatelnost

2. Ортинський В. Основи держави і права України. Вид. друге, допов. і переробл. Львів: Оріяна-Нова, 2005. – 368 с.

3. Банківська енциклопедія за ред. А. М. Мороза. Ельтон, 1993. – 336 с.

4. Про банки і банківську діяльність: Закон України від 07.12.2000 No 2121-III. Режим доступу до ресурсу: http://zakon4.rada.gov.ua/laws/show/2121-14

5. Домарєв В. В. Обґрунтування основних функцій системи управління інформаційною безпекою. Вісник Державного університету інформаційно-комунікаційних технологій. 2012. Т. 10, No 2. С. 102-104.

6. Шевчук О., Небесний Р. Заходи безпеки інформації у комп'ютерних системах. 2018. Режим доступу до ресурсу: https://core.ac.uk/download/pdf/161835086.pdf.

7. Securing Information Technology for Banks and Accounting Information Systems. 2018. Режим доступу до ресурсу: https://www.ripublication.com/ijaer18/ijaerv13n6_21.pdf.

8. Payment Card Industry Data Security Standard. 2022. Режим доступу до ресурсу: https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf.

9. Постанова НБУ №95. 2017. Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/v0095500-17.

10. International Standard ISO/IEC 27002. 2013. Режим доступу до ресурсу: https://trofisecurity.com/assets/img/ISO-IEC_27002-.pdf.

11. Ткаченко В. Периметр щезає, а NGFW — ні. Режим доступу до ресурсу: http://sib.com.ua/sib-02-117-2021/ngfm.html

12. Microsoft documentation. Режим доступу до ресурсу: https://learn.microsoft.com/en-us/sql/relational-databases/security/encryption/transparent-data-encryption?view=sql-server-ver16

13. Broadcom. Режим доступу до ресурсу: https://www.broadcom.com/products/cybersecurity/information-protection/data-loss-prevention

14. Qualys. Режим доступу до ресурсу: https://www.qualys.com/

15. IBM documentation. Режим доступу до ресурсу: https://www.ibm.com/products/qradar-siem

16. Cybersecurity Maturity Model, 13.01.2021. Режим доступу до ресурсу: https://www.securitymagazine.com/articles/94324-cybersecurity-maturity-model-certification-center-of-excellence-partners-with-capitol-technology-university

17. Впровадження IdM-системи Oracle. Режим доступу до ресурсу: https://si-solutions.com.ua/portfolio-posts/idm-integration/

18. IBM documentation. Режим доступу до ресурсу: https://www.ibm.com/products/backup-and-restore-manager-for-zvm?mhsrc=ibmsearch_a&mhq=IBM%20Backup%20and%20Restore%20Manager%20for%20z%26sol%3BVM

19. IBM documentation. Режим доступу до ресурсу: https://www.ibm.com/downloads/cas/L9MD4MEZ

20. ОРГАНІЗАЦІЙНІ ОСНОВИ ЗАБЕЗПЕЧЕННЯ БАНКІВСЬКОЇ БЕЗПЕКИ. О. Л. Пластун, 2011 Режим доступу до ресурсу: https://essuir.sumdu.edu.ua/bitstream-download/123456789/56454/7/Plastun_Bankivska_bezpeka.pdf

21. Інформаційна безпека банків: шляхи розв’язання проблеми. Режим доступу до ресурсу: https://journal.bank.gov.ua/archive/2010/5.pdf#page=3

22. Microsoft documentation. Режим доступу до ресурсу: https://learn.microsoft.com/en-us/azure/security/fundamentals/network-best-practices

23. Microsoft documentation. Режим доступу до ресурсу: https://azure.microsoft.com/

24. Онлайн блог Microsoft Azure. Режим доступу до ресурсу: https://habr.com/ru/hub/azure/

ДОДАТОК А

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Тези наукових доповідей:

Жаронкін Максим і Сергій Толюпа.. Захист кіберпростору у банківській сфері. Матеріали V Міжнародної науково-практичної конференції "Проблеми кібербезпеки інформаційно-телекомунікаційних систем (PCSITS)" (Київ, 2023).