Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри кібербезпеки та захисту інформації
_____ Іван ПАРХОМЕНКО
«____» червня 2023 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітній ступень бакалавр

освітня програма Кібербезпека
(назва освітньо-професійної програми)

на тему: Механізми захисту інформації в інформаційних систем у банківських установ

Виконавець: студент IV курсу, групи КБ-41

Сергій ЛУЦЕНКО
(підпис) (ім'я, прізвище)

	Ім'я, прізвище	**Підпис**
Керівник	Сергій ДАКОВ	

Нормоконтроль	Елена БОГУСЛАВСЬКА	

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)

освітньої програми Кібербезпека
(назва освітньо-професійної програми)

Студенту **КБ-41** (група) **Сергію Андрійовичу Луценко** (прізвище ім'я по ')

Тема кваліфікаційної роботи Механізми захисту інформації в інформаційних систем у банківських установ

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема кваліфікаційної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №3 від 20.10.2022 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Модель інформаційної-безпеки банківської системи України

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Необхідно ознайомитися з теорією забезпечення інформаційної безпеки банківського сектору, вразливостями з боку безпеки даних, та коштів банку та його клієнтів
Розробити механізми захисту інформації та надати рекомендації до автоматизованої системи виявлення шахрайств

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність В результаті побудови механізмів безпеки були виділені найбільш впливові на результат нормативи, які враховуються при виявленні кібершахрайств.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 24 жовтня 2022 року

Завдання видав _____ (підпис) Сергій ДАКОВ (ім'я, прізвище)

Завдання прийняла до виконання _____ (підпис) Сергій ЛУЦЕНКО (ім'я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	24.10.2022 – 28.10.2022	*виконано*
2	Аналіз літератури	29.10.2022 – 11.02.2023	*виконано*
3	Обґрунтування вибору рішення	12.02.2023 – 15.02.2023	*виконано*
4	Концепція механізму захисту інформації	16.02.2023 – 04.03.2023	*виконано*
5	Аналіз проблем інформаційної безпеки в банківському секторі	05.03.2023 – 21.03.2023	*виконано*
6	Дослідження вразливостей та загроз	22.03.2023 – 08.04.2023	*виконано*
7	Вироблення рекомендацій до механізму автоматизованого попередження шахрайств	09.04.2023 – 10.05.2023	*виконано*
8	Оформлення пояснювальної записки	11.05.2023 – 27.05.2023	*виконано*
9	Підготовка до захисту кваліфікаційної роботи	28.05.2023 – 12.06.2023	*виконано*

Завдання видав _____ (підпис) Сергій ДАКОВ (ім'я, прізвище)

Завдання прийняв до виконання _____ (підпис) Сергій ЛУЦЕНКО (ім'я, прізвище)

Термін подання кваліфікаційної роботи до ЕК 12 червня 2023 року

РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатків, має 86 сторінок основного тексту, 7 таблиць та 18 рисунків. Список використаних джерел містить 22 найменування.

Метою є розробка механізму захисту інформації в інформаційних систем у банківських установ України.

У процесі підготовки кваліфікаційної роботи було встановлено наступні задачі:

1. Аналіз фінансової безпеки банківського сектора системи України
2. Підходи до оцінки фінансової безпеки банківської системи України
3. Розробка комплексу автоматизованих превентивних заходів попередження шахрайств.

Методи дослідження кваліфікаційної роботи:

- аналіз фінансової безпеки банківського сектора України;
- дослідження підходів до оцінки фінансової безпеки;
- аналіз стандартів безпеки;

Об'єкт дослідження. Процес забезпечення кібербезпеки в банківській системі України.

Предмет дослідження. Методи та механізми оцінки безпеки банківської системи України.

Вивчення та узагальнення вітчизняної і зарубіжної практики. У роботі проаналізована існуюча література та стандарти безпеки для банківського сектору, виконаний аналіз документів, порівняння, вивчення та узагальнення вітчизняної і зарубіжної практики з інформаційної безпеки, як складової фінансової безпеки, розроблено рекомендації для автоматизованої системи попередження шахрайств.

Ключові слова: Захист персональних даних, системи попередження шахрайств, безпека банківського сектору, фінансова безпека, інформаційна безпека. .

ЗМІСТ

СПИСОК УМОВНИХ СКОРОЧЕНЬ

AES	–	Advanced Encryption Standard
API	–	Application Programming Interface
(D)DoS	–	(Distributed) Denial-of-Service
IEEE	–	Institute of Electrical and Electronics Engineers
IoT	–	Internet-of-Things
IPS	–	Intrusion Prevention System
IaaS	–	Infrastructure as a service
IT	–	Information Technology
PaaS	–	Platform as a service
SSL	–	Secure Sockets Layer
SaaS	–	Software as a service
TLS	–	Transport Layer Security
VPN	–	Virtual Private Network
ДПД	–	Діаграма потоків даних
ІКТ	–	Інформаційно-комунікаційні технології
ПЗ	–	Програмне забезпечення
ЦОД	–	Центр обробки даних

ВСТУП

Фінансова безпека банківського сектору нерозривно пов'язана з інформаційною безпекою, і виявлення будьяких проблем важливо для швидкого реагування. Відповідно, важливо враховувати безпеку з боку фінансового сектору. Фінансовий успіх залежить від інформаційної безпеки.

Якщо врахувати останні тенденції, банкам доводеться інвестувати в кіберзахист, купуючи або створюючи сучасні системи виявлення та запобігання шахрайству, які в кінцевому підсумку можуть виявитися неефективними.Причиною цього є те, що банки повинні застосовувати систематичний і послідовний підхід до боротьби з шахрайством. По-перше, необхідне регулювання діяльності персоналу щодо доступу до даних, що дозволить уникнути факту володіння персональною інформацією клієнтів і, як наслідок, її викрадення. Дві стратегії, які включають навчання шахрайству, охоплення громадськості через ЗМІ та Інтернет, оцінку ризику шахрайства в постійному моніторингу. Вдруге необхідно вдосконалити програмно-інформаційне забезпечення автоматизованої банківської системи із збільшенням кількості інтелектуальних технологій обробки, що дозволить виявляти шахраїв на стадії шахрайства, запобігати здійсненню такої операції та ідентифікувати злочинець.

Метою є розробка механізму захисту інформації в інформаційних систем у банківських установ України.

У процесі підготовки кваліфікаційної роботи було встановлено наступні задачі:

1. Аналіз фінансової безпеки банківського сектора системи України
2. Підходи до оцінки фінансової безпеки банківської системи України
3. Розробка комплексу автоматизованих превентивних заходів попередження шахрайств.

Об'єкт дослідження – процес забезпечення фінансової безпеки та кібербезпеки в банківській системі України.

Предмет дослідження – методи та механізми оцінки безпеки банківської системи України.

Практична цінність. В результаті побудови механізмів безпеки були виділені найбільш впливові на результат нормативи, які враховуються при боротьби з кібершахрайством у банківському секторі.

РОЗДІЛ 1 АНАЛІЗ ФІНАНСОВОЇ БЕЗПЕКИ БАНКІВСЬКОЇ СИСТЕМИ УКРАЇНИ

1.1 Банківська система України як об'єкт фінансової безпеки

Набір різних типів національних банків і кредитних установ, що діють на основі спільних фінансових механізмів, називається банківською системою. Банківська система складається з мережі центральних банків, комерційних банків та інших кредитних і розрахункових центрів .

Банки розвиваються як елемент банківської системи, який співпрацює з іншими елементами банківської інфраструктури. Розвиток банків можливий лише як елемента , який взаємодіє з іншими елементами,

Елементи банківської інфраструктури :

- Правовий(Юридичний) кодекс;
- Внутрішні правила роботи операції
- побудова інфраструктури обліку, звітності та аналізу бухгалтертерії ;
- Структура апарату управління банком.
- основні функції системи включають в себе]?
- забезпечення економічної функції та розвитку шляхом надання банківських кредитів та організації платіжних систем;
- перерахування коштів від кредиторів до позичальників і від продавців до покупців;
- Накопичення вільних ресурсів в Україні; ·
- Власне виготовлення, постачання продукції та надання кредитів за потреби.

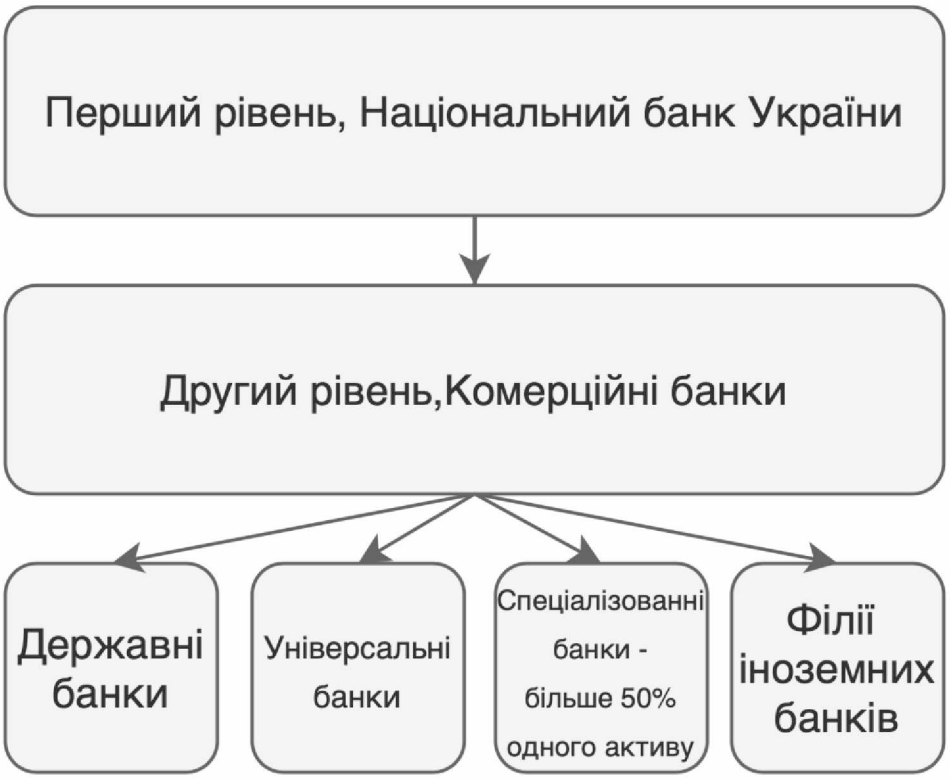

Рисунок 1.1 – Банківська система України

Національний банк України є центральним банком, який реалізує монетарну політику єдиної держави для забезпечення стабілізації та зміцнення її валюти. Банки створювалися державою та приватними особами. Вони організовані компаніями або приватними особами, капітал яких вказано на акціях компанії або акціонерах. Банки мають право виконувати власні функції, провадячи такі види діяльності, як банківські депозити, недепозитні інвестиції та особисте фінансування. Банки здатні виконувати такі операції, як: організаційні фінанси в цілому, інвестиції в цінні папери для юридичних або фізичних осіб; кредитні операції з юридичними установами великих компаній

Нижче описано структуру банківського сектора в Україні за двома методами поділу, які її характеризують.

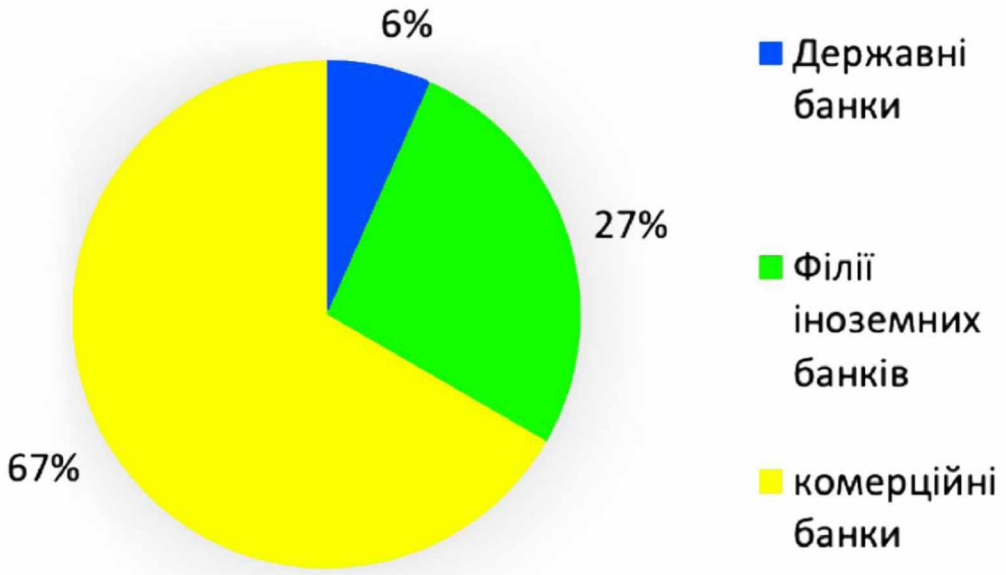

Рисунок 1.2 – Банки за формою власності

Національний банк України виділяє спеціалізовані ощадні банки. Інші названі Національним банком України універсальними.

Таким чином ми маємо 88% універсальних банків, та 12% спеціалізованих ощадних.

1.2 Фінансова безпека як частина кібербезпеки

Неспроможність правильного функціонування призводить, внаслідок неспроможності банківської системи чи її учасника забезпечити належне функціонування, до порушень чи спотворень, які впливають на всю економічну діяльність і розвиток держави.

В економічно-силовому відомстві необхідно захистити національні інтереси від несприятливих умов внутрішніх і зовнішніх процесів. Економічна безпека – стан економіко-силового відомства, що забезпечує захист національних інтересів, соціальну політику та ефективний захист, у тому числі за несприятливих умов внутрішніх і зовнішніх обставин.

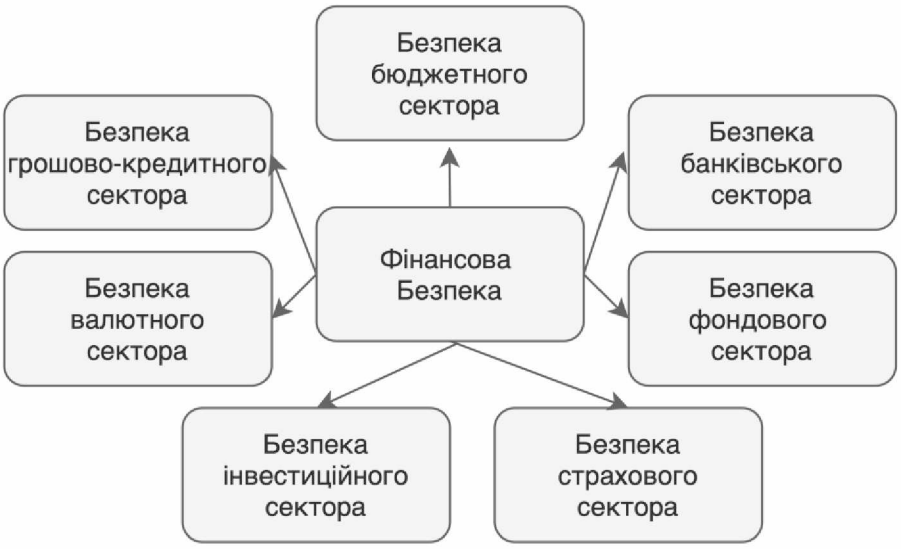

Рисунок 1.3 – Складові фінансової безпеки

Система економічної безпеки банківського сектору побудована на наступних принципах:

- Складність системи захисту.
- пріоритет запобіжних заходів у разі вторгнення.
- Безперервність роботи.
- Законність вжитих методів захисту.
- Ощадливість та ціна вжитих методів чи комплексов захисту.
- Взаємодія модулів захисту чи підрозділів системи.
- Здатність системи.

Найбільш характерні такі загрози :

- низька якість капіталів банків;
- інтеграція кредитної політики з високим рівнем ризику банками;
- недостатня ефективність нагляду;
- недостатня компенсація депозитів системою страхування депозитів;
- ліквідність банківських активів низька;
- низький рівень кредитоспроможності підприємств у фактичному секторі економіки.

Непрямі фактори, котрі вважаються суттєвими для визначення рівня економічної безпеки :

- рівень конкуренції між банківськими установами;
- якість банківського нагляду чи якість управління банком;
- економічний статус галузі;
- національна валюта та економічна політика знаходяться в положенні стабільності.

1.3 Аналіз загроз банківській системі України

Для моделювання фінансової безпеки банківського сектора України слід розуміти актуальні загрози .

Національний банк України здійснює статистичний аналіз основних загроз для банківського сектора.

Таблиця 1.1

Фактори та заходи щодо зменшення негативного впливу

Фактори	Заходи зменьшення негативного впливу
Під час планового швидкого вилучення групою клієнтів, вкладників регулярно розміщених грошових коштів із банків, планується їх швидке вилучення. Це призводить до підриву його платоспроможності	Необхідно диверсифікувати пасиви, щоб захистити незалежність банку від джерела фінансування, поведінку якого неможливо передбачити
Блокування іншими фінансовими установами активів банку	Розміщення основних рахунків лише в авторитетних фінансових

Фактори	Заходи зменьшення негативного впливу
	установах. Моніторинг їх фінансового стану і політичних залежностей.
Фіктивне банкрутство - це ті підприємства, що є позичальниками банків, борги яких знижують його платоспроможність;	Введення в керівництво(Рада, Правління) підприємств - значних позичальників представників банку
Використання ЗМІ для дискредитації банківської установи;	Рекламна компанія спрямована на підтримку постійного позитивного іміджу, а також організацію заходів, спрямованих на забезпечення прозорості фінансового стану банку.
Політичний вплив на рух капіталів (управління рахунками держпідприємств і організацій, фондів і тощо)	Особливо важливою є самостійність або скорочення залежності від політичних впливів, а також виконання всіх вимог, встановлених законодавством, під час проведення цих операцій.
Загальна зміна позиціонування банку на певних ринках банківських послуг, що призводить до його відсторонення від цих ринків.	Реалізація стратегії з урахуванням розумної цінової політики та включення банку до регіональних економічних проектів.

Фактори	Заходи зменьшення негативного впливу
Застосування демпінгових стратегій на ринку послуг.	Впровадження постійних заходів з метою покращення продуктивності та зниження витрат на надання банківських послуг.
Відтік кваліфікованого персоналу через їх переход до конкуруючих банків із втратою ключових кадрів.	Здійснення обґрунтованої кадрової стратегії, встановлення справедливої оплати праці та забезпечення соціального захисту для співробітників.

Національний банк України виокремлює шість загроз:

- кредитний ризик;
- ризик достатності капіталу;
- ризик ліквідності;
- юридичний ризик;
- валютний ризик;
- ризик прибутковості.

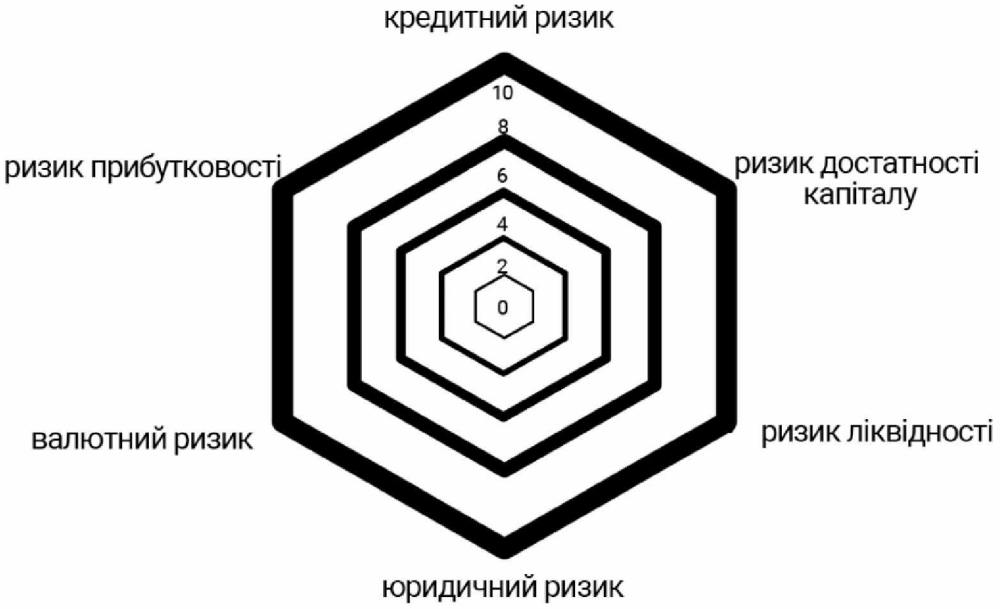

Рисунок 1.4 – Картка ризиків

Наприклад, у поточний період вимоги до оцінки кредитного ризику є набагато вищими, вимагаючи від банків швидкого та ефективного реагування на погіршення портфеля шляхом управління адекватними резервами, а також капіталом для потенційних збитків. Щорічний стрес-тест, запроваджений НБУ, сприяє підготовці сектору до макроекономічних шоків і сприяє створенню резервів капіталу. Річний стрес-тест використовується НБУ, який стимулює реакцію на економічні шоки та стимулює виробництво резервів капіталу. У лютому 2021 року норматив достатності основного регулятивного капіталу на кінець березня 2020 року становив 28,3%, а у 2022 році – 21,3%. Найголовніший – 22,3 відсотка.

Фінансові установи з високим ризиком належать до тих, які мають корпоративні кредити, вони дуже зосереджені в цій сфері. а також ті, які працюють тільки в сегменті кредитування фізичних осіб

Криза має особливість: зростання ризиків для банків, які активно кредитують малий і середній бізнес. Під час щорічних стрес-тестів неможливо спрогнозувати великі втрати в сегментах МСБ, оскільки вони толерантні до попередніх кризових шоківю Швидкий стрес-тест забезпечує таке ж усвідомлення ризику, як і щорічні повні стрес-тести, але є відмінності.

- Кредитний ризик - основний з точки зору впливу на капітал.

- Впровадження процентного ризику в експрес-стрес-тесті незначне порівняно зі стрес-тестом попереднього року.
- Ризик зниження попиту на банківські послуги.
- Валютний ризик,який реалізується за умови помірної девальвації.

Для зменшення наслідків кризи банкам необхідно вживати заходів щодо запобігання негативним наслідкам кризи.Банки повинні поєднувати антикризове управління власним кредитним портфелем та операційною діяльністю з активним антикризовим управлінням кредитним портфелем банку включаючи наступне:

- Надання реструктуризації позичальникам, управління

погіршенням портфеля та своєчасне реагування.

- Можна своєчасно підготувати активи з низькою якістю та високим кредитним ризиком.
- Зменшувати депозит з урахуванням рівня дисконтної ставки, а також у разі зміни макроумов;
- Підвищення операційної ефективності, зокрема за допомогою онлайн-інструментів.

1.4 Сутність операційного ризику банку та класифікації, що використовуються в системі управління ним в сфері інформаційної безпеки

Причиною підвищеної уваги банківського контролю та вітчизняних банків до управління інформаційною безпекою (ІБ) є постійне вдосконалення, а також безпрецедентний рівень зовнішніх і внутрішніх загроз у цій сфері. Крім того, те, що можна досягти прямих збитків, а непрямі збитки в разі їх реалізації будуть великими.

Банківська інформаційна система, чутлива до збільшення кількості загроз, які можуть бути спричинені зовнішніми зловмисними та злочинними діями,або особистим шахрайством (помилками або шахрайством співробітників) , чи наприклад природні та штучні катастрофами\випадками. Це пов'язано з тим, що банки:

- Здатні зберігати та обробляти надмірну кількість даних про фінансовий стан, та інформацію про діяльність як фізичних, так і юридичних осіб, клієнтів та контрагентів, інших банківських установ.
- Мати інструменти транзакцій, які призводять до фінансових наслідків; -
- Вони не повністю закриті, оскільки мають відповідати сучасним вимогам обслуговування клієнтів у частині дистанційних надання послуг.

Відслідковування ключових довгострокових подій у банківському бізнесі вплине на те, як забезпечується інформаційна безпека та які ризики ІБ зростають у банках,а саме:

1) розвиток комунікаційних систем, що є фундаментальним драйвером змін у сфері надання фінансових послуг та взаємодії з клієнтами;

2) інтеграція – підвищення інтеграції інформаційних потоків і додатків, що дозволить трансформувати потік фінансової інформації та архітектуру фінансових додатків;

3) модульність, технологія інтеграції призводить до розвитку «модульної економіки», в якій бізнес-діяльність поділяється на невеликі елементи, які можна об'єднати в організаційних і національних межах. Це пояснюється її успіхом у створенні «інтегрованої економіки».

Порушення принципів конфіденційності,цілісності, доступу до інформації, відсутність контролю за змінами в інформації або можливість несанкціонованого доступу до неї може не тільки завдати збитків окремому банку, але й призвести до повної зупинки бізнес-процесів. Причиною цього є відсутність ризиків і наслідків від їх порушення.

Банківська система є частиною найважливішої та стратегічної інфраструктури країни, збої в її роботі можуть дестабілізувати фінансову та економічну системи. Масштабна кібератака 2017 року, здійснена за допомогою вірусу Petya.A, була спрямована на об'єкти критичної інфраструктури України, зокрема банки. У НБУ повідомили, що від кібератаки різного ступеня постраждали близько 30 українських банків.

У зв'язку з цим питання забезпечення інформаційної безпеки українських банків набуває особливого значення.

Для досягнення поставленої мети важливо дослідити сутність поняття «інформаційна безпека банку». У результаті вивчення наукових праць з даної теми ми визначили наступні підходи авторів до визначення цього поняття. Ними пропонуютьсярозглянути наступні крітерії : І

1. Як стан безпеки,різні джерела визначають різні об’єкти, які охоплюються необхідністю захисту інформації:

- Всі інформаційні активи банку проти внутрішніх і зовнішніх загроз Інформаційні активи – це будь-яка інформація, яка має цінність для банку, системи його обробки або місця зберігання .
- Крім того, це – системи обробки та зберігання даних, які забезпечують конфіденційність інформації. створення систем обробки та зберігання даних, під контролем яких забезпечується захист цілісності та конфіденційності інформації, а також комплекс заходів щодо захисту інформації від несанкціонованого доступу, використання, розголошення, знищення, модифікації, перегляду.
- Необхідно захищати інформацію та її допоміжну інфраструктуру від випадкових або навмисних дій штучного або природного характеру, які можуть призвести до завдання шкоди людям, які їй користуються у комунікаційних відносинах, зокрема користувачам і власникам інформації та інфраструктури. що підтримує її.
- інформаційні ресурси банку від внутрішніх і зовнішніх нападів.

2. Як сукупність методів і засобів (організаційних, методичних або технічних) захисту інформації від:

- загроз, які спрямовані на забезпечення продовження бізнес-процесів, зниження ризиків та оптимізацію витрат банку:
- Випадкова і навмисно виникла загроза, в результаті чого реалізація служб (властивостей) безпеки: доступності, цілісності, конфіденційності ;

- Широкий спектр загроз використовується для захисту щоб забезпечити безперервну роботу бізнесу, мінімізувати ризик бізнес-процесів і отримати максимальну віддачу від інвестицій і можливості для бізнесу.

3. Безпека, пов'язана з інформаційною безпекою, тобто: забезпечення безпеки набору властивостей (доступності та цілісності) у сфері даних. Це, а також забезпечення захисту власності особи від факторів ризику, таких як доступ до конфіденційності та автентичності інформаційних активів. .

Наприклад, згідно з результатами дослідження ІБ у банку, ми пропонуємо визначити стан безпеки інформаційних активів та інформаційних мереж, що забезпечує оптимальний рівень властивостей (конфіденційність,доступність або цілісність) під впливом зовнішніх і внутрішній тиск.

Відповідно до системи підтримки ІБ банку, інформаційні активи - це матеріальні або нематеріальні об'єкти, які містять інформацію та служать для обробки, зберігання або передачі інформації. Цінність цього визначається його використанням як об'єкта системи підтримки ІБ. У внутрішніх політиках і планах управління ІБ кожен банк самостійно визначає свій склад інформаційних активів, що розглядаються як об’єкти інформаційної безпеки. Склад описано в термінах об’єкта захисту інформації. Це основний критерій для цього, оскільки важливо враховувати важливість і цінність інформаційного активу для діяльності банку.

Як наслідок, основними типами банківських інформаційних активів, які є вразливими до ризиків інформаційної безпеки, є комерційна та банківська таємниця, конфіденційні дані та персональні дані. На інформаційну безпекубанку впливає велика кількість зовнішніх та внутрішніх загроз, які породжені як зовнішнім, так і внутрішнім середовищем. Необхідно визначити та скласти можливі негативні впливи (загрози) на інформаційні активи, способи реалізації та ступінь.Це вразливість ІБ банку, і є ймовірність реалізації цих загроз

В результаті адаптації загальних знань про поняття «загроза» до дослідницьких завдань ми визначаємо, що банку ІБ загрожує випадкова або навмисна подія, дія (вплив), процес або явище, які можуть призвести до втрати інформаційних активів. та інформаційної мережі, або порушення властивостей інформаційних активів. Загроза ІБ банку – це потенційно можливий випадковий інцидент, дія (вплив) у разі неотримання або несвоєчасного отримання інформації легальними користувачами.

Зазначать, що загрози ІБ полягають
у повному або частковому припиненню роботи системи, а також втрати вартості та часткове знецінення інформації можуть призвести до прямих і непрямих збитків з боку банку. Узагальнюючи нововведення вчених, які займалися загальною класифікацією загроз та об'єднували їх уявленням про «інформаційну безпеку банків», вважаємо за доцільне.

До найважливіших загроз пропонується віднести такі основні типи загроз (таблиця 1.2).

Таблиця 1.2

Класифікація загроз ІБ банку.

Ознака	Вид загрози
За джерелом	- Внутрішні події, такі як втрата, знищення, викрадення, викривлення або розголошення інформації, а також витік інформації. Зовнішні події, які включають модифікацію змісту, порушення конфіденційності, порушення логічної цілісності, порушення прав власності на інформацію, порушення фізичної цілісності, природні та техногенні катастрофи, що порушують нормальний режим роботи інформаційних систем та інші подібні події.
	- Природні обставини, що характеризуються впливом фізичних процесів або стихійних природних

Ознака	Вид загрози
За походженням	явищ на об'єкт захисту, які не залежать від людської діяльності. - Суб'єктивні фактори, що характеризуються впливом людської діяльності на об'єкт захисту. - Результати соціальної інженерії, які включають фішинг, фармінг, претекстинг, скрімінг та інші методи.
За ступенем впливу на інформаційну систему	- Пасивні, не впливають на стан інформаційної системи. - Активні, які порушують нормальний процес функціонування інформаційної системи банку.
За цілеспрямованістю	- Невідомі (ненавмисні, випадкові, необдумані, без злого наміру та корисливих цілей) дії персоналу та користувачів банківських послуг. - Усвідомлені (з корисливими цілями, під примусом третіх осіб, зі злим умислом тощо) дії персоналу, користувачів банківських послуг, злочинних груп та структур, політичних і економічних формувань, а також окремих осіб.
За способом реалізації	- розголошення; - витік; - несанкціонований доступ.
За ступенем сформованості	- реальні; - потенційні.
За можливістю прогнозування	- прогнозовані; - не прогнозовані;
За ймовірністю виникнення	- реальна; - ймовірна; - малоймовірна; неймовірна.
	- - Відкриті, прямі (загрози, реалізація яких прямо шкодить безпеці інформаційних активів).

Ознака	Вид загрози
За характером впливу	- - Приховані, опосередковані (загрози, що створюють умови для виникнення прямих загроз).
За масштабами наслідків	- катастрофічні; - критичні; - середні; - незначні.
За можливістю нейтралізації	можливо нейтралізувати; можливо частково нейтралізувати; нейтралізувати неможливо.

Таблиця 1.3

Перелік способів реалізації загроз ІБ банку [узагальнено автором]

Рівні ІБ	Об’єкти забезпечення ІБ банку	Способи реалізації загроз
Фізичний рівень	- Фізичні носії інформації, що знаходяться у системах зберігання даних, резервних копіях та на автоматизованих робочих місцях. - Знімні носії інформації та канали зв'язку. - Монітори. - Приміщення, будівлі та споруди. - Технічні засоби інформаційних систем.	Розкрадання / крадіжка
		Знищення / руйнування / диверсії
		Несанкціонований фізичний доступ
		Витік інформації
Мережевий рівень	Комунікаційне обладнання.	Атаки «відмова в обслуговуванні»
		Заміна довіреного об'єкта мережі та передача повідомлень через канали зв'язку від його імені з наданням його прав доступу.

Рівні ІБ	Об’єкти забезпечення ІБ банку	Способи реалізації загроз
		Порушення штатних режимів роботи мережевого обладнання
		Впровадження апаратних закладок
Рівень мережевих додатків і сервісів	Мережеві додатки та сервіси.	Впровадження шкідливого ПЗ
		Аналіз трафіку
		Атаки «відмова в обслуговуванні»
		Використання спеціалізованих програм
		Порушення штатних режимів роботи мережевих
Рівні ІБ	Об’єкти забезпечення ІБ банку	Способи реалізації загроз
		додатків
		Сканування мережі, спрямоване на виявлення відкритих портів та служб, відкритих з’єднань
Рівень операційних систем	- Файли, що містять персональні дані, банківські та комерційні таємниці. - Загальносистемні програмні засоби, що містять інформацію, необхідну для ідентифікації, автентифікації та (або) авторизації.	Крадіжка / втрата паролів
		Копіювання
		Модифікація / видалення
		Порушення штатних режимів роботи операційних систем
		Поширення шкідливих програм
		Неправильна (неповна) конфігурація систем захисту інформації

Рівні ІБ	Об'єкти забезпечення ІБ банку	Способи реалізації загроз
	- Файли з відкритою інформацією.	Несанкціонований логічний доступ до операційних систем з використанням спеціалізованого ПЗ
Рівень систем управління базами даних	У базах даних інформаційних систем міститься важлива інформація, що використовується для ідентифікації, автентифікації та (або) авторизації користувачів.	Копіювання
		Модифікація
		Неправильна (неповна) конфігурація систем захисту інформації
		Модифікація / видалення
		Порушення штатних систем режимів роботи управління базами даних
		Підміна ідентифікаторів користувача
		Несанкціонований логічний доступ до управління базами даних систем
		Поширення шкідливих програм
		Крадіжка паролів
Рівень банківських технологічних процесів та програм	Програмне забезпечення для обробки особистих даних, банківської та комерційної інформації, програмне забезпечення для обробки відкритої інформації,	Модифікація / видалення
		Розповсюдження / передача
		Друк документів
		Крадіжка документів та карток

Рівні ІБ	Об’єкти забезпечення ІБ банку	Способи реалізації загроз
	пластикові картки, інформація, необхідна для ідентифікації, автентифікації та (або) авторизації, паперові документи.	Крадіжка паролів
Рівень бізнес-процесів	Дані обмеженого доступу Персонал	Саботаж
		Халатність та помилки
		Шкідництво

Модель аналізу загроз ІБ Банку є основою для створення внутрішньобанківського заходу, який зосередиться на нейтралізації ризиків методами технічного захисту інформаційних систем від несанкціонованого доступу, попередження несанкціонованого впливу на програмні засоби та обладнання.

Для забезпечення працездатності ІБ банку з метою захисту його безпеки рекомендується сформувати модель порушника (організації, зацікавленої в отриманні прибутку від порушень шляхом порушення інформаційних активів), розділивши їх за типом і розміром. Це також допомагає визначити, який тип ризику буде націлений на нього самого.

Крім того, підсумовуючи напрацювання з даного питання, пропонуємо таку структуру порушників інформаційної безпеки банку (табл.). Порушники інформаційної безпеки банку об'єднані в наступну таблицю: 1.4).

Передумови для реалізації загрози ІБ формуються за наявності внутрішніх слабких місць у системі підтримки ІБ банку, як наслідок:

- збитки, пов'язані з втратою, витоком або недоступністю інформації, зі знищенням і подальшим відновленням інформації;
- збитки від дезорганізації діяльності банку та заборгованості, пов'язані з невиконанням ним зобов'язань
- Репутаційні втрати

- збитки від реалізації правового ризику внаслідок санкцій з боку клієнтів, контрагентів та регулятора.

Ризики інформаційної безпеки є невід'ємною частиною операційних ризиків банку.

Загальновизнаним є визначення операційного ризику згідно з Базельською угодою: «...ризик збитків, що виникає в результаті неадекватних або помилкових внутрішніх процесів, дій співробітників і систем або в результаті зовнішніх подій. Поняття включає юридичний ризик, але виключає стратегічний ризик та ризик втрати ділової репутації».

Кримінальні ризики включають, але не обмежуються ризиком штрафів, пені або штрафних збитків у результаті судових позовів. У цьому випадку також можливі приватні позови.

З точки зору методичних рекомендацій щодо управління ризиками, банки піддаються операційному та технологічному ризику: «...потенційна загроза для стану через неадекватність або збій внутрішніх систем, персоналу та системних компонентів або зовнішніх подій, що проявляється у зміні мережі прибутку та/або власного капіталу».

У багатьох визначеннях використовується непрямий підхід до операційного ризику або той, який поєднується з прямим і непрямим підходами до визначення операційного ризику, тобто вони означають ризики, які не підпадають під іншу категорію банківських ризиків (процентна ставка кредитного ринку), та розраховується як резервна вартість. Якщо використовувати непрямий підхід, то неможливо управляти якістю. Практичне застосування непрямого підходу об'єднує в одну групу стільки різних ризиків, що управління ними стає неможливим.

Через недостатню вивченість, а також дефіцит ризиків інформаційної безпеки з наукової літератури, а також через проблему уніфікації з чинним законодавством про правові ризики в Україні та інших країнах. Необхідно чітко розмежовувати операційний стратегічний та правовий ризики для підвищення ефективності управління ризиками інформаційної безпеки як складової операційних ризиків.

Отже, підсумовуючи вищесказане:

- Ризики людського фактора (помилки, зовнішнє та внутрішнє шахрайство тощо);
- Ризики техніки (несправність обладнання, його невідповідність, несправність системи,тощо);- Ризики зовнішніх подій (стихійні лиха, катастрофи тощо).

Таблиця 1.4 – Склад можливих порушників ІБ банку Дивітся **додаток Б**

Системи управління операційним ризиком у банках повинні класифікувати події, які несуть операційний ризик наступним чином:

- внутрішнє шахрайство: навмисна відсутність інформації про несанкціоновані операції з данними, навмисне невідображення таких операцій у системі звітності. Можливе створення внутрішньої шахрайської операції, яка передбачає умисне знищення або викрадення документів і конфіденційної інформації у власних цілях;
- Зовнішнє шахрайство: усі випадки внутрішнього шахрайства, але за участю третьої сторони;
- Пошкодження інформаційних активів: внаслідок стихійного лиха (катастрофи, пожежі) або навмисних дій персоналу банку чи інших осіб;
- Порушення в інформаційній системі банку: несправність програмного, технічного та телекомунікаційного обладнання.
- Помилка в управлінні процесом: введення даних, завантаження або передача даних, в обліку та звітності, при наданні зовнішньої та внутрішньої звітності;
- Можливість інших подій, які можуть призвести до операційних ризиків.

Ці операційні ризики в контексті ІБ банку, які призводять до збитків або відсутності прибутку, також є технологічними ризиками, і основними індикаторами для їх підтвердження є :

- Збої та помилки в роботі автоматизованих банківських систем (АБС) за відсутності або недостатнього контролю;
- Внутрішнє та зовнішнє шахрайство, пов’язане з наданням послуг, що реалізується через віддалений доступ до коштів або інформації

• Тимчасові перерви в діяльності банків через вихід з ладу комп'ютерних, телекомунікаційних та інших систем життєзабезпечення банків;

Більшість визначень базується на елементах операційного ризику в контексті ІБ банку на наступному:

1) внутрішні процеси: ризик втрат через недоліки або відсутність чітко задокументованих і добре затверджених процесів для проведення операцій

2) людський фактор: ризик збитків від впливу персоналу, клієнтів, постачальників і зовнішніх партнерів. Ця група включає:

3) Ненавмисні - під час експлуатації інформаційних систем працівниками здійснюються випадкові порушення встановлених стандартів збору та обробки даних, а також інші дії персоналу під час експлуатації. Це призводить до непродуктивних витрат часу і ресурсів, розголошення конфіденційних даних, втрати або несправності окремих робочих станцій, підсистем або всієї системи в цілому;

4) Навмисні - дії осіб з корисливими цілями, примус з боку іншої сторони або зі зловмисним умислом, уповноважених працювати з інформаційними системами, а також працівників, відповідальних за адміністрування, управління та контроль програмного та апаратного забезпечення, засобів, які захищають безпеку даних;

5) Діяльність злочинних груп і формувань у вигляді політичних і економічних структур, а також окремих осіб щодо отримання інформації від людей, нав'язування їм фейкових даних, порушення функціонування системи в цілому та окремих її складових;

6) Помилки в проектуванні інформаційних систем та систем їх захисту, помилки в програмному забезпеченні, збої та відмови технічного обладнання.

7) Саме це джерело ризику є основним і найпоширенішим. Більш імовірно, що людський ризик втрати буде навмисним.

8) Системи: ризик збитків внаслідок відсутності та/або несправностей систем, технологічного обладнання та компонентів системи банку в цілому.

Ризики інформаційної безпеки як об'єкти управління є комплексними, оскільки виникають у зв'язку з проведенням значної кількості операцій з контрагентами, а

отже, зазнають впливу різноспрямованих загроз із зовнішнього та внутрішнього середовища, які призводять до неочікувано високого операційного ризику банку.

1.5 Система управління операційними банківськими ризиками в сфері інформаційної безпеки

Крім того, невід'ємною частиною операційного ризику банку інформаційна безпека. У будь-якому разі, управління ними є складовою ризик-менеджменту банку, а система управління ІБ має бути ризикоорієнтованою. Управлінське рішення приймається на основі аналізу, який порівнює поточний ризик інформаційної безпеки з допустимим.

За результатами дослідження, виявлено, що управління ІБ часто розглядає системний підхід, як частину загальної системи управління банком, яка базується на підході, що враховує ризики інформаційної безпеки як операційні ризики та призначений для розвитку, впровадження, моніторингу роботи, перегляду, підтримки та вдосконалення.

У результаті дослідження ми вважаємо, що управління ІБ банку структурно є організацією з трьома основними підсистемами: методологічною (об'єкти та принципи, призначені для забезпечення ризику інформаційної безпеки), функціональною (набір для моніторингу та контролю обсягу ризиків інформаційної безпеки), функціональні (набір інструментів для ідентифікації, оцінки та моніторингу ризиків безпеки даних) та організаційно-управлінські (суб'єкти, через які здійснюються регулятивні впливи).

Як об'єкти управління ризики інформаційної безпеки як об'єкт управління входять до групи операційних ризиків банку, її елементами є: внутрішні процеси, людський фактор і система. Як об'єкти управління вони складні тим, що виникають як результат багатьох масштабних операцій з контрагентами, на вплив яких впливають різноспрямовані загрози зовнішнього та внутрішнього середовища.

Ця система має забезпечувати безпеку інформаційних активів з урахуванням зовнішніх і внутрішніх ризиків. Система управління ІБ банку повинна забезпечувати

безпеку інформаційних активів у зв'язку з впливом зовнішніх і внутрішніх факторів, а саме:

- конфіденційність – забезпечення того, що інформація не може бути отримана неавторизованим користувачем та/або процесом;
- цілісність, забезпечення того, що інформація не може бути змінена неавторизованим користувачем та/або процесом;
- цілісність системи – забезпечення того, що жоден системний компонент не може бути видалений, змінений або доданий з порушенням політики безпеки
- доступність, гарантія того, що такий об'єкт системи може використовуватися користувачем і/або процесом, який має належний доступ до нього, може використовувати ресурс відповідно до політики безпеки, але не чекати більше заданого періоду. Тобто, коли він у тому вигляді, який вимагається користувачами в потрібний їм час;
- спостережливість - надання такої властивості для запису користувачів і обробки, використання пасивних пристроїв, а також однозначної ідентифікації людей, які беруть участь у подіях, використовується цією системою. Можна надати такі властивості, які дозволять реєструвати дії користувачів, також за допомогою активного визначення імен або ідентифікацій користувачів і систем, що включають певні події, щоб запобігти порушенням політики безпеки/або захистити їх від певного роду дії.

Наприклад, підсумовуючи напрацювання з даної теми та нормативно-правову базу, виділимо наступні вимоги, яких слід дотримуватися при створенні системи управління ІБ для банків:

- Адекватність реальним і потенційним внутрішнім, зовнішнім ризикам безпеки ІБ банку;
- Комплексність – складність та наявність усіх необхідних методів і технік захисту інформаційних активів та захист усіх інформаційних активів, які визначені як важливі чи цінні для банку;

- Безперервність і своєчасність заходів захисту від реальних і потенційних загроз.
- ІБ банку;
- Висока продуктивність - обробка значних обсягів інформації без зниження швидкості виконання;
- Надійність і відмовостійкість системи - досягається за рахунок використання кластеризації, віртуалізації або технології балансування навантаження;
- Інформаційне забезпечення - за рахунок наявності збору, аналізу даних про інциденти та реагування на події безпеки;
- Достатність усіх ресурсів, у тому числі фінансових, для сталого розвитку систем ІБ банку;

Організаційно-управлінська підсистема об'єднує весь персонал, що бере участь у процесі забезпечення безпеки інформації в банку. Вона включає системи управління, які формують загальну систему безпеки інформації, а також системи, які регулюють ризики як невід'ємну складову управління ризиками.

Рисунок 1.5 – Організаційно-управлінська підсистема управління ризиками ІБ банку

Наглядова рада та Правління мають повноваження щодо ефективного управління ризиками ІБ на стратегічному рівні. Вони є лідерами у визначенні

організаційної та управлінської структури ІБ, визначають основні контури організації забезпечення ІБ, розробляють або приймають політику та стратегію її розвитку, політику управління ризиками. Саме вони визначають основні напрями її організації, а також керують адміністрацією ІБ.

Правління банку відповідає за безпосередню організацію та реалізацію процесу управління ризиками, у тому числі за забезпечення ідентифікації, оцінки, контролю та моніторингу ризиків інформаційної безпеки у складі операційних ризиків. Це включає оцінку, ідентифікацію, оцінку, контроль і моніторинг ризиків інформаційної безпеки як частини операційних ризиків.

На тактичному рівні можна виявитиТактичний рівень включає реалізацію функцій управління ризиками ІБ на рівні вищого керівництва та комітетів, що передбачає затвердження політики управління ризиками, впровадження процесів управління ризиками та створення ефективних внутрішніх систем та механізмів контролю, щоб забезпечити збереження ризиків на припустимому рівні. функції управління ризиками ІБ, які виконуються на рівні вищого керівництва та комітетів, тобто затвердження планів управління ризиками для всіх секторів бізнесу, а також створення внутрішніх систем і контролю, які захищають ризик від неприйнятних умов, щоб цей ризик управляється прийнятним способом.

Відповідно до вимог НБУ банк зобов'язаний утворити орган управління ІБ для її функціонування та функціонування або надати ці повноваження існуючому колективному органу управління з чіткими завданнями, функціями та відповідальністю. Склад такого комітету повинен включати голову правління або його заступника, відповідального за інформаційну безпеку, керівників підрозділів, власників критично важливих інформаційних активів та критичних бізнес-процесів, а також керівника підрозділу з управління ризиками. Банки України виконують цю вимогу, більшість з них створили окремі комітети з управління інформаційною безпекою, підпорядковані правлінню, а рішення цих комітетів є обов'язковими для всіх співробітників банку.

Підрозділ з управління ризиками має відповідальність за забезпечення надійного процесу виявлення, оцінки, контролю та моніторингу ризиків

інформаційної безпеки банку. Крім того, на цей підрозділ покладаються функції розробки внутрішніх нормативних актів.

Операційний рівень – це функції управління ризиками ІБ, які здійснюються в підрозділі банку шляхом впровадження правильних контрольних заходів, керуючись відповідними оперативними інструкціями та посібниками. Це робиться під наглядом вищого керівництва. .Зазвичай тут працюють підрозділи – власники критичних інформаційних активів і бізнес-процесів, до яких вони належать,

Необхідно, щоб ці підрозділи впроваджували в свою діяльність політику та порядок управління ризиками ІБ, а також впроваджували нормативні документи банків у частині управління ризиками. Ними виконуються такі функції:

- В межах компетенції цього підрозділу можливо забезпечити функціонування процесів підтримки діяльності у сфері управління ризиками ІБ
- Здійснення ідентифікації та формування управлінських звітів щодо операційних подій, пов'язаних з ризиками інформаційної безпеки.
- Забезпечення дотримання показників якості звітів про операційні події, пов'язані з ризиками інформаційної безпеки.
- Участь у наступному контролі якості даних про операційні події, пов'язані з ризиками інформаційної безпеки.
- Постійний аналіз процесів, продуктів та систем з метою ідентифікації потенційних ризиків інформаційної безпеки в рамках відповідальності.
- Виявлення значних ризиків інформаційної безпеки для проведення сценарного аналізу, включаючи стрес-тестування.
- Участь у сценарному аналізі та стрес-тестуванні ризиків інформаційної безпеки.
- Проведення експертної оцінки ризиків інформаційної безпеки.
- Первинна ідентифікація та оцінка впливу ризиків інформаційної безпеки при впровадженні нових банківських продуктів, систем, проектів, змін у бізнес-діяльності або організаційній структурі і т.д.

•Розробка та впровадження ключових показників ризиків інформаційної безпеки, забезпечення регулярного моніторингу їх динаміки.

•Розробка та впровадження заходів щодо обмеження (контролю) ризиків інформаційної безпеки.

•Підготовка регулярних звітів щодо ризиків інформаційної безпеки (збитки, показники, сценарії, ризикова експозиція, заходи з обмеження ризику тощо).

•Забезпечення участі працівників підрозділу у регулярних тренінгах з ризиків інформаційної безпеки.

•Підтримка та супроводження впровадження нових ІТ-систем та/або рішень з управління ризиками інформаційної безпеки на рівні та в межах функцій підрозділу.

У службі внутрішнього аудиту, яка не бере безпосередньої участі в процесі управління ризиками ІБ і безпосередньо не керує ІБ банку, її роль полягає лише в оцінці відповідності та адекватності цієї системи та вимогам і планам банку.

Функціональна підсистема – це набір інструментів та заходів, які керують банками для формування політики та стратегії управління ІБ, а також система дій для виявлення інформації про ризики у зв'язку з політикою та стратегією управління ІБ банку, а також моніторинг та контроль. Ризики ІБ як складова операційних ризиків.

Це основа управління ІБ банку, якою має стати ефективна політика інформаційної безпеки та комплекс заходів, що дають змогу реалізувати її якістне виконання. Державний банк України зобов'язаний розробити, затвердити в установленому порядку та підтримувати в актуальному стані політику ІБ на підставі її перегляду протягом одного року.

Включаються такі змістовні частини політики ІБ українських банків: визначення мети політики, сфери її застосування, переліки об'єктів, на які поширюється дія ІБ банку, ролі та відповідальність установ, що забезпечують інформаційну безпеку.

Системним документом, який впливає на забезпечення ІБ, є стратегія її розвитку, яку необхідно розробити та затвердити банками. Інформацію про питання забезпечення ІБ мають узагальнювати та затверджувати банки. ІБ політика, стратегічні цілі банку, які пов'язані з новими видами діяльності та продуктами з

використанням технологій, які вимагають захисту інформації, а також враховують плани розвитку ІБ .

Крім того, банк повинен ефективно розробляти, впроваджувати та тестувати плани відновлення бізнесу. Зокрема, необхідно створити план безперервності бізнесу на основі ІБ, щоб не втрачати прибутки від діяльності останнього.

Для забезпечення ІБ банку важливою складовою є успішна система управління ризиками ІБ, яка здійснюється за циклом: « ідентифікація - оцінка та аналіз – мінімізація - моніторинг і контроль».

Для покращення ідентифікації ризиків ІБ в банках необхідно:

по-перше, створити об'єднання персоналу підрозділу управління ризиками та співробітників підрозділів – власників критичних інформаційних активів і бізнес-процесів,

по-друге, розробити системи для виділення окремого виду ризиків ІБ банку, в тому числі тих, що зумовлюють виникнення ризиків ІБ банку, в тому числі тих, що виникають в умовах аутсорсингу.

Наприклад, ефективна оцінка ризиків ІБ у грошовій формі безпосередньо залежить від правильного виявлення її потенційних ризиків, відповідно до напряму діяльності банку. Використання математичних і статистичних моделей, що використовуються для оцінки ринкових, кредитних ризиків або ризиків ліквідності, неможливе як через природу ризиків ІБ (різноманітні загрози, які їх фактично викликають, так і через особливості управління процесами). Ці ризики повинні бути лише мінімізовані, а не оптимізовані, тому інструменти регулювання та контролю є спеціальними). Слід зазначити, що використання математичних і статистичних моделей, які використовуються для оцінки ризиків ІБ, не має шансів.

На основі ризиків ІБ є метод аналізу причинно-наслідкових зв'язків зовнішніх і внутрішніх небезпек, реалізація яких може призвести до певних відхилень від цільових параметрів ІБ банку та її цільового курсу. Фінансові втрати, погіршення репутації, втрати та руйнування в бізнесі, невдоволення клієнтів, санкції керівного персоналу (табл. 1.5).

Top-down models (низхідні моделі) - У низхідних моделях ризики ІБ розглядаються з точки зору його кінцевих результатів у діяльності банку та наслідків, які до них призводять. Банк, як правило, може втратити кошти в разі аварії (Exposure Indicators).

Для ідентифікації ризику використовується база операційних інцидентів (подій, які призвели до збитків). Це класифіковані та згруповані ризики.

Bottom-up models (висхідні моделі) - Основну увагу слід приділити джерелам, тобто причинам ризиків ІБ. Ідентифікація ризиків здійснюється шляхом оцінки реакції співробітників, систем і технологій на загрози ІБ. Цей метод є основним методом декомпозиції всіх дій у банку та всіх дій у кінцевий бізнес-процес із виділенням важливих елементів для інформаційної безпеки. Основним методом є декомпозиція від банків і всіх видів діяльності до кінцевих бізнес-процесів, відбір критичних для інформаційної безпеки на основі аналізу їх продуктивності за стандартами конфіденційності, цілісності та доступності. На основі результатів моделі «знизу вгору» результати можна використовувати, наприклад, для розробки та оцінки методів управління ризиками ІБ.

RSCA – це самооцінка, яку повинні проводити всі підрозділи банку, щоб самостійно оцінити можливий ризик ІБ. При класичному підході в самооцінці беруть участь керівники, підрозділи та ключові особи банку.

Скорингові картки можна використовувати для оцінки ризиків окремої групи, наприклад банківських підрозділів або регіонів. Вони використовуються для оцінки ризиків для окремих груп і дозволяють отримати інформацію про рівень ризику в будь-якій події. Оскільки оцінка, отримана за допомогою скорингових карток, має суб'єктивний характер, але вона дозволяє визначити ймовірність ризикових подій ІБ та чітко визначити, які банки є його джерелом.

Аналіз ключових індикаторів ризику (аналіз KIP) — це інструмент оцінки ризику ІБ, який базується на вивченні еволюції ризику в окремих бізнесах або банках загалом і використовується для моніторингу, контролю та попереднього попередження про зміни.

Аналіз КІР проводиться для раннього розпізнавання та прийняття правильних рішень щодо зменшення втрат від ризику ІБ. Він проводиться з метою виявлення позитивних зрушень в окремих видах господарської діяльності чи діяльності банку в цілому та запобігання або мінімізації збитків від його використання банками.

КІР - використовується у критичних бізнес-процесах банку, для моніторингу ризиків, притаманних певному бізнес-процесу, які значною мірою створюють ІБ-загрози. Цілі цього аналізу: виявлення небажаних тенденцій і запобігання їх реалізації в майбутньому.

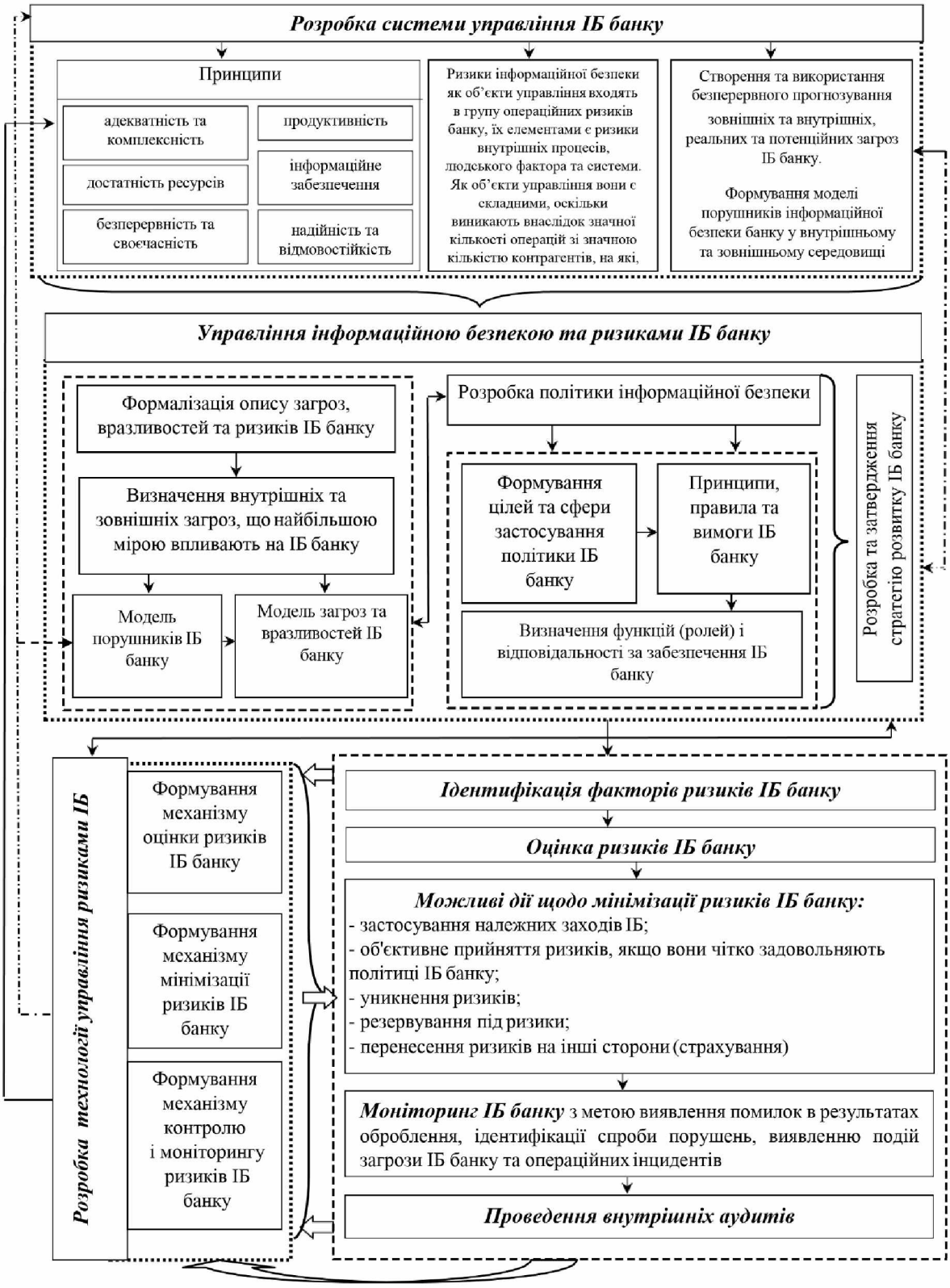

Рисунок 1.6 – Основні функції управління ІБ та ризиками ІБ банку.

Таблиця 1.5 – Наслідки реалізації ризиків ІБ банку дивіться в **додатку Б**

Нижче наведено приклади, які використовують банки для підходу до оцінки ризику ІБ.

Класифікація ключових індикаторів ризиків ІБ базується на наступних типах:

- синхронний індикатор – дані про зареєстровані збитки та включають результати реалізації або нереалізовані збитки (наприклад, суми втрачених через шахрайські операції платіжних карток з платіжними картками, кількість невдалих шахрайських банківських переказів)
- казуальні індикатори – показники, пов'язані з первинною причиною події реалізації ризиків ІБ (наприклад, частка часу недоступності інформаційної системи / ресурсу);
- показник ефективності контролю – поточний моніторинг виконання та операційної діяльності (наприклад, кількість коштів, використаних для укладання договорів з постачальниками послуг).

Це робиться на основі історичних даних (емпіричний підхід) та/або експертних оцінок персоналу банку. У відповідних бізнес-процесах ризики ІБ характеризуються визначенням граничного значення показника KIP.

Аналіз сценаріїв ризиків ІБ – це інструмент оцінки, який вивчає несподівані, але потенційно можливі події. Результати реалізації таких заходів можуть призвести до значних збитків або катастрофічно вплинути на здатність банку виконувати притаманні йому функції та навіть бути фатальними.

Сценарії ризику ІБ складаються на основі фокусування на можливому розвитку майбутніх подій, заснованих на передумовах, які не були зафіксовані в банку на поточний момент.

Сценарний аналіз ризиків ІБ банку може передбачати використання наступних сценаріїв:

Співробітники або треті сторони, які порушують фідуціарні зобов'язання перед клієнтами, вимоги конфіденційності, конфлікт інтересів; збої глобальної інфраструктури; збої ключових ІТ-систем; помилки в операціях або їх обробці, зломи внутрішньої інформаційної чи платіжної системи банку.

Аналіз сценаріїв дозволяє визначити перелік подій, які малоймовірно відбудуться, але можуть призвести до значних збитків, а згодом і до банкрутства.

Після визначення переліку подій кожен банк повинен провести стрес-тест і на його основі розрахувати, які збитки можуть виникнути внаслідок них, і розробити необхідні програми управління.

Висновки з оцінки ІБ-ризиків використовуються для прийняття управлінських рішень щодо розподілу ресурсів для мінімізації виявлених ризиків. Це приклад одного набору можливих наслідків, які виникнуть у результаті використання та забезпечення його безпеки.

Для зниження рівня ризику інформаційної безпеки (ІБ) банку та його складових, таких як ймовірність виникнення загроз, втрати через реалізацію цих загроз та втрати внаслідок вже виниклих інцидентів, банк повинен вживати відповідні заходи для їх мінімізації. Оскільки ефективна система оцінки ризиків ІБ відсутня, інструменти для їх зменшення є обмеженими.

Створення резервів під ризики є одним із методів, який найбільш поширений в менеджменті.

Страхування – метод, який поширився в Західній Європі та Північній Америці. Окрім спільного страхування майна та страхування відповідальності між банками, вони вважаються факторами, які зменшують ризик ІБ. Bankers Blanket Bond (BBB) є важливою інвестицією з точки зору захисту від злочинної діяльності та професійної відповідальності установ. Програма страхування може включати три види захисту, спрямовані на зниження операційного ризику банку.

BBB страхування надає основну статтю захисту від збитків, спричинених шахрайством персоналу. Поліс BBB також забезпечує страховий захист від збитків, які виникають внаслідок операцій, здійснених банком на основі підроблених письмових документів та інструкцій. Крім того, страхова компанія компенсує збитки, що виникають в результаті операцій з підробленими цінними паперами та фальшивою валютою. Покриття страхування також включає "класичні" злочини, такі як пограбування банку, крадіжки цінного майна з його приміщень та під час інкасації, а також збитки, спричинені пошкодженням або втратою цінного майна з будь-якої причини.

Наприклад, поліс страхування від електронних і комп'ютерних злочинів, придбаний на додаток до стандартного ВВВ, забезпечує захист від збитків у результаті несанкціонованого доступу до електронних систем банку. Ризик збитків спричинений шахрайськими інструкціями, отриманими через мережі зв'язку (наприклад, SWIFT); операції з бездокументарними цінними паперами; злом комп'ютерних систем клієнта, здійснений з його комп'ютерів (наприклад), недобросовісним персоналом).

У системі комплексного страхування банків, окрім кримінальних аспектів, присутнім є додатковий елемент, який суттєво підвищує загальний рівень захисту. Це поліс страхування професійної відповідальності (Professional Indemnity Policy), що покриває співробітників банку в разі недбалості або неумисних помилок, що виникають у процесі виконання професійних обов'язків перед клієнтами.

По суті, цей комплекс страхових продуктів забезпечує найбільш повний захист діяльності банку, а ще за взаємною згодою захищена не лише одна компанія, а всі банки автоматично включаються в систему страхування з подальшою сплатою премії. страхувальникам.

Управління ризиками ІБ стикається з найбільш складним етапом - створенням ефективної системи контролю. Це пов'язано з труднощами оцінки ефективності оцінки та управління ризиками, особливо після виникнення ризикової події, через їх багатовекторність та невизначеність.

Поліс страхування від електронних та комп'ютерних злочинів, що придбаний як доповнення до стандартного ВВВ, забезпечує захист від збитків у результаті несанкціонованого проникнення в електронні та комп'ютерні системи банку та зміни даних, що знаходяться в них; дії комп'ютерного вірусу; здійснення операцій за шахрайськими інструкціями, одержаними за електронними каналами зв'язку (наприклад, SWIFT); операціями з бездокументарними цінними паперами; зламу комп'ютерних систем клієнта, здійсненого з комп'ютерів банку (наприклад, неблагонадійними співробітниками); загибелі та пошкодження електронних даних та їх носіїв.

Третім елементом у системі комплексного страхування банків, не пов'язаним з криміналом, але таким, що значно збільшує загальний ступінь захисту, є поліс страхування професійної відповідальності (Professional Indemnity Policy) співробітників банку за недбалості й ненавмисні помилки, допущені в процесі виконання ними професійних обов'язків перед клієнтами.

Таким чином, цей комплекс страхових продуктів надає найповніший захист діяльності банку, причому комплексність полягає ще й у тому, що під покриття, за взаємною угодою, підпадає не тільки головна компанія, але і вся система філій банку, причому нові підрозділи автоматично включаються в застраховану систему з подальшою доплатою премії страхувальникам.

Найбільш складним етапом в управлінні ризиками ІБ є формування ефективної системи контролю, оскільки важко оцінити ефективність оцінки, а, тим більше, управління, завдяки їх багатовекторності та невизначеності навіть після настання ризикової події.

Доцільним є використання наступних елементів контролю та моніторингу управління ризиками ІБ:

1. Здійснення контролю за виконанням встановлених правил та процедур діяльності банку за допомогою використання принципу багатосторонньої відповідальності за здійснення операцій;

2. Використання програм-менеджерів та програм підтримки прийняття рішень при здійсненні операцій в інформаційній системі банку, що дозволить оптимальним чином розподілити обов'язки, права та відповідальність між користувачами інформаційної системи, розробити зручний інтерфейс для програм, що призначені для відстеження здійснення несанкціонованих операцій як з внутрішніх, так і зовнішніх терміналів;

3. Визначення критеріїв ефективності застосування різноманітних програм страхування за допомогою порівняння сум страхових тарифів із сумами отриманих страхових відшкодувань унаслідок настання страхових подій.

Чинним законодавством регулюються, здебільшого, превентивні інструменти мінімізації ризиків ІБ банку, а не подальшого контролю за дотриманням визначених

правил та процедур, тому банкам знадобиться міжнародний досвід, щоб сформувати цілісну систему управління ІБ в цілому, та ризиками ІБ.

1.6 Законодавча база банківської системи України

Закон України "Про захист прав споживачів фінансових послуг" є важливим інструментом, який був прийнятий Верховною Радою декілька років тому з метою захисту прав та інтересів споживачів банківських послуг в Україні. Цей закон був впроваджений для забезпечення безпеки та надійності фінансових транзакцій та зменшення ризиків, пов'язаних зі шахрайством у банківській сфері.

Одним з основних зобов'язань, встановлених цим законом, є повернення коштів клієнтам банку, якщо їх рахунки були піддані крадіжці шахраями. Це означає, що банки несуть відповідальність за збереження коштів своїх клієнтів та зобов'язані компенсувати збитки, якщо така ситуація сталася через шахрайські дії.

Застосування цього закону має важливе значення для захисту споживачів банківських послуг. Воно допомагає збільшити довіру до банківської системи в Україні, оскільки споживачі можуть бути впевнені, що вони несуть мінімальний ризик втрати грошей у разі крадіжки або шахрайства.

Для того, щоб дотримуватись вимог цього закону, банки повинні приділяти особливу увагу безпеці фінансових транзакцій та ефективно впроваджувати заходи для запобігання шахрайству. Це має включати вдосконалення систем безпеки, виявлення та блокування підозрілих транзакцій, а також надання інформаційних кампаній для підвищення свідомості клієнтів

Дивлячись на все це, у банків з'являється потреба в автоматизованній, багаторівневій перевірці кожного платежу, забезпечення надійного захисту кошт громадян та інші процедури захисту без втрат швидкостей виконання робіт, які полегшують взаємодії з банком, та гарантують збереження фінансів користувача.

Висновки до першого розділу

У першому розділі нашої дипломної роботи ми досліджували банківську систему України як об'єкт фінансової безпеки. Було з'ясовано, що банківська система відіграє важливу роль у забезпеченні стабільності фінансової системи країни. Виявлено основні характеристики та функції банківської системи, а також проаналізовано її роль у забезпеченні фінансової безпеки.

У другому розділі ми розглянули фінансову безпеку як частину кібербезпеки. Було встановлено, що в сучасному цифровому світі фінансові установи стикаються з різноманітними кіберзагрозами, які можуть негативно позначитися на їх фінансовій стійкості. Досліджено основні аспекти фінансової безпеки та визначено її взаємозв'язок з кібербезпекою.

У третьому розділі ми провели аналіз загроз, якими зіткнулася банківська система України. Було виявлено, що загрози можуть бути як зовнішніми, так і внутрішніми. Було проаналізовано такі типи загроз, як кібератаки, шахрайство, витік інформації та інші. Встановлено, що ці загрози можуть призвести до серйозних фінансових втрат та пошкодження репутації банківської системи.

У четвертому розділі ми досліджували сутність операційного ризику банку та класифікації, що використовуються в системі управління ним в сфері інформаційної безпеки. Було встановлено,що операційний ризик включає в себе ризик втрати через недосконаліть процесів, людські помилки, технічні несправності та інші фактори. Було проаналізовано основні класифікації операційного ризику та визначено їх значення для системи управління операційними банківськими ризиками.

У п'ятому розділі ми розглянули систему управління операційними банківськими ризиками в сфері інформаційної безпеки. Було встановлено, що ефективна система управління ризиками є ключовим елементом забезпечення фінансової безпеки банківської системи. Було розглянуто основні компоненти системи управління ризиками та проаналізовано методи та інструменти, які використовуються для оцінки та контролю операційних ризиків.

У шостому розділі була розглянута законодавча база банківської системи України. Було досліджено основні нормативно-правові акти, що регулюють діяльність банківської системи, включаючи закони, постанови та регуляторні акти. Визначено важливість належного дотримання законодавства для забезпечення фінансової безпеки банківської системи.

Загалом, результати нашого дослідження свідчать про важливість забезпечення фінансової безпеки банківської системи України в умовах зростаючих кіберзагроз. Отримані висновки та рекомендації можуть бути використані як основа для подальшого розвитку системи управління операційними ризиками в банківській сфері інформаційної безпеки та поліпшення законодавчої

РОЗДІЛ 2 ПІДХОДИ ДО ОЦІНКИ БЕЗПЕКИ БАНКІВСЬКОЇ СИСТЕМИ УКРАЇНИ

2.1 Дослідження нормативів банківської безпеки України

Норматив Н1 відображає рівень регулятивного капіталу, який є ключовим показником для оцінки діяльності банків. Він вказує на здатність фінансової установи пом'якшувати фінансові ризики, які можуть виникнути під час її діяльності .

Регулятивний капітал складається з основного капіталу, який включає статутний капітал і резерви, сформовані за рахунок нерозподіленого прибутку, та додаткового капіталу, який включає резерви переоцінки основних засобів і цінних паперів, що обліковуються на балансі банку, а також субординований борг.

Регулятивний капітал банку не повинен бути меншим за розмір статутного капіталу. Відповідно до закону, мінімальний розмір регулятивного капіталу має становити 120 мільйонів гривень. Згідно з вимогами НБУ, банки повинні підтримувати рівень капіталу на рівні не менше 120 млн. грн.

Норматив адекватності капіталу Н2 відображає здатність банку виконувати свої зобов'язання. Вище значення цього нормативу свідчить про те, що власники банку беруть на себе більші ризики, тоді як нижче значення - про те, що більша частка ризику перекладається на кредиторів та вкладників банку .

Це співвідношення запроваджено для того, щоб запобігти перекладанню банками ризиків на своїх кредиторів та вкладників .

Для діючих банків регулятивний поріг Н2 становить мінімум 10%, тоді як для нових банків він встановлюється на рівні 15% у перший рік після отримання ліцензії, 12% у другий рік і 10% у подальшому .

Норматив миттєвої ліквідності Н4 визначає мінімальний обсяг високоліквідних активів, необхідних для виконання поточних зобов'язань протягом одного робочого дня. Цей норматив слугує механізмом контролю за тим, щоб банк міг виконувати свої фінансові зобов'язання за рахунок високоліквідних активів .

Розрахунок цього показника передбачає порівняння високоліквідних активів з поточними зобов'язаннями банку .

Нормативне значення нормативу Н4 становить не менше 20% .

Норматив поточної ліквідності Н5 встановлює мінімальний обсяг активів банку, необхідний для покриття його поточних зобов'язань протягом календарного місяця .

Цей норматив використовується для оцінки збалансованості між строками та сумами ліквідних активів і пасивів банку .

Розрахунок нормативу Н5 передбачає ділення активів зі строком погашення до 31 дня на зобов'язання зі строком погашення до 31 дня .

Нормативне очікування для нормативу Н5 має становити щонайменше 40%.

Норматив короткострокової ліквідності Н6 відображає мінімально необхідний обсяг активів для погашення зобов'язань протягом одного року. Він слугує контрольним заходом для визначення того, чи може банк виконати короткострокові зобов'язання за рахунок ліквідних активів .

Норматив Н6 розраховується шляхом ділення ліквідних активів на зобов'язання зі строком погашення до одного року .

Нормативне значення нормативу Н6 має бути не менше 60% .

Норматив максимального розміру кредитного ризику на одного контрагента Н7 застосовується для обмеження кредитного ризику, пов'язаного з можливим дефолтом окремих контрагентів. Він розраховується шляхом ділення суми всіх вимог банку до окремого контрагента на регулятивний капітал банку .

Норматив Н7 не повинен перевищувати 25% .

Норматив великих кредитних ризиків Н8 встановлюється з метою обмеження концентрації кредитного ризику на одного контрагента або групу контрагентів .

Кредитний ризик вважається значним, якщо вимоги банку до контрагента або групи контрагентів становлять 10% і більше регулятивного капіталу банку .

Норматив Н8 розраховується шляхом ділення суми всіх великих кредитних ризиків за контрагентами на регулятивний капітал банку. Регулятивний поріг для Н8 не повинен перевищувати 8-кратного розміру регулятивного капіталу банку .

Норматив Н9, що являє собою максимальний розмір кредитного ризику за операціями з пов'язаними з банком особами, встановлюється для управління ризиком, що виникає за операціями з інсайдерами. Він розраховується шляхом ділення зобов'язань інсайдера перед банком на статутний капітал фінансової установи .

Нормативне значення Н9 не повинно перевищувати 25% .

Норматив Н11, відомий як норматив інвестування в цінні папери для кожної установи, встановлюється з метою нагляду за інвестиційною діяльністю банків, у тому числі за прямими інвестиціями .

Норматив Н11 розраховується шляхом ділення суми коштів, інвестованих у придбання акцій, паїв, часток, паїв та інвестиційних сертифікатів окремої юридичної особи, на статутний капітал банку .

Стандартне очікування для показника Н11 не повинно перевищувати 15%.

2.2 Дослідження кібершахрайств в банківській системі України

Широке розповсюдження банківських карток та інтеграція комп'ютерних технологій у платіжні системи стали визначальними аспектами нашого повсякденного життя. Безготівкові способи оплати переживають стрімке зростання і пропонують численні переваги. Безготівкові операції сприяють підвищенню швидкості транзакцій, зменшенню залежності від фізичного обігу готівки, що призводить до зниження операційних витрат, а також підвищенню прозорості платіжних процесів. Однак популярність і зручність операцій з банківськими картками також роблять їх привабливою мішенню для шахрайських дій.

За період з 01.01.2017 по 26.08.2017 платіжними сервісами системи "Біржа-онлайн" було виявлено та зафіксовано 12 416 підозрілих операцій на загальну суму 3 409 000 гривень. У цих операціях було використано 7390 банківських карток, емітованих 135 банками з 53 країн світу, в тому числі 67 українськими банками. Шахраї намагалися зняти кошти за допомогою мобільних пристроїв.

На рисунку 2.1 показано країни, картки яких були використані в шахрайських операціях, ідентифікованих системою, а також відсоток операцій, які були підтверджені як шахрайські.

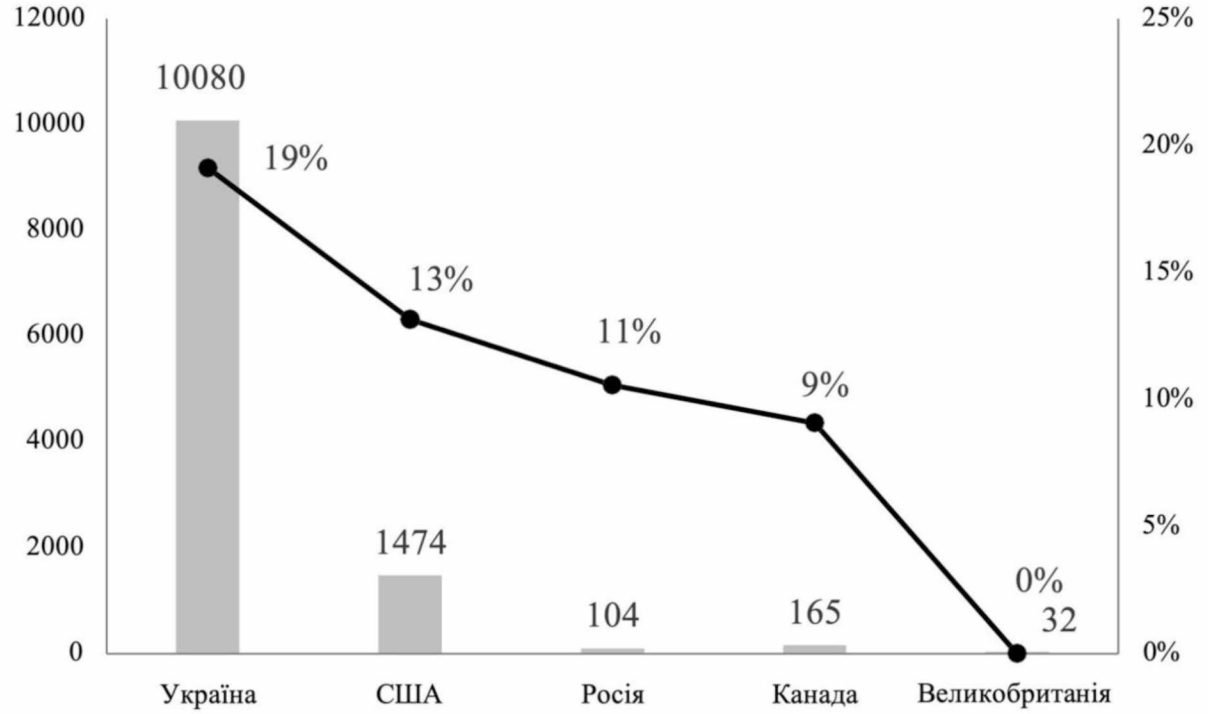

Рисунок 2.1 – Аналіз шахрайських операцій, здійснених у 2017 році (графік побудовано на основі статистичних даних Української міжбанківської Асоціації членів платіжних систем)

Дані, представлені на рисунку 2.1, свідчать про те, що Україна є провідною країною з недостатніми заходами безпеки при здійсненні банківських платіжних операцій. Дивно, але 19% цих транзакцій були визнані шахрайськими, що перевищує показники, які спостерігаються в інших країнах. В результаті кібершахрайства з карток українських громадян було незаконно знято 238 955 гривень. Ця тривожна ситуація становить значний ризик для банківських платіжних систем, оскільки вони можуть втратити клієнтів через вразливість своїх заходів безпеки. Отже, вирішення цього питання потребує комплексного підходу із залученням різних зацікавлених сторін, таких як уряд, населення, банки та інвестори, оскільки це не лише проблема фінансових установ, а й ширша соціальна проблема.

На сьогоднішній день шахрайські операції з банківськими картками можуть проявлятися в декількох поширених формах:

- Скімінг: викрадення інформації з картки, включаючи дані магнітної смуги або ПІН-код, за допомогою спеціальних пристроїв.

- Пастки: розміщення пасток на кришках банкоматів з метою унеможливлення вилучення карток.

- Фізичне пошкодження банкоматів.

- Фішинг: шахрайські дії, що здійснюються через Інтернет з метою обманом змусити користувачів розкрити конфіденційну інформацію.

- Вішинг: шахрайство, що здійснюється через канали мобільного зв'язку.

- Вірусні та хакерські атаки, серед інших методів.

На рисунку 2.2 показано різні категорії шахрайських операцій, що відбулися протягом першого півріччя 2017 року, класифіковані відповідно до застосованого методу та представлені у відсотках.

Рисунок 2.2 – Групи шахрайських операцій, об’єднаних за однаковим способом здійснення (графік побудовано на основі статистичних даних Української міжбанківської Асоціації членів платіжних систем)

Більшість шахрайських операцій, здійснених за допомогою методів соціальної інженерії (41%), пов'язані з вішингом та фішингом, коли шахраї обманом отримують дані платіжних карток клієнтів, отримують доступ до їхніх рахунків та знімають кошти. Як правило, жертвами схем соціальної інженерії стають люди старшого віку від 55 років (15%) та люди середнього віку від 35 до 44 років (13%).

Найпоширенішими способами викрадення грошей шахраями є банкомати (32%) та Інтернет (16%) (див. рис. 2.2). Це підкреслює необхідність розробки додаткових заходів для захисту банківських систем кібербезпеки від цих видів шахрайства.

Шахрайство із застосуванням соціальної інженерії є глобальною проблемою. Станом на кінець першого кварталу 2017 року фішингові атаки завдали найбільшої шкоди 51,70% банків у всьому світі. До країн з найбільшим відсотком атак на користувачів належать Китай (20,87%), Бразилія (19,16%), Макао (11,94%), Російська Федерація (11,29%), Австралія (10,73%), Аргентина (10,42%), Нова Зеландія (10,18%), Катар (9,87%), Казахстан (9,61%) та Тайвань (9,27%). Щодо частки користувачів, на яких спрямовані вішинг-атаки, то найбільш постраждалими країнами є Росія (1,2%), Узбекистан (0,40%), Казахстан (0,36%), Таджикистан (0,35%), Туреччина (0,34%), Молдова (0,31%), Україна (0,29%), Киргизстан (0,27%), Білорусь (0,26%) та Латвія (0,23%).

В Україні у 2017 році клієнти банків зазнали збитків у розмірі 509,72 млн грн через тактику соціальної інженерії, що майже вдвічі більше, ніж у 2016 році, і в дев'ять разів більше, ніж у 2015 році. Середня сума шахрайської транзакції, здійсненої за допомогою методів соціальної інженерії, також зросла до 2 543 грн у 2017 році, що в 1,8 раза більше, ніж у 2016 році (див. Таблицю 2.1).

Таблиця 2.1

Збитки від шахрайських операцій, здійснених з використанням соціальної інженерії та інтернету

Вид збитку	2015		2016		2017	
	Соціальна інженерія	Інтернет	Соціальна інженерія	Інтернет	Соціальна інженерія	Інтернет
Середня сума збитку від однієї шахрайської операції, грн.	834	206	1403	345	2543	145
Загальні збитки від шахрайських операцій, млн. грн.	51,74	32,62	275,45	63,68	509,72	159,91

Таблицю побудовано на основі даних Української міжбанківської Асоціації членів платіжних систем

В Україні наблюдається значна кількість випадків платіжного шахрайства, особливо з використанням методів соціальної інженерії в середовищі Card-Not-Present, де операції здійснюються без наявності фізичної картки та присутності користувача. У порівнянні з обслуговуванням через банкомати, POS-термінали та дистанційне банківське обслуговування, цей вид шахрайства виявляється найпоширенішим (див. рис. 2.3).

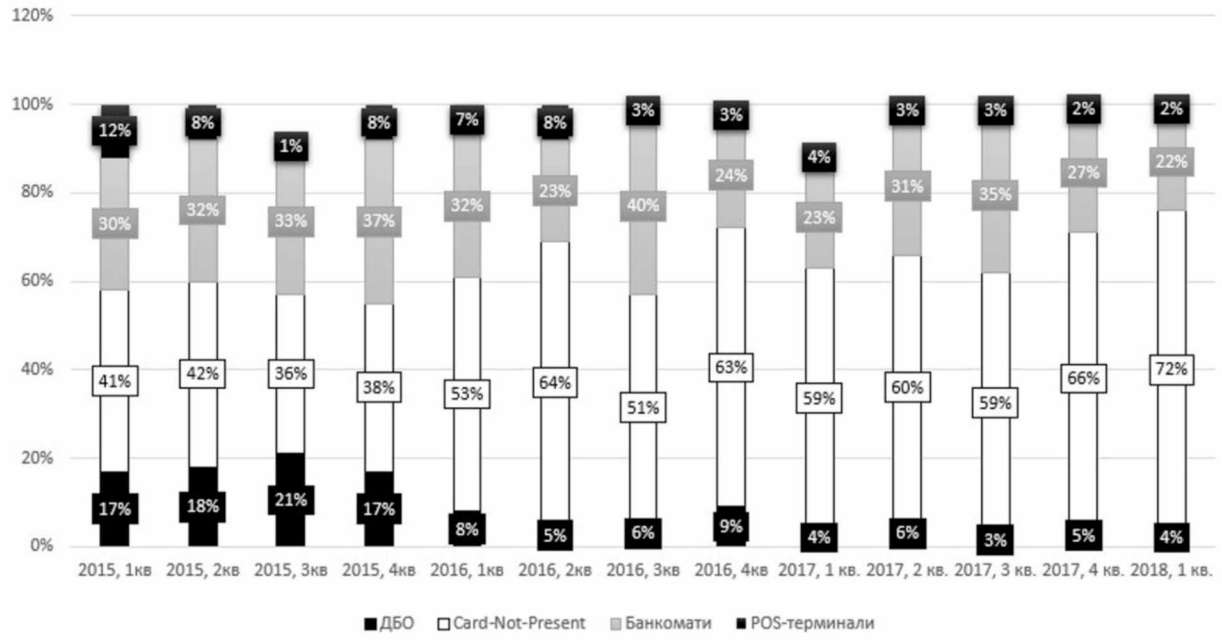

Рисунок 2.3 – Шахрайські операції за різними видами банківського обслуговування (графік побудовано на основі статистичних даних Української міжбанківської Асоціації членів платіжних систем)

Методи соціальної інженерії набули значної популярності серед шахраїв, дозволяючи їм отримувати не лише інформацію про платіжні картки, але й ідентифікаційні дані клієнтів. Використовувати цей метод шахрайства відносно просто, незважаючи на зусилля банків застерегти клієнтів від розголошення платіжних реквізитів по телефону. Шахраї використовують різні психологічні тактики для маніпулювання жертвами.

Вивчення наслідків кібершахрайства у сфері платіжних інструментів показує, що клієнт є найбільш вразливою мішенню, схильною до маніпуляцій за допомогою методів соціальної інженерії. Українським банкам бракує ефективних інструментів для адекватної боротьби з цим видом шахрайства. На нашу думку, боротьба з цією формою шахрайства потребує комплексного підходу з використанням інструментів інтелектуального аналізу та інформаційних технологій.

Для протидії кібершахрайству, зокрема соціальній інженерії, автори пропонують наступні заходи:

1) Розробка алгоритмів з використанням методів інтелектуального аналізу даних для моніторингу та виявлення шахрайських транзакцій за певними ознаками. Ця тема детально розглянута в роботі. Особливо ефективним є використання нейронних мереж, які дозволяють системі постійно адаптуватися до нових індикаторів шахрайства. Наприклад, якщо шахрай намагається зняти весь залишок на рахунку, система ретельно перевіряє транзакцію і в разі виявлення шахрайства блокує її.

2) Створення автоматизованого модуля моніторингу, інтегрованого в банківські та платіжні системи для автоматичної перевірки транзакцій на предмет шахрайства, блокування підозрілих операцій та забезпечення подвійної (або потрійної) ідентифікації клієнтів. Хоча існуючі платіжні системи частково реалізують ці функції, вони часто не здатні протидіяти випадкам соціальної інженерії. Коли система виявляє потенційно шахрайську транзакцію, вона повинна повідомити клієнта про тип, місце та суму транзакції. Наприклад, якщо несанкціонована транзакція ініційована з іншої країни, клієнт повинен отримати повідомлення, щоб підтвердити або заблокувати транзакцію, надавши банку певний код.

3) Створення централізованої бази даних, яка міститиме інформацію про різні методи шахрайства, характеристики шахраїв та жертв, номери мобільних телефонів, IP-адреси тощо. Така база даних допоможе сформулювати нові правила перевірки та контролю банківських операцій на основі індикаторів шахрайства. Важливо, щоб ці бази даних охоплювали всю банківську систему, а не обмежувалися окремими банками для забезпечення стандартизованого обміну інформацією.

4) Суворе обмеження прав доступу банківських працівників до клієнтських баз даних для зменшення внутрішнього шахрайства. Цього можна досягти за допомогою чіткого контролю доступу, налаштованого на програмному рівні. Такий підхід потребує розробки та модифікації посадових інструкцій для банківських працівників, а також інструкцій та рекомендацій від найбільших банків та Національного банку України.

5) Розширення соціальних ініціатив через ЗМІ та Інтернет з метою підвищення обізнаності та зменшення кількості випадків шахрайства із застосуванням соціальної

інженерії. Це сприятиме створенню ефективної системи комунікації та співпраці між банками та клієнтами.

Отже, кібершахрайство, пов'язане з банківськими картками та різними платіжними операціями, має негативні наслідки для стабільності фінансової системи. Це включає в себе перешкоджання впровадженню безготівкових платежів та підрив довіри населення до банків для зберігання коштів та отримання кредитів. Недостатнє розуміння механізмів кіберзлочинності ускладнює процес виявлення шахрайства. Дослідження індикаторів шахрайства є життєво важливим для розробки більш надійних засобів і методів захисту від таких злочинів. Аналіз наслідків кібершахрайства допомагає виявити вразливі місця в банківській системі та накопичити знання про методи шахрайства, профілі шахраїв, характеристики жертв та індикатори шахрайства.

Аналіз, представлений у цій статті, підкреслює зростання збитків, яких зазнають банки від кібершахрайства, незважаючи на впроваджені заходи безпеки. Як клієнти, так і банки зазнають фінансових втрат через різні шахрайські схеми, причому найбільшої шкоди завдають методи соціальної інженерії. Для ефективної боротьби з цим видом шахрайства необхідно впроваджувати запропоновані заходи, використовуючи методи інтелектуального аналізу даних та передові інформаційні технології.

2.3 Оцінка впливу макроекономічних факторів на формування схильності до шахрайства в банківській сфері

Шахрайські дії виникають у складній взаємодії економічних, політичних та соціальних елементів. Макроекономічний стан країни відіграє вирішальну роль у створенні умов, що сприяють шахрайству. Ці фактори в сукупності впливають на систему та формують її поведінку. Тому було проведено оцінку впливу макроекономічних чинників на вразливість до шахрайства. Визначивши ситуації, в яких можна впливати на шахрайство, ми можемо сформулювати основні гіпотези:

- Суспільства з нижчим рівнем мінімальної заробітної плати більш схильні до шахрайських операцій порівняно з суспільствами з вищим рівнем заробітної плати.
- Країни зі значною часткою населення, що заробляє нижче порогу валового доходу, демонструють підвищену схильність до шахрайства.
- Широко розповсюджена корупція в країні перешкоджає ефективному державному управлінню і гіпотетично сприяє підвищенню ймовірності шахрайських дій.
- У країнах, де держава не контролює територіальну цілісність і намагається впливати на демографічний, соціальний і політичний ландшафт, шахрайство є більш вірогідним.
- У суспільствах, де відсутні економічні свободи, такі як право обирати роботу, виробляти товари, здійснювати різні витрати та інвестиції, рівень шахрайства вищий, ніж у тих, де є економічні свободи.
- Країни з низьким рівнем економічного розвитку та купівельної спроможності населення є більш вразливими до шахрайських операцій.
- Створення сприятливих умов для добробуту громадян може потенційно знизити ймовірність шахрайства.
- У країнах з високим рівнем безпеки життя шахрайство трапляється рідше.
- Вища схильність до шахрайства очікується в країнах, де рівень цін на невиробничі споживчі товари та послуги зростає, а купівельна спроможність населення залишається низькою.
- Рівень шахрайства в країні може змінюватися залежно від темпів зростання населення та співвідношення статей у суспільстві.
- Створення умов для національного процвітання знижує ймовірність шахрайських операцій.

Побудова моделі передбачає включення конкретних макроекономічних показників певної країни, які відображають схильність населення до шахрайства. Такими показниками можуть бути індекс бідності, індекс споживчих цін, рівень злочинності, ВВП на душу населення, гендерний розподіл та інші. Ці фактори були обрані з огляду на їхній вплив на формування схильності до шахрайства внаслідок

різних макроекономічних подій у країні. Зміни в економічному, соціальному та політичному ландшафті країни сприяють виникненню шахрайських операцій. Зрештою, шахрайство виникає в результаті складної взаємодії економічних, політичних і соціальних факторів, які в сукупності формують поведінку системи.

Підсумовуючи усе вищесказане можемо побудувати схему впливу факторів на схильність до шахрайства Рис2.4

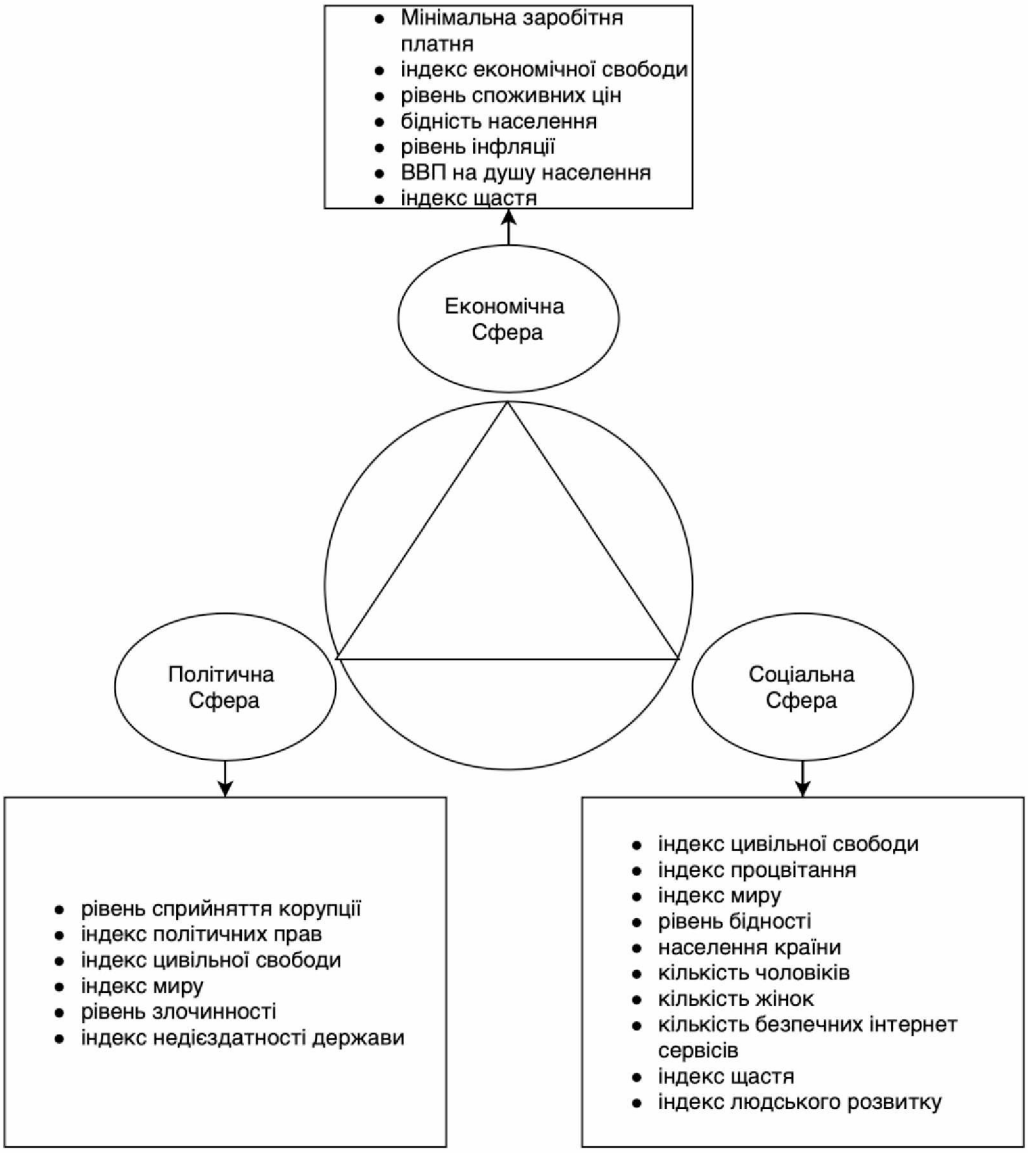

Рисунок 2.4 – Трикутник

2.4 Оцінювання збитків банків від їх залучення до шахрайських операцій

За даними Національного банку України, у 2017 році вітчизняні банки зазнали збитків на суму 24,4 млрд грн. Більшість цих збитків були спричинені насамперед збільшенням відрахувань до обов'язкових банківських резервів, вимоги до яких значно зросли протягом останніх трьох років. Однак частина цих збитків у банківському секторі є наслідком участі банків у шахрайських операціях. Цікаво, що менеджмент банків в першу чергу зосереджується на фінансовому моніторингу власних операцій, як того вимагає державний регулятор. Ймовірний розмір збитків від участі фінансової установи у шахрайських операціях сприймається керівництвом банків зі скепсисом. Тим не менш, ми вважаємо, що кількісна оцінка цих втрат є важливим елементом внутрішньобанківської системи протидії незаконним операціям. Це дасть змогу виявити сфери, де відбуваються втрати, та визначити відповідальних за їх нейтралізацію.

Метою роботи є розробка науково-методичного підходу до визначення релевантних факторів ризику, формування матриць вартості негативних наслідків їх настання та побудови дерева рішень, що окреслює потенційні альтернативи зниження банківських ризиків. Цей підхід має на меті оцінити ймовірні збитки, яких можуть зазнати банки від участі в шахрайських операціях.

Розглянемо поетапну реалізацію науково-методичного підходу до визначення ймовірних втрат банку від шахрайських операцій:

Етап 1: Формування простору ознак, що охоплює ключові індикатори втрат банку від шахрайських операцій. На цьому етапі враховуються як зовнішні, так і внутрішні зміни в банківському середовищі. Він передбачає визначення релевантних факторів ризику, пов'язаних з шахрайськими операціями в банківській діяльності, а також переваг, які отримують банки при уникненні або усуненні наслідків цих ризиків.

Етап 2: Вибір або розробка математичних моделей для кількісної оцінки кожного виявленого релевантного фактору ризику шахрайства. Важливо враховувати, що фактори ризику можуть мати як якісні, так і кількісні значення.

Етап 3: Оцінка порівнянності між факторами банківських ризиків та вигодами, які банки отримують від уникнення або подолання наслідків ризиків шахрайства. Цей

етап передбачає формалізацію виявленої відповідності в табличній формі. Крім того, необхідно провести аналіз чутливості відповідних факторів ризику шахрайства, притаманних банкам, з урахуванням підсумків бінарних показників з таблиць порівнянності факторів ризику та відповідних переваг.

Етап 4: Використання витратного підходу для відповідних факторів ризику шахрайських операцій, які не дають можливості отримати відповідні вигоди. Це передбачає побудову матриць витрат та визначення ймовірності їх отримання в конкретних ситуаціях.

Етап 5: Побудова дерева рішень, що охоплює потенційні альтернативи зниження ризиків, пов'язаних із шахрайськими банківськими операціями.

Детально розглянувши послідовність визначення ймовірних втрат банку від шахрайських операцій, слід приділити подальшу увагу формалізації вищезазначених етапів та визначенню математичного апарату, що забезпечує їх реалізацію.

Тому в рамках вивчення відповідних факторів ризику, пов'язаних з шахрайськими операціями, необхідно розрізняти наступні категорії аналізу:

1) Шахрайство з банкоматами: Це включає зняття готівки з використанням підроблених пластикових карток ("білий" пластик) (Z1), використання скімінгових інструментів для копіювання даних платіжних карток (включаючи дані з магнітної смуги) та запису ПІН-коду (Z2), зняття коштів у банкоматах без відображення операції на рахунку (шахрайство з відміною транзакції) (Z3), зняття готівки власниками карток без фізичного отримання грошей (Cash Trapping) (Z4) та фізичні напади на банкомати (Z5).

2) Шахрайство в термінальній мережі: Сюди відносяться операції з використанням підроблених/викрадених/втрачених платіжних карток (S1), зняття готівки через касу банку за підробленими документами та платіжними картками (S2), дублювання операцій касирами/операторами (S3), несанкціоновані або неточні списання (розбіжності між сумою чека та сумою, закладеною в розрахунок) (S4), компрометація даних платіжних карток касирами під час розрахунків у торгово-сервісних мережах для подальшого несанкціонованого використання (S5), використання накладок (скімерів) на термінальне обладнання для перехоплення та

передачі даних платіжних карток під час проведення операцій (через незаконні домовленості з касирами) (S6), встановлення шкідливого програмного забезпечення, яке пошкоджує програмне забезпечення терміналів (S7).

3) Інтернет-шахрайство: Передбачає використання шкідливих програм (вірусів) та підроблених веб-сайтів для компрометації реквізитів електронних платіжних інструментів та/або логінів/паролів до систем інтернет-/мобільного банкінгу (RC1), а також поширення (продаж, розповсюдження) скомпрометованої інформації (RC2).

4) Шахрайство в системах дистанційного обслуговування (ДБО): Несанкціоноване втручання та/або встановлення шкідливих програм (вірусів), які пошкоджують програмне забезпечення персональних комп'ютерів, перехоплюють паролі до облікових записів, отримують інформацію з секретних ключів/токенів тощо (РК1).

5) Соціальна інженерія: Це означає, що шахраї входять у довіру до власників рахунків/карток, отримують їхні персональні дані та реквізити платіжних карток або переконують власників рахунків переказати кошти шахраям (RP1).

Ефективно уникаючи або зменшуючи ризики, пов'язані з банкоматним шахрайством, шахрайством у термінальних мережах, інтернет-шахрайством, шахрайством у системах дистанційного обслуговування та соціальною інженерією, банки можуть отримати низку переваг, серед яких збільшення фінансових потоків, розширення клієнтської бази, підвищення попиту на банківські послуги, збереження банківської ліцензії, стабільна робота фінансової установи та посилення співпраці з міжнародними партнерами.

Вивчення та ідентифікація відповідних факторів ризику шахрайства, притаманних банківській діяльності, а також переваг, отриманих від їх уникнення та подолання, формують підґрунтя для наступного етапу реалізації методологічного підходу до визначення ймовірних збитків, яких можуть зазнати банки від їх залучення до шахрайських операцій. Відповідно, це призводить до побудови таблиці відповідності (див. табл. 2.2).

Таблиця 2.2

Таблиця відповідності ймовірних сбитків

Релевантні фактори ризиків шахрайських операцій, притаманних банківській діяльності	Переваги, які отримує банк у випадку уникнення або подолання наслідків впливу ризиків шахрайських операцій					
	Нарощування обсягів фінансових потоків (P1)	Розширення клієнтської бази банку (P2)	Інтенсифікація попиту на банківські послуги (P3)	Збереження ліцензії на здійснення банківських послуг (P4)	Стабільне функціонування фінансової установи (P5)	Співпраця з міжнародними партнерами (P6)
Шахрайство з використанням банкомату						
Z1	$z11$	$z12$	$z13$	$z14$	$z15$	$z16$
Z2	$z21$	$z22$	$z23$	$z24$	$z25$	$z26$
Z3	$z31$	$z32$	$z33$	$z34$	$z35$	$z36$
Z4	$z41$	$z42$	$z43$	$z44$	$z45$	$z46$
Z5	$z51$	$z52$	$z53$	$z54$	$z55$	$z56$
Шахрайство в термінальній мережі						
S1	$s11$	$s12$	$s13$	$s14$	$s15$	$s11$
S2	$s21$	$s22$	$s23$	$s24$	$s25$	$s21$
…	…	…	…	…	…	…
S7	$s111$	$s112$	$s113$	$s114$	$s115$	$s111$
Інтернет шахрайство						
RC1	$c11$	$c12$	$c13$	$c14$	$c15$	$c16$
RC2	$c21$	$c22$	$c23$	$c24$	$c25$	$c26$
Шахрайство в системах дистанційного обслуговування						
RK1	$k11$	$k12$	$k13$	$k14$	$k15$	$k16$
Соціальна інженерія						

RP1	$p11$	$p12$	$p13$	$p14$	$p15$	$p16$

Висновки до другого розділу

Інформаційні моделі: Інформаційні моделі для виявлення ознак шахрайства з боку зовнішніх та внутрішніх шахраїв були розроблені з використанням системного підходу та стандарту BPMN 2.0. Ці моделі слугуватимуть основою для автоматизованого модуля банківського моніторингу, забезпечуючи інтеграцію в автоматизовану банківську систему.

Математичні портрети: Математичні портрети потенційних жертв та шахраїв були розроблені для визначення ситуацій, в яких найімовірніше виникають індикатори кібершахрайства. Врахування таких факторів, як вік, стать, соціальний статус, способи здійснення транзакцій, історія клієнта та місце проведення транзакції, дозволяє підрозділам кіберзахисту банків швидко реагувати та завчасно запобігати шахрайським діям.

Вартісний підхід та дерево рішень: Було розроблено науково-методичний підхід для визначення потенційних збитків, яких можуть зазнати банки від шахрайських операцій. Цей підхід використовує вартісну оцінку та будує дерева рішень з можливих альтернатив, зменшуючи ризики, пов'язані з шахрайськими операціями.

Вплив макроекономічних факторів: Модель досліджує вплив макроекономічних факторів на вразливість до шахрайства в банківському секторі. Розглядаються економічні показники (мінімальна заробітна плата, індекс економічної свободи, ВВП на душу населення), політичні фактори (рівень сприйняття корупції, індекс громадянських свобод, рівень злочинності) та рівень корупції в банківському секторі. Аналіз формує трикутник, який визначає схильність до шахрайства з банківськими продуктами, що дозволяє розробити превентивні заходи контролю на макрорівні в рамках системи кібербезпеки.

Гравітаційна модель оцінки привабливості: Для оцінки привабливості країни для легалізації злочинних доходів через банківський сектор була розроблена гравітаційна модель. Ця модель допомагає зменшити ризики, пов'язані з вразливістю держави до відмивання коштів та фінансування тероризму.

РОЗДІЛ 3 РЕКОМЕНДАЦІЇ ДО РОЗРОБКИ КОМПЛЕКСУ АВТОМАТИЗОВАНИХ ЗАХОДІВ ПОПЕРЕДЖЕННЯ ШАХРАЙСТВ

3.1 Розробка інформаційної моделі виявлення ознак шахрайств у банках

Уявімо собі банк як складну структуру, що складається з внутрішніх компонентів: персонал, керівництво банку, власники, автоматизована банківська система (АБС); та зовнішніх компонентів: клієнти, кіберзлочинці, афілійовані особи, програмне забезпечення та технічні пристрої. По суті, банк являє собою мережу взаємопов'язаних об'єктів як у внутрішньому, так і в зовнішньому середовищі. Системи будь-якого типу включають елементи з різним рівнем надійності, які за певних обставин можуть бути вразливими до вторгнення, що потенційно може призвести до негативних наслідків. По суті, кожен з цих елементів може слугувати потенційним джерелом шахрайської діяльності - як підбурювач, співучасник або опосередковано залучена сторона.

Існуючі дослідження банківського шахрайства переважно пов'язують ініціацію шахрайства із зовнішнім середовищем, що не зовсім вірно. Насправді, 80% всіх випадків шахрайства пов'язані з персоналом банку. Отже, можливості вторгнення повинні також враховувати внутрішні аспекти загрози.

Тому, визначаючи банківську систему, ми застосовуємо принцип професійного скептицизму, який використовують аудитори, що не виключає можливості зловживань на будь-якому робочому місці в банку або ймовірності проникнення сторонніх осіб з метою вчинення шахрайства або завдання шкоди. Іншими словами, шахрайство може бути здійснене будь-ким, будь-де, з використанням будь-яких інструментів та методів. Отже, система повинна враховувати негативні зміни та реагувати на них. З огляду на це, ми представляємо архітектуру АБС, розглядаючи модуль моніторингу як центральний компонент, який об'єднує інформаційні потоки, що генеруються суб'єктами як у зовнішньому, так і у внутрішньому середовищі (рис. 3.1).

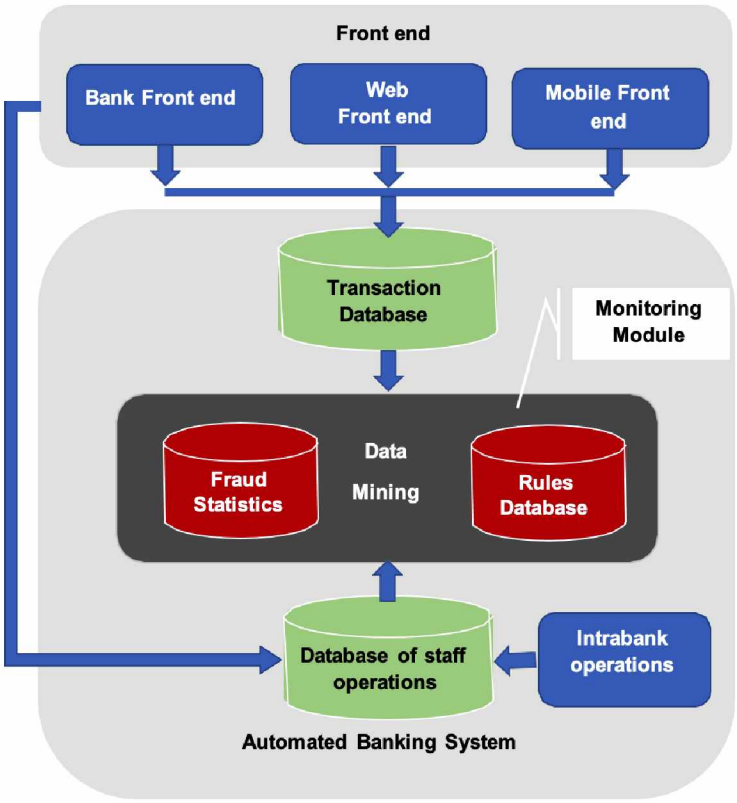

Рисунок 3.1 – Архітектура автоматизованої банківської системи з урахуванням модулю моніторингу

Основною метою системи є передбачення, виявлення та запобігання шахрайству. Для цього доцільно включити модуль моніторингу, який називається "Модуль моніторингу", що працює на принципах інтелектуального аналізу даних і створює базу даних статистики шахрайства, відому як "Статистика шахрайства", а також базу даних правил ("База даних правил") для відстеження індикаторів шахрайської діяльності (як показано на рис. 3.1). Основною функцією цього модуля є виявлення потенційних випадків шахрайства, незалежно від того, чи походять вони ззовні, наприклад, від клієнтів банку та їхніх транзакцій, що зберігаються в "Базі даних транзакцій", чи зсередини, за участю персоналу банку та їхніх транзакцій, що зберігаються в "Базі даних операцій персоналу". Кожна транзакція оцінюється за певними критеріями, викладеними в базі правил, отриманих на основі накопичених статичних даних про шахрайство.

Відповідно до запропонованої архітектури АБС, ми розробимо інформаційну модель для виявлення ознак шахрайства в операціях, ініційованих зовнішнім середовищем. Ця модель охоплюватиме інформаційні потоки, що функціонують у середовищі АБС, зокрема в модулі моніторингу (як показано на рис. 3.2).

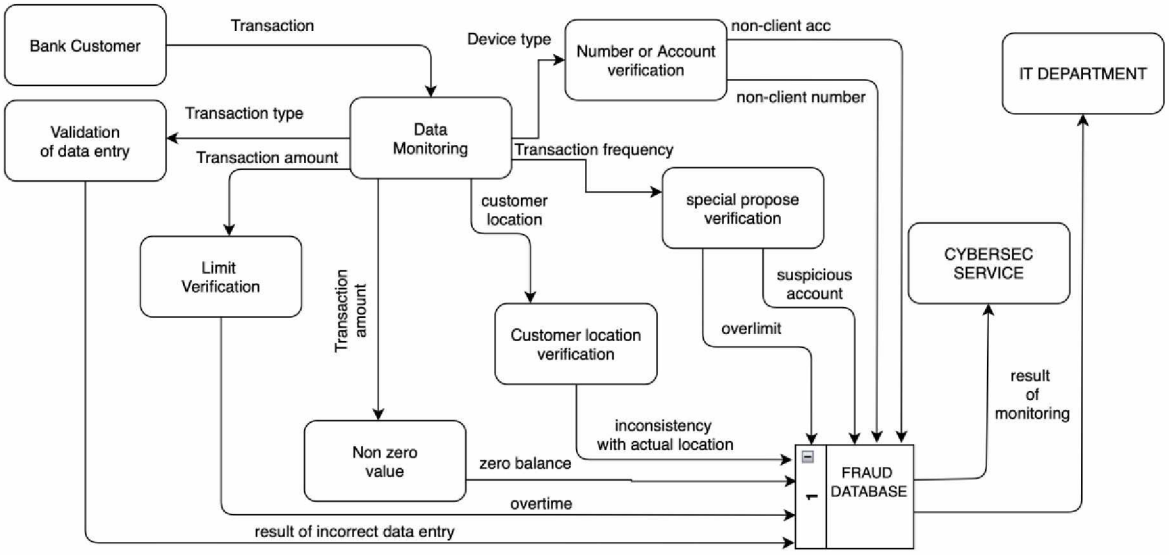

Рисунок 3.2 – Інформаційна модель виявлення ознак шахрайств клієнтів

Для побудови моделі за допомогою програмного забезпечення All Fusion Process Modeller було використано нотацію DFD (Data Flow Diagrams), яка слугує інструментом для структурного моделювання та проектування інформаційних систем. DFD модель ефективно описує потоки даних.

Модель, представлена на Рисунку 3.2, відображає інформаційні потоки, що використовуються в модулі моніторингу для виявлення та запобігання шахрайству. Це досягається за допомогою функцій "Моніторингу даних", які аналізують банківські операції ("Операція"), що здійснюються клієнтами (далі - "Клієнт банку"). Виконуються наступні перевірки:

- "Перевірка ненульового значення" гарантує, що сума транзакції не призведе до нульового балансу на рахунку. Шахрайські операції часто передбачають повне спустошення рахунку, що є вкрай нетиповим для законних власників рахунків. Отже, якщо виявляється нульовий баланс, це викликає тривогу.

- "Перевірка лімітів" перевіряє, чи не перевищує сума транзакції встановлені ліміти ("Перевищення ліміту"). Під час шахрайських дій транзакції можуть перевищувати ліміти, встановлені банком або клієнтом, що свідчить про спробу незаконної транзакції.

- "Перевірка місцезнаходження клієнта" підтверджує походження транзакції, оскільки вона може походити з будь-якої країни або міста і не відповідати фактичному географічному розташуванню клієнта.

- "Верифікація рахунку спеціального призначення" підтверджує відповідний рахунок, який може бути позначений у "чорному списку" підозрілих рахунків або мати суму транзакції, що перевищує ліміт ("Перевищення ліміту"), якщо цільовий рахунок відкрито в іншому банку.

- "Перевірка номера або рахунку" здійснює перехресну перевірку номерів і рахунків клієнтів залежно від типу пристрою ("Тип пристрою"), з якого ініціюється транзакція. Якщо транзакцію намагаються здійснити з номера та рахунку, які не належать клієнту ("Неклієнтський рахунок" та "Неклієнтський номер"), з'являється сповіщення.

- "Перевірка введення даних" перевіряє правильність введення даних залежно від типу транзакції ("Тип транзакції"). Неправильні спроби ("Результат неправильного введення даних") можуть свідчити про потенційну компрометацію облікового запису клієнта.

Інформація про можливі порушення, шахрайство або злом передається до Бази даних шахрайства для подальшої обробки. Результат моніторингу ("Результат моніторингу") передається як до ІТ-відділу, так і до служби кібербезпеки банку ("Служба кібербезпеки").

Відповідно до запропонованої інформаційної моделі (рис. 3.2) було розроблено діаграму процесу транзакції клієнта, яка включає заходи з виявлення шахрайства з використанням BPMN 2.0 (Business Process Model and Notation) в програмному забезпеченні Bizagi Modeller (рис. 3.3).

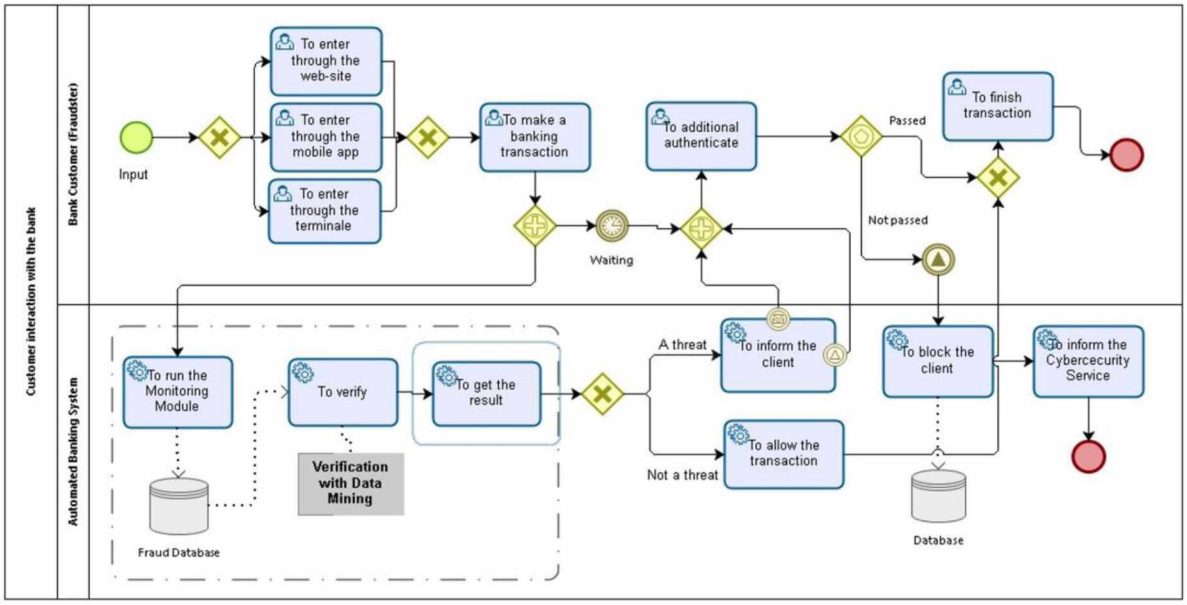

Рисунок 3.3 – Схема процесу здійснення операції клієнтом банку [22]

На Рисунку 3.3 зображено наступну послідовність дій:

1) Користувач, незалежно від того, чи є він справжнім клієнтом банку, чи потенційним шахраєм ("Клієнт банку (шахрай)"), отримує доступ до системи за допомогою різних засобів, таких як веб-сайт, мобільний пристрій або термінал.

2) Користувач, діючи як клієнт банку або потенційний шахрай, ініціює проведення банківської операції ("Здійснити банківську операцію").

3) Автоматизована банківська система використовує модуль моніторингу, оснащений інтелектуальними методами аналізу, для ретельної перевірки транзакції на наявність ознак шахрайської діяльності ("Перевірка за допомогою інтелектуального аналізу даних"). Процес перевірки ґрунтується на заздалегідь визначених критеріях, що зберігаються в базі даних ("База даних шахрайства"),

4) Якщо під час верифікації не виявлено ознак потенційного шахрайства, система переходить до авторизації транзакції ("Дозволити транзакцію"), що дозволяє клієнту успішно завершити транзакцію ("Завершити транзакцію").

5) У разі виявлення ознак шахрайства в процесі верифікації, система пропонує користувачеві додатково підтвердити транзакцію за допомогою SMS, дзвінка або іншим способом ("To inform the client").

6) Після цього клієнту необхідно пройти додаткові заходи автентифікації ("Додатково автентифікуватися").

7) Якщо операція підтверджена як законна і ініційована справжнім клієнтом, вона буде успішно виконана.

8) Якщо ж клієнт виявився шахраєм, не пройшовши додаткову автентифікацію, його доступ блокується ("Заблокувати клієнта"), а служба кібербезпеки негайно сповіщається ("Повідомити службу кібербезпеки").

У випадку внутрішнього шахрайства була розроблена окрема інформаційна модель з використанням нотації DFD (рис. 3.4) для виявлення шахрайських дій, скоєних власним персоналом банку.

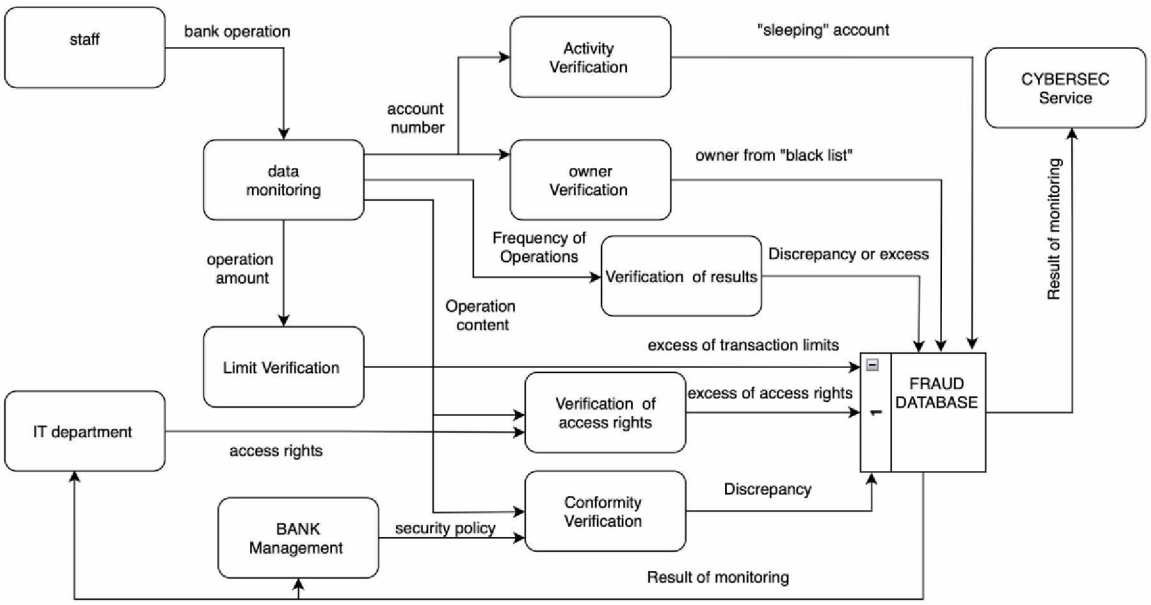

Рисунок 3.4 – Інформаційна модель виявлення ознак шахрайств персоналу банку

Модель, зображена на Рисунку 3.4, відображає інформаційні потоки, що беруть участь у перевірці операцій банку модулем "Моніторинг даних" з метою виявлення потенційних ознак шахрайства. Ретельній перевірці підлягають наступні аспекти:

- "Перевірка діяльності" ретельно вивчає активність на рахунку, щоб виявити випадки, коли працівники банку використовують "сплячі рахунки" для отримання особистої вигоди.

- "Верифікація власника" перевіряє власників рахунків за різними критеріями, такими як наявність у "чорному списку", іноземні громадяни, померлі особи тощо.

- "Перевірка лімітів" забезпечує дотримання лімітів операцій, встановлених НБУ, політикою банку, посадовими інструкціями та іншими відповідними вимогами. Будь-які випадки перевищення лімітів транзакцій позначаються як "Перевищення лімітів транзакцій".

- "Частота операцій" оцінює рівень активності працівників банку, перевіряючи дотримання встановлених банківських стандартів. Ця перевірка виявляє випадки, коли співробітники відхиляються від встановлених норм, демонструючи невідповідність або перевищення очікуваної частоти.

- "Перевірка прав доступу" перевіряє, чи відповідають операції співробітників призначеним їм правам доступу. Вона розглядає випадки, коли співробітники перевищують призначені їм привілеї, проводячи операції, що виходять за межі їх функціональних обов'язків і посадових інструкцій, що називається "Перевищенням прав доступу".

- "Перевірка відповідності" гарантує, що операції співробітників відповідають політиці безпеки банку. Сюди входять такі сценарії, як несанкціоноване копіювання бази даних, використання некорпоративних електронних поштових скриньок, доступ до клієнтських рахунків без належного дозволу, особливо VIP-клієнтів, і так далі.

Результати цих перевірок накопичуються в базі даних шахрайств, обробляються і згодом передаються до служби кібербезпеки банку, IT-департаменту та керівництва банку для вжиття відповідних заходів.

Відповідно до запропонованої інформаційної моделі (рис. 3.4) була розроблена діаграма процесу транзакції за участю персоналу банку, що включає заходи з виявлення шахрайства з використанням нотації BPMN 2.0 (рис. 3.5).

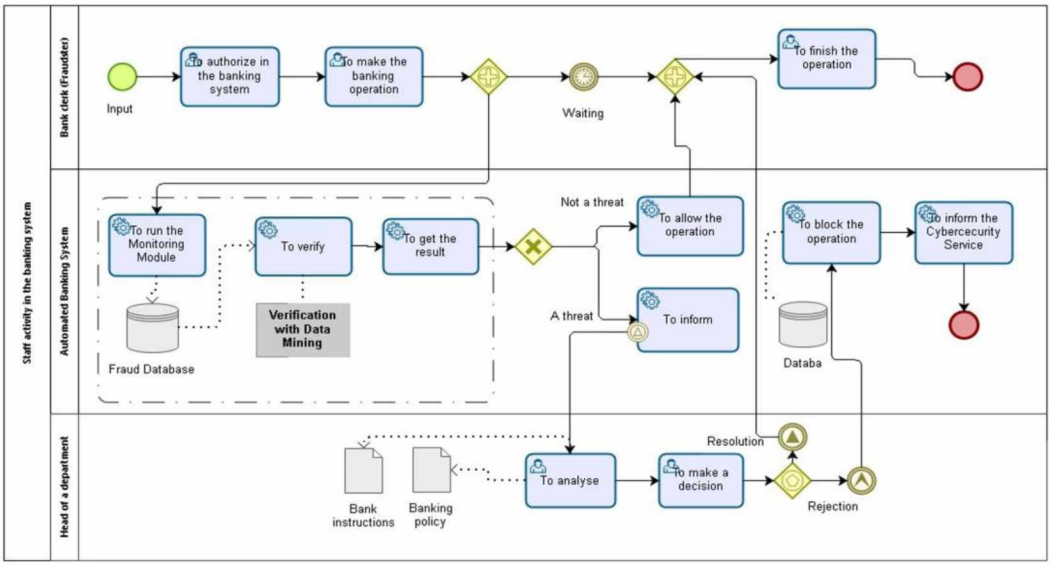

Рисунок 3.5 – Схема процесу здійснення операцій персоналом банку [22]

Процес розгортається наступним чином:

1) Працівник банку, який потенційно може бути залучений до шахрайських дій ("Банківський працівник (Шахрай)"), входить до банківської системи для авторизації свого доступу ("Авторизація в банківській системі") та переходить до проведення банківської операції ("Здійснення банківської операції").

2) Автоматизована банківська система проводить ретельну перевірку операції на наявність ознак шахрайства ("Перевірка за допомогою інтелектуального аналізу даних"). Цей процес передбачає звернення до встановлених критеріїв, що зберігаються в інформаційній моделі, зображеній на рисунку 4.5 ("База даних шахрайства").

3) Якщо транзакція відповідає всім критеріям і не має ознак шахрайства з боку персоналу, система надає дозвіл на проведення операції ("Дозволити операцію"), що дозволяє співробітнику успішно завершити транзакцію ("Завершити операцію").

4) У разі виявлення системою підозрілих шаблонів або ознак шахрайства, система негайно повідомляє про це керівника відповідного відділу, відповідального за проведення операції. Керівник підрозділу аналізує надану інформацію ("Проаналізувати") та приймає обґрунтоване рішення ("Прийняти рішення").

5) Якщо за результатами аналізу операція визнана допустимою, співробітник отримує необхідне погодження і приступає до завершення операції.

6) Якщо ж операція викликає тривогу і вважається потенційно шахрайською, система блокує транзакцію ("Блокувати операцію") та оперативно інформує службу кібербезпеки ("Інформувати службу кібербезпеки").

3.2 Рекомендації щодо системи фінансової безпеки для банківського сектору

Впровадження запропонованих моделей відіграватиме важливу роль у виявленні основних факторів та індикаторів, які можуть призвести до шахрайства, незаконних дій або негативних наслідків як для банку, так і для його клієнтів. Завдяки системному підходу ці моделі об'єднують усіх зацікавлених осіб, незалежно від їхнього внутрішнього чи зовнішнього середовища. Крім того, розроблені моделі закладають основу для створення автоматизованого модуля моніторингу, призначеного для ретельної перевірки банківських операцій та транзакцій на наявність ознак шахрайства. Такий модуль необхідний для системного вирішення проблем, пов'язаних з виявленням та запобіганням шахрайству в банківській сфері. Зрештою, такий підхід сприяє комплексній інтеграції всіх бізнес-процесів банку в єдину автоматизовану банківську систему. Впровадження автоматизованої системи моніторингу підвищує ефективність системи управління, надаючи своєчасні попередження та сприяючи оперативному прийняттю рішень.

Для банків важливо постійно вдосконалювати механізми виявлення шахрайства, використовуючи передові технології, такі як штучний інтелект і машинне навчання. Ці технології можуть значно підвищити точність та ефективність виявлення шахрайства, допомагаючи банкам випереджати нові загрози. Крім того, розвиток культури етики, підзвітності та прозорості в організації має вирішальне значення для стримування та запобігання шахрайським діям. Регулярні навчальні та інформаційні програми для співробітників можуть ще більше посилити захист банку від шахрайства, гарантуючи безпеку як установи, так і її клієнтів.

Шахрайство з банківськими картками є серйозною проблемою в онлайн-бізнесі, оскільки воно може перешкоджати зростанню та призводити до фінансових втрат. Шахраї використовують вразливості, використовуючи викрадені дані карток, отримані різними способами, такими як скімінг, злом погано захищених веб-сайтів або технологічне шахрайство з банкоматами. Коли клієнти вводять дані своєї картки під час онлайн-транзакцій, вони можуть бути перехоплені або скомпрометовані, що призводить до несанкціонованих покупок і втрати коштів.

Попереднє моделювання є важливим кроком у розробці ефективної інформаційної системи. Воно дає цілісне уявлення про дані системи, що дозволяє застосувати системний підхід до проекту. Під час початкового дослідження визначаються найважливіші елементи даних, враховуючи їхній обсяг і частоту використання в процесах. Ця підгрупа інформації формує основу для створення надійної моделі даних і підсистем всередині системи.

Система виявлення шахрайства складається з декількох компонентів або підсистем. До них відносяться служба Fraud Predictor, яка використовує різні фільтри для виявлення потенційно шахрайських транзакцій, журнал транзакцій, який зберігає записи про операції з банківськими картками, та служба SMS API, яка перевіряє транзакції шляхом надсилання повідомлень на мобільні телефони. Крім того, невід'ємною частиною системи є клієнтські веб-додатки, такі як банківський додаток для відображення транзакцій для виявлення шахрайських дій.

Взаємодія між компонентами єдиної системи відбувається у певній послідовності:

1. Клієнт ініціює запит до системи.

2. Сервіс виявлення шахрайства обробляє запит і повертає результат із зазначенням того, чи є платіж шахрайським.

3. Дані про транзакцію зберігаються.

4. У разі необхідності запускається додаткове вікно верифікації.

5. Результат верифікації повідомляється клієнту.

6. Клієнт вводить код верифікації, отриманий у повідомленні.

7. Інформація про транзакцію оновлюється відповідним чином.

8. Клієнту повертається фінальний результат.

Кроки з 4 по 8 виконуються лише у випадку виявлення шахрайського платежу.

Для опису та моделювання бізнес-процесів можуть використовуватися різні нотації моделювання:

- BPMN (Business Process Model and Notation): Забезпечує візуальне представлення процесів за допомогою стандартних блок-схем.

- BPEL (Business Process Execution Language): Мова XML для виконання бізнес-процесів у вигляді послідовності веб-сервісів.

- DFD (Data Flow Diagramming): Описує потоки даних та обмін інформацією в системі, включаючи документообіг.

- IDEF0 (Моделювання бізнес-процесів): Методологія опису бізнес-процесів, яка включає в себе входи, виходи, засоби контролю та механізми управління процесами.

- IDEF3 (моделювання робочих потоків): Зосереджується на описі робочих потоків і включає алгоритмічні методи побудови діаграм бізнес-процесів.

- XPDL (XML Process Definition Language): Формат для обміну описами бізнес-процесів між BPM-системами.

У нашому випадку ми будемо використовувати нотації IDEF0 та IDEF3 для опису бізнес-моделі нашої системи.

При розробці автоматизованого модуля виявлення шахрайських операцій з банківськими картками важливо враховувати елементи, перераховані в таблиці 3.1 (специфічні для контексту звіту). Ці елементи є важливими орієнтирами для побудови ефективної та комплексної системи виявлення шахрайства.

Таблиця 3.1 – Опис основних елементів контекстної діаграми

Елемент	Опис	Тип
Онлайн операція	Операція купівлі товару в інтернет-магазині за допомогою банківської картки	Input
Історія платежів	Попередні операції в Інтернеті	Input

Елемент	Опис	Тип
Законодавство України	Закони України, що регулюють процес проведення онлайн-платежів та взаємодію його учасників	Control
Фільтри системи	Критерії, яким повинні відповідати нешахрайські операції	Control
Стандарт безпеки PCI DSS	Стандарт безпеки даних індустрії банківських платіжних карток	Control
МПС	Міжнародна платіжна система	Mechanism
Веб-додаток	Форми для зв'язку з клієнтом	Mechanism
Банк	Банк, який випустив банківську картку клієнту	Mechanism
Клієнт	Особа, яка проводить платіж в мережі Інтернет	Mechanism
Проведений платіж	Успішно проведена транзакція клієнта	Output
Шахрайська операція	Виявлена шахрайська операція	Output

Наступним кроком є декомпозиція попередньої таблиці, тобто розбиття на частини (підпроцеси), щоб глибше розібрати даний процес виявлення шахрайських операцій

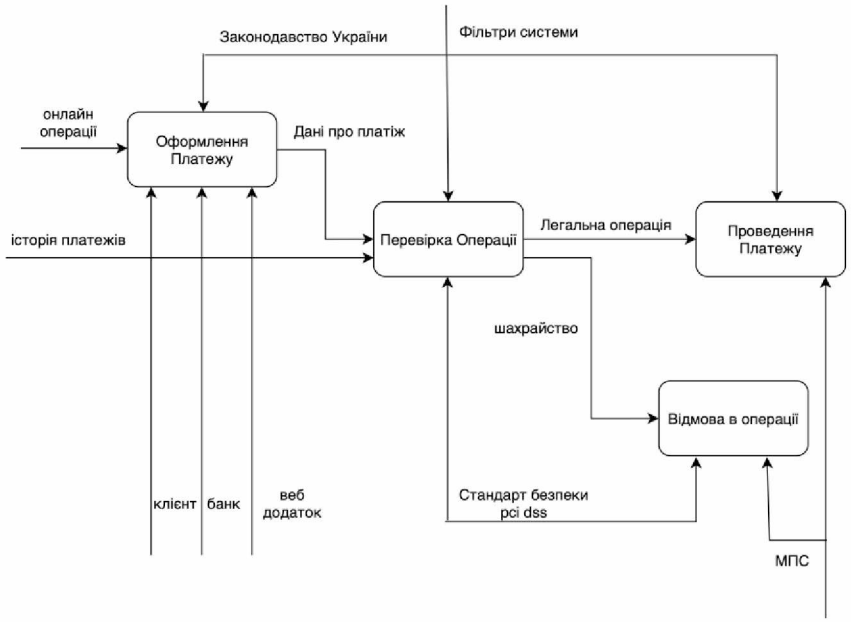

Рисунок 3.6 – процес виявлення шахрайських операцій

Оформлення платіжу виконується наступним чином:

1.Заповнення форми купівлі товару в Інтернеті

2. Моніторинг операції та аналіз її на можливість шахрайства

3. Підтвердження транзакції купівлі

4. Операцію визнано шахрайською, транзакція відхилена

Перевірка операцій містить в собі наступне:

- Оформлення платежу (ОНЛАЙН ОПЕРАЦІЯ)
- Перевірка операції – перегляд історії платежів
- Оформлення платежу, проведення платежу згідно законодавства України
- Перевірка та відмова операції здійснюється за допомогою фільтрів системи та стандартів безпеки
- Оформлення й проведення платежу на стороні клієнта, банка та веб-додатка
- Проведення чи відмова міжнародної платіжної системи

На основі даних про платіж система здійснює перевірку та робить свій висновок. В результаті чого платіж проводиться, або блокується як шахрайська операція.

Оформлення платежу виглядає наступним чином: заповнення банківських реквізитів, адреси доставки та визначення місцезнаходження клієнта

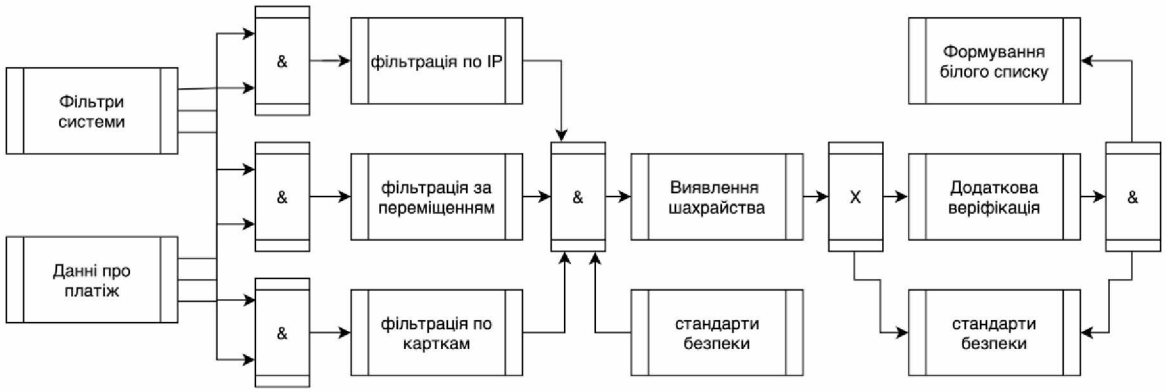

Рисунок 3.7 – IDEF3 діаграма системи виявлення шахрайства[22]

Опис робіт діаграми

Процеси

- Фільтрація по IP – процес порівняння поточного місця знаходження та адреси доставки
- Фільтрація за переміщенням – Процес аналізу швидкості переміщення клієнта
- Фільтрування по картках – Розрахунок унікальних банківських карт
- Виявлення шахрайства – узагальнення результатів роботи фільтрів
- Додаткова верифікація – підтвердження достовірності особи, яка здійснює платіж
- Формування «білого списку» - процес верифікаціх банківських карт та IP-адрес

База даних

- Дані про платіж - інформація про місце знаходження клієнта, адреса замовлення, минулі платежі
- «Білий» список - карти, платежі за якими не потребують підтвердження

•Фільтри системи - фільтри, які використовуються для виявлення шахрайства

•Історія платежів – список всіх транзакцій по окремій картці

•Стандарт безпеки – вимоги забезпечення безпеки даних банківських карт

Впровадження автоматизованого модуля вимагає створення інформаційного забезпечення, яке буде представлено у вигляді реляційної бази даних. Саме в цій базі даних буде зберігатися основна інформація, пов'язана з верифікацією шахрайства при здійсненні платежів. Важливо зазначити, що дані, які стосуються валідації банківських карток та CVV2, зберігатимуться у відповідних банках, а не в цьому автоматизованому модулі.

Усю інформацію, яку обробляє автоматизований модуль, можна поділити на три групи:

- Інформація, яку надають клієнти під час здійснення транзакцій.

- Інформація, що зберігається в системі, включаючи історію транзакцій.

- Інформація, що відображається співробітникам банку для перегляду та аналізу.

Для ефективного зберігання та впорядкування наданої інформації в системі необхідно створити наступні сутності:

- сутність "клієнти", в якій зберігається інформація про самих клієнтів.

- сутність "картки", що відповідає за зберігання даних про банківські картки.

- сутність "транзакції", що містить інформацію про всі здійснені транзакції.

- сутність "шахрайства", призначена для реєстрації транзакцій, ідентифікованих як шахрайські.

- сутність "location", що слугує довідником на основі IP-адрес для визначення місця проведення транзакцій.

- сутність "location_ua", спеціально розроблена для визначення місцезнаходження в межах України на основі IP-адрес.

Основна логіка автоматизованого модуля полягає в його функціональному та алгоритмічному забезпеченні. Основним завданням цього модуля є виявлення шахрайських транзакцій та відповідне управління ними. Для цього в модулі

використовується система аналізу, яка оцінює онлайн-платежі за різними параметрами, надаючи результати для кожного компонента системи. Ця внутрішня система аналізу складається з трьох фільтрів, і на кожному етапі система оцінює, чи є транзакція шахрайською, повертаючи відповідний результат.

Для візуального представлення сутностей, їхніх атрибутів та взаємозв'язків між ними, будь ласка, зверніться до структурної схеми на Рисунку 3.8. Ця діаграма демонструє взаємозв'язок та структуру сутностей в автоматизованому модулі.

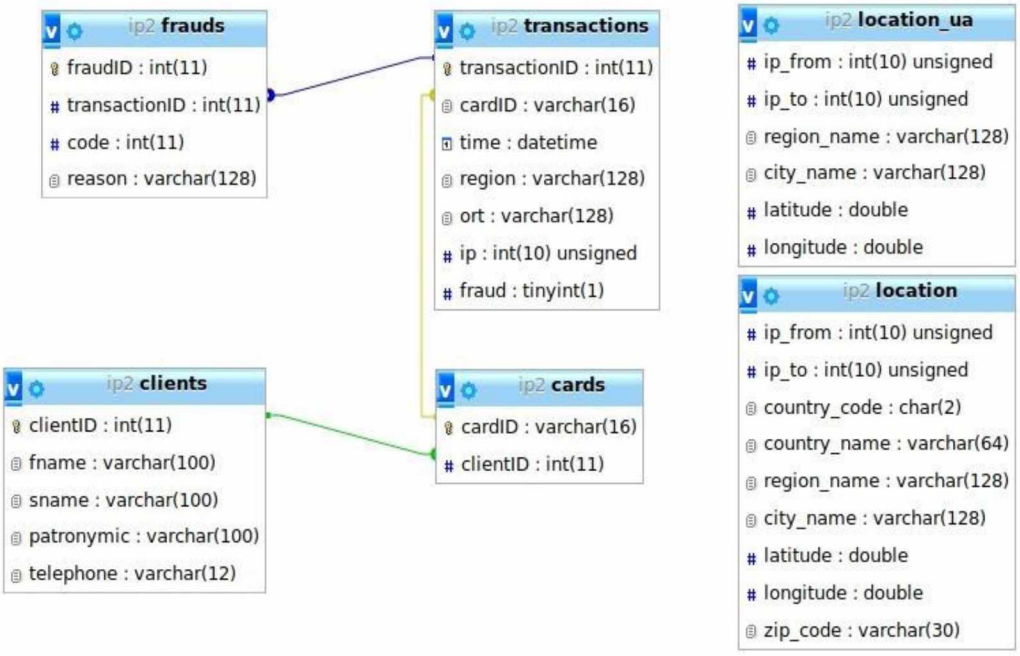

Рисунок 3.8 – Схема бази даних автоматизованого модуля виявлення шахрайських операцій з картками

Для вдосконалення автоматизованої системи доцільно підвищувати її складність і додавати нові функції. Додавання додаткових фільтрів для перевірки платежів може допомогти зменшити кількість шахрайських транзакцій. Однак дуже важливо дотримуватися балансу, оскільки ці фільтри також можуть впливати на коефіцієнт конверсії. Тому дуже важливо налаштувати систему під конкретні типи електронної комерції.

Для компаній, які продають низькомаржинальні, дорогі товари, стає необхідним продавати значні обсяги продукції, щоб компенсувати втрати від шахрайства. У таких випадках мінімізація кількості шахрайських транзакцій має

вирішальне значення. І навпаки, для бізнесу, де продукт або послуга приносить понад 80% прибутку, пріоритетом стає максимізація коефіцієнта конверсії.

Для впровадження ефективної фільтрації платежів я рекомендую розглянути наступні заходи:

- Фільтрація на основі операційної системи та пристрою, з якого здійснюється платіж.

- Фільтрація на основі суми платежу, особливо коли ціна покупки перевищує 90% заощаджень на рахунку.

- Фільтрація для виявлення випадків недостатньої кількості коштів.

- Фільтрація на основі характеристик придбаних товарів.

Крім того, для подальшого вдосконалення системи доцільно надати співробітникам банку можливість формувати звіти, зберігати їх для подальшого використання та імпортувати відповідні дані за потреби. Ця функція розширить їхні можливості з аналізу та моніторингу транзакцій, що сприятиме більш ефективному виявленню та запобіганню шахрайству.

Висновки до третього розділу

Ми провели розробку інформаційної моделі виявлення ознак шахрайства у банках. В процесі дослідження було встановлено, що інформаційна модель є важливим інструментом для виявлення та аналізу шахрайських дій у банківському секторі. Були розглянуті основні етапи розробки моделі, включаючи збір та обробку даних, визначення ознак шахрайства, розробку алгоритмів виявлення та аналіз результатів.

Також були надані рекомендації щодо системи фінансової безпеки для банківського сектору. Було виявлено, що ефективна система фінансової безпеки є критично важливою для запобігання шахрайству та забезпечення стійкості банківської системи. Були розглянуті такі аспекти, як розробка політик та процедур фінансової безпеки, впровадження заходів контролю та моніторингу, підвищення

свідомості та навчання персоналу, встановлення механізмів співпраці з правоохоронними органами та інші.

Рекомендації, надані в даному розділі, можуть бути використані як основа для подальшої розробки та впровадження системи заходів фінансової безпеки, що сприятиме запобіганню шахрайству та підвищенню стійкості банківської системи.

ВИСНОВКИ

Результати дослідження заклали основу для створення ефективної системи кібербезпеки банків, спрямованої на боротьбу з шахрайством.

Вищезазначені результати дослідження в сукупності сприяють розвитку передової системи кібербезпеки банків, сприяючи запобіганню та виявленню шахрайських операцій, захищаючи при цьому банківський сектор та його стейкхолдерів. Використання цього підходу сприятиме створенню інформаційного сховища, яке підтримуватиме прийняття рішень щодо посилення заходів кіберзахисту. Це дозволить зосередити увагу на країнах з високим ризиком відмивання коштів, що сприятиме розробці нових інструментів моніторингу, аналізу, оцінки та прогнозування фінансових транзакцій, що здійснюються за межами національних кордонів.

Крім того, створено функціональний прототип автоматизованого модуля для виявлення шахрайських онлайн-транзакцій з банківськими картками. Цей модуль дозволяє відстежувати транзакції, що мають потенційні ознаки шахрайства, з урахуванням різних параметрів, таких як номери карток клієнтів, місця проведення транзакцій, адреси доставки тощо. Використовуючи цей модуль, клієнти можуть бути попереджені про потенційні випадки шахрайства, таким чином ефективно запобігаючи шахрайським діям.

Подальші дослідження мають бути спрямовані на розробку методичних рекомендацій щодо створення системи незалежного аудиту для боротьби з внутрішнім шахрайством з боку банківського персоналу. Ця ініціатива дасть змогу комерційним банкам впроваджувати комплекс превентивних заходів у цій сфері.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Кібальник Л. О. Концептуальний підхід до формування інформаційної безпеки банківських установ в системі економічної безпеки [Електронний ресурс] / Л. О. Кібальник, І. Ю. Напора // Ефективна економіка.

2. Кібальник Л. О. Впровадження політики інформаційної безпеки банківських установ [Електронний ресурс] / Л. О. Кібальник, І. Ю. Напора // Причорноморські економічні студії. - 2016. - Вип. 12(2). - С. 119-122. - Режим доступу: http://nbuv.gov.ua/UJRN/bses_2016_12(2)_ 23.

3. Король О. Г. Аналіз загроз і механізмів забезпечення безпеки інформації в системі електронних платежів комерційного банку України [Електронний ресурс] / О. Г. Король // Системи обробки інформації. - 2015. - Вип. 9. - С. 88-95. - Режим доступу: http://nbuv.gov.ua/UJRN/soi_2015_9_21

4. Belotti F., Daidone S., Ilardi G., Atella V. Stochastic frontier analysis using Stata. The Stata Journal. 2013. Vol. 13 (4). P. 719-758.

5. AllFusion® Process Modeler Data Flow Diagramming. Design Guide r7.2 [Електронний ресурс] // The official site of the company “CA”. – 2006. – Режим доступу до ресурсу: https://supportcontent.ca.com/cadocs/0/e002761e.pdf.

6. Business Process Model and Notation (BPMN) version 2.0. [Електронний ресурс] // The official site of the company «Object Management Group». – 2011. – Режим доступу : http://www.omg.org/spec/BPMN/2.0

7. "Information Security in Banking Institutions: The Role of Technology in Security Management" by Charith Perera (https://ieeexplore.ieee.org/document/7397993

8. The Impact of Information Technology on Bank Performance in the Nigerian Banking Industry" by Anastasia Bermudez, Angeles Escriva (https://www.researchgate.net/publication/317444375_The_Impact_of_Information_Technology_on_Bank_Performance_in_the_Nigerian_Banking_Industry)

9. Kaur, P., & Sharma, S. "Security Mechanism for Information Protection in Banking Sector"

https://www.researchgate.net/publication/330452524_Security_Mechanism_for_Information_Protection_in_Banking_Sector

10. Dhande, S. M., & Pacharne, S. V. Information Security and Privacy Mechanisms in Banking Sector https://www.researchgate.net/publication/323723127_Information_Security_and_Privacy_Mechanisms_in_Banking_Sector

11. Khan, N., & Mattoo, M. M "Information Security Management Framework for Banks in India" https://www.researchgate.net/publication/338121393_Information_Security_Management_Framework_for_Banks_in_India

12. Kshetri, Nir "Cybercrime and Cybersecurity in the Global South" https://www.cambridge.org/9781108853279

13. Bélanger, France; Crossler, Robert E.; Ward, Brian T. "The Privacy Paradox: Theorizing the Privacy Behavior of Young Users in the Online Social Networking Context" https://aisel.aisnet.org/misq/vol36/iss4/6/

14. Herath, Thushara; Rao, H. Raghav; Chiu, Chao-Min "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in IT" https://aisel.aisnet.org/cais/vol34/iss1/12/

15. Stahl, Bernd Carsten; Doherty, Neil F.; Shaw, Michael J. "Digital Identity Management: A Multidisciplinary Approach" https://www.cambridge.org/9781108831956

16. Aggarwal, Charu; Xu, Yuan "Privacy-Preserving Data Mining: Models and Algorithms" https://link.springer.com/book/10.1007%2F978-1-4614-8588-7

17. Von Solms, Rossouw; Van Niekerk, Jan “From Information Security to Cyber Security"https://www.sciencedirect.com/science/article/pii/S2212017312002724

18. Zambon, Emilia "Cybersecurity and Human Rights in the Age of Cyberveillance "https://onlinelibrary.wiley.com/doi/abs/10.1111/joac.12355

19. Klischewski, Ralf; Leimeister, Jan Marco"Requirements for IT Security Management Systems: Towards a Standardized Assessment of Information Security" https://aisel.aisnet.org/ecis2010/21/

20. De Hert, Paul; Gutwirth, Serge; Mosquera Valderrama, José Miguel "Legal Instruments for Combating Cybercrime" https://books.google.com/books?id=BRo5DwAAQBAJ

21. Karyda, Maria; Kokolakis, Spyros "Assessing Information Security Culture: A Critical Examination of Current Approaches"https://link.springer.com/article/10.1007/s11416-018-0334-3

22. Яровенко Г.М. Розробка інформаційної моделі виявлення ознак шахрайств у банках / Г.М. Яровенко // Інвестиції: практика та досвід. – 2018. - № 14. – С. 23-28.

ДОДАТОК А
СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті у наукових фахових виданнях України

1. Даков С.Ю., Луценко С.В., Сіренко М.Ю.,Тестування на проникнення Ddos-бота killnet vera, V Міжнародна науково-практична конференція “Проблеми кібербезпеки інформаційно-телекомунікаційних систем (PCSITS), 27-28 ЖОВТНЯ 2022, КИЇВ, Україна",

2. Даков С.Ю., Луценко С.В., Сіренко М.Ю.,Підвищення ефективності моніторингу за допомогою технології Deception, IV Міжнародна науково-практична конференція “Проблеми кібербезпеки інформаційно-телекомунікаційних систем (PCSITS), 24 квітня 2023, КИЇВ, Україна",

ДОДАТОК Б

Склад можливих порушників ІБ банку

Ознака	Види		Склад		Приклади
Відношення до банку	сторонні особи, які здійснюють атаки поза контрольованою зоною банку.	хакери та кіберзлочинці, які свідомо здійснюють деструктивні дії, включаючи використання комп'ютерних вірусів, шкідливого програмного коду та інших типів атак.	хакери; комп'ютерні хулігани; - терористи, кримінальні елементи		- Внедрення шкідливого програмного забезпечення: закладок, вірусів та черв'яків, та їх виконання в системі. - Соціальний інжиніринг, що включає шахрайські дії сторонніх осіб, спрямовані на обман та введення в оману працівників банку. - Диверсії, які передбачають зловмисне фізичне пошкодження апаратного забезпечення та комп'ютерних систем.
		провайдери	провайдери каналів інтернет-провайдери	зв'язку,	- Невдачі при укладанні контрактів з провайдерами, які можуть вплинути на роботу інформаційної системи банку. - Помилки, допущені під час угод з провайдерами, які можуть створити труднощі в роботі інформаційної системи банку. - Недоліки, що виникають при укладанні контрактів з провайдерами, які можуть призвести до проблем в функціонуванні інформаційної системи банку.

		- фірми, які виконують монтаж, пусконалагоджувальні роботи та ремонт обладнання в рамках підрядницьких угод.	- співробітники підтримки; - сервісні інженери.	технічної	- Неповні або неналежні виконання третіми особами своїх зобов'язань перед банком щодо якості, складу, змісту та/або порядку надання послуг, постачання продукції та інших аспектів. Наприклад, невиконання розробниками або постачальниками програмно-технічних засобів та послуг вимог, встановлених банком. - Невиконання третіми особами, зобов'язаними перед банком, встановлених стандартів та вимог щодо якості, складу, змісту та/або порядку надання послуг, постачання продукції та інших аспектів. Це може включати невиконання розробниками або постачальниками програмно-технічних засобів та послуг вимог, встановлених банком.
		клієнти / контрагенти банку			Банк залежить від своїх клієнтів/контрагентів у плані інформаційної безпеки, тому важливо, щоб банк мав впевненість в їх здатності забезпечити належний рівень безпеки.
	внутрішні, які здійснюють атаки,	співробітники банку, які є легальними учасниками процесів в ІС та діють в межах наданих повноважень	- особи, які використовують інформаційну систему (ІС);	захисту	- - Відмова від виконання обов'язків (навмисне неповне або неналежне виконання обов'язків працівниками). - - Недбалість (невиконання або неналежне виконання обов'язків без злого умислу).

	перебуваючи в межах контрольованої зони банку	співробітники банку, які є легальними учасниками процесів в ІС та порушують межі наданих повноважень	- особи, які керують інформаційною системою (ІС); - технічний персонал, що має доступ до апаратного забезпечення; - - особи, які управляють інформаційними системами.		- - Шкідництво (умисне завдання шкоди інформаційним активам). - - Помилки (дії персоналу, які не відповідають встановленим регламентам або практикам, без злого умислу) через нечітко визначені обов'язки, недбалість, недостатнє навчання або кваліфікація персоналу. Виникненню помилок сприяють відсутність дисциплінарного процесу та документування процесів, надання надлишкових повноважень та використання зловмисниками методів соціального інжинірингу на персоналі.
Можливість доступу до банку	персонал, який не має допуску до приміщень, де знаходяться технічні та програмні засоби.				
	персонал, що має право на постійний або тимчасовий доступ до приміщень, де знаходяться технічні та програмні засоби.				

	Характеристика	Вид	Характеристика	Підвиди
Фінансові втрати	Оцінюються в грошовому еквіваленті і мають прямий вплив на фінансовий результат банку.	Очікувані	Сума повторюючихся втрат, які виникають не рідше одного разу на календарний рік і знаходяться в межах оцінки очікуваних фінансових збитків у грошовому еквіваленті.	Структурація втрат визначається індивідуально для кожного банку, враховуючи їх масштаби.
		Неочікувані	Максимальні можливі збитки, які можуть виникнути внаслідок суттєвих недоліків (помилок) в системі внутрішнього контролю або надзвичайних зовнішніх подій, і знаходяться в межах оцінки грошового еквівалента неочікуваних фінансових втрат.	
Нефінансові втрати	Не мають прямого впливу на фінансовий результат діяльності, але можуть мати негативні наслідки для банку.	Очікувані	вплив, який очікується, і не є фінансовим, на значущий період у межах одного календарного року.	Незавдана шкода для репутації або іміджу банку може призвести до наступних наслідків: - Зменшення обсягу проведених транзакцій. - Втрата клієнтів. - Втрата груп клієнтів або портфелю. - Застосування санкцій та стягнень.
		Неочікувані	максимальний можливий вплив, який не є фінансовим, унаслідок серйозних недоліків (помилок) у системі внутрішнього контролю або випадків непередбачених зовнішніх подій.	