Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Система управління інформаційною безпекою для підвищення ефективності захисту банківських транзакцій в системах інтернет-банкінгу
Назва теми

КРКБ 190109.19.01.09 ПЗ
Шифр

Галузь знань 12 «Інформаційні технології»
Шифр, назва

Спеціальність 125 «Кібербезпека»
Шифр, назва

Освітня програма «Кібербезпека»
Назва

Виконала: студентка IV курсу, група КБ-19-1 _____ О.В.Пирч
Підпис Ініціали, прізвище

Керівник _____ 06.06.2023 В.Ю. Тітова
Підпис, дата Ініціали, прізвище

Нормоконтролер _____ 06.06.23 С.В. Мостовий
Підпис, дата Ініціали, прізвище

До захисту допускаю:
Зав. кафедри кібербезпеки _____ Ю.П. Кльоц
Підпис Ініціали, прізвище

«6» 06 2023 р.

Хмельницький 2023

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра КІБЕРБЕЗПЕКИ

Освітній рівень БАКАЛАВР

Галузь знань 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Спеціальність 125 КІБЕРБЕЗПЕКА

Освітня програма ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА ПІДГОТОВКИ БАКАЛАВРІВ

ЗАТВЕРДЖУЮ

Зав. кафедри Ю.П. Кльоц

"1" 03 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Пирч О. В.
Прізвище, ім'я, по батькові студента

1. Тема роботи Розробка системи управління інформаційною безпекою банку

Керівник роботи к.т.н., доц. Тітова В.Ю.
Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджено наказом ректора університету від 01 березня 2023р. №5

2. Строк подання студентом роботи на кафедру

3. Вихідні дані до проекту (роботи) спроєктувати та змоделювати систему управління інформаційною безпекою банку. Передбачити стійкість до найчастіших загроз для системи. Покращити існуючу систему управління інформаційною безпекою банку на основі доступних даних. Вибрати програмне забезпечення (обгрунтувати вибір програмного забепечення за критерієм необхідні функції — легкість використання) для забезпечення проходження дозволеного та блокування забороненого трафік. Провести розрахунок ефективності впроваджених рішень.

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити) Вступ. Аналіз предметної області, аналіз завдання та пошук теоретичної інформації. Побудова системи управління інформаційної безпеки банку. Оцінювання ефективності системи управління інформаційної безпеки банку. Висновки.

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень): «Модель загрози витоку інформації у системі управління інформаційної безпеки банку», «Модель загрози фішингу та соціальної інженерії у системі управління інформаційної безпеки банку». «Діаграма порівняння рівня загроз у системі до та після покращення управління інформаційною безпекою банку »

6. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
		—	
		—	

7. Дата видачі завдання _____2023 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) кваліфікаційної роботи	Термін виконання етапів проекту (роботи)	Примітка
1	Ознайомлення з предметною областю	Січень	–
2	Пошук теоретичної інформації про проектування системи управління інформаційною системою банку	Січень	–
3	Дослідження існуючих рішень	Лютий	–
4	Постановка задачі	Лютий	–
5	Пошук теоретичної інформації про найкращі рішення для покращення системи управління інформаційною безпекою банку	Березень	–
6	Початок впровадження покращень до системи управління інформаційною безпекою банку	Квітень	–
7	Завершення реалізації покращень системи управління інформаційною безпекою банку	Квітень\Травень	–
8	Оформлення пояснювальної записки згідно вимог	Травень	–
9	Оформлення графічної частини	Червень	–
10	Захист КР	08.06.2023	

Студент _____ Підпис _____ Ініціали, прізвище

Керівник проекту (роботи) _____ Підпис _____ Ініціали, прізвище

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Система управління інформаційною безпекою для підвищення ефективності захисту банківських транзакцій в системах інтернет-банкінгу.»

Автор роботи: Пирч Олена Вадимівна.

Керівник роботи: Тітова Віра Юріївна.

Пояснювальна записка: 62 с., 1 додаток, 18 рис., 40 джерел.

Графічна частина: 13 презентаційних слайдів.

СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ СИСТЕМОЮ БАНКУ, ЗАХИСТ БАНКІВСЬКИХ ТРАНАЗКЦІЙ, ЗАХИСТ ІНФОРМАЦІЙНОЇ СИСТЕМИ БАНКУ

Метою роботи є розробка системи управління інформаційною безпекою, яка дозволить підвищити рівень ефективності захисту банківських транзакцій у системах інтернет-банкінгу.

У цій роботі було досліджено і проаналізовано предметну область, теоретичну інформацію про проектування системи управління інформаційною безпекою, а також створено і розроблену таку систему, яка дозволяє протестувати впровадження певних правил або методів захисту інформації в лімітованому середовищі, перш ніж вводити виправлення до всієї системи, що спрощує роботу системних адміністраторів та адміністраторів безпеки банку, щодо модерування системи та її захисту.

05.06.2023

ANNOTATION

Course project: Development of a secure network of the enterprise.

Author of the work: Pyrch O.V.

Supervisor: Titova. V. Y.

Amount - 62 pages, 1 application,18 figures, 40 sources.

Graphic part: 13 presentation slides.

The purpose of the work is to develop an information security management system that allows to increase the level of effectiveness of bank transaction protection in Internet banking systems.

In this work, the subject area, theoretical information on the design of the information security management system was researched and analyzed, and a system was created and developed that allows testing the implementation of certain rules or methods of information protection in a limited environment before introducing corrections to all systems that simplifies the work of system administrators and security administrators of the bank, regarding system moderation and its protection.

05.06.2023

Формат	Зона	Позиц	Позначення	Найменування	Кільк.	Прим.
А4		1	КРКБ.190109.19.01.09 ПЗ	Система управління	62	
				інформаційною безпекою		
				для підвищення		
				ефективності захисту		
				банківських транзакцій в		
				системах інтернет-банкінгу		
				Пояснювальна записка		
А4		2	КРКБ. 190109.19.01.09 Е1	Модель загрози витоку	1	
				інформації у системі		
				управління інформаційною		
				безпекою банку		
А4		3	КРКБ. 190109.19.01.09 Е8	Модель загрози фішингу	1	
				та соціальної інженерії у		
				системі управління		
				інформаційною безпекою		
				банку		
А4		4	КРКБ. 190109.19.01.09 Е8	Діаграма порівняння рівня	1	
				загроз до та після		
				покращення системи		
				управління інформаційною		
				безпекою банку		

Зм.	Арк.	№ Докум.	Підп.	Дата	КРКБ.190109.19.01.09 ВП		
Розробив		Пирч О.В.		06.06.20	Система управління інформаційною безпекою для підвищення ефективності захисту банківських транзакцій в системах інтернет-банкінгу Відомість проекту	Літера	Аркуш	Аркушів
Перев.		Тітова В.Ю.		06.06.20		н	1	1
Н. контр.		Мостовий С.В.		06.06.23		ХНУ, КБ-19-1		
Затв.		Кльоц Ю.П.		6.06.23				

ЗМІСТ

ВСТУП

На сьогодні більшість транзакцій, які проходять у банку, відбуваються за допомогою мережі Інтернет та додатків. Майже кожен банк має додаток для смартфонів, аби спростити доступ до транзакцій простому користувачеві, спонукаючи того робити все самому. Проте з ростом попиту на такі додатки зростає і попит на викрадення інформації.

Раніше, аби отримати якусь банківську інформацію потрібно було фізично проникати у банк, знаходити сейф з усіма документами та красти його. Зараз, у вік мережевих операцій, це стало і простіше з одного боку, і складніше. Простіше, тому що тепер не потрібно нікуди проникати фізично, достатньо проникнути віртуально на персональний комп'ютер чи телефон жертви за допомогою шкідливого програмного забезпечення або ж іншим способом, і вся інформація буде «як на долоні». Проте складніше, адже системи захисту банківських транзакцій є одними із найбільш стійких до зламу.

За останні роки зловмисники дослідили системи управління інформаційною безпекою банків і випадки зламів, або ж витоку інформації, стало набагато більше. Вони пристосувалися, адаптувалися до реалій сьогодення та стали проводити свої хакерські атаки з метою дестабілізації роботи банківських систем та порушення проведення інтернет транзакцій. Все більше і більше банків звертаються до спеціалістів із кібербезпеки, аби ті забезпечили високий рівень захисту інформації.

Завданням кваліфікаційної роботи буде покращення існуючої системи управління інформаційною безпекою, а також впровадження нових рішень, для забезпечення цілісності системи, як комплексної системи захисту від можливих загроз.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Особливості інформаційної безпеки банків

На сьогодні існує дуже багато систем захисту інформації як в Інтернеті, так і в окремо захищених установах. Ні для кого не секрет що певні компанії та певні установи мають вищий ступінь захисту, аніж інші, до прикладу державні установи, установи воєнно-промислового комплексу та установи зв'язані з банківською справою. Через те що в банку на постійній основі і безперестанно відбуваються мільйони, якщо не мільярди переведень грошей, то система захисту у банку є дуже і дуже надійною. Моєю задачею буде проаналізувати існуючі системи захисту інформації у банківських установах та проаналізувати, яка з них краще підійде для побудови власної системи безпеки.
Перш за все потрібно звернути увагу на те, що банківська система будь-якої сучасної держави не існує «сама в собі», а перебуває у тісному взаємозв'язку із банківськими системами інших держав і міжнародними банківськими організаціями, тому проблема забезпечення надійності, безпечності, стабільності банківської діяльності виходить далеко поза межи суто внутрішньодержавного регулювання [1].

В умовах значної залежності банківської діяльності від надійності інформаційних технологій, які вона використовує, забезпечення інформаційної безпеки стає однією з фундаментальних засад існування банківської системи взагалі. Одним з основних напрямів забезпечення інформаційної безпеки будь-якої банківської установи є охорона банківської таємниці.

У структурі інформаційної безпеки банківської установи виділяють такі основні складові:

— безпека інформаційних ресурсів;

— безпека інформаційної інфраструктури;

— безпека «інформаційного поля».

Інформаційні ресурси банківської установи – це взаємозв’язана, упорядкована, систематизована і закріплена на матеріальних носіях інформація, яка належить банківській установі.

— Безпека інформаційних ресурсів полягає у збереженні такої інформації від несанкціонованого розповсюдження, використання і порушення її конфіденційності (таємності).

— Безпека інформаційної інфраструктури полягає у такому стані захищеності електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку банківської установи, яка забезпечує цілісність і доступність інформації, що в них обробляється (зберігається чи циркулює).

— Безпека «інформаційного поля» банківської установи ґрунтується на контрольованості здебільшого несистематизованих потоків інформації, що оприлюднюється різноманітними учасниками інформаційних відносин: телерадіоорганізаціями, друкованими ЗМІ, Інтернет-виданнями, конкурентами, органами державної влади, місцевого самоврядування тощо.

Ураховуючи складність системи захисту інформації банку, необхідність її функціонування в умовах невизначеності, побудова такої системи має базуватися на відповідних принципах [2].

1.2 Огляд існуючих рішень

При створенні системи економічної безпеки банківської установи інформаційна безпека повинна розглядатися як невід'ємна та вкрай важлива її складова. Досягнення інформаційної безпеки банку залежить від проведення збору та аналізу інформації про внутрішнє і зовнішнє середовище банку, аналітичної обробки інформації щодо партнерів та конкурентів, визначення категорій банківської інформації та застосування заходів щодо її захисту, а також

дотримання правил роботи з інформацією персоналом банку та своєчасного виявлення спроб і каналів витоку інформації.

Для організації системи інформаційної безпеки банківських установ необхідний комплексний підхід. Це включає суб'єкти, принципи, нормативно-правову базу, політику інформаційної безпеки та інші складові, які спрямовані на виявлення вразливих місць та загроз і запобігання їх негативному впливу на нормальне функціонування банку.

Загальна концепція організації системи інформаційної безпеки банківських установ полягає в забезпеченні стійкого функціонування банку, виявленні та запобіганні внутрішнім і зовнішнім загрозам інформаційної безпеки. Серед внутрішніх загроз інформації можна виділити втрату інформації, некомпетентність персоналу, розголошення інформації, знищення інформації, викривлення інформації, та її викрадення. На рисунку 1.1 зображено класифікацію основних загроз для банківської системи [3].

Основними завданнями системи інформаційної безпеки є:

— класифікація інформації щодо рівня доступу
— запобігання витоку інформації
— прогнозування і своєчасне виявлення та усунення загроз
— створення механізму та умов оперативного реагування на загрози
— ефективне припинення посягань на інформаційні ресурси

Класифікація інформації щодо рівня доступу означає, що система повинна визначати рівні конфіденційності та встановлювати відповідні обмеження доступу до інформації залежно від її характеру.

Запобігання витоку інформації означає, що система повинна мати механізми та заходи, спрямовані на запобігання несанкціонованого розголошення, витоку або неправомірного використання інформації.

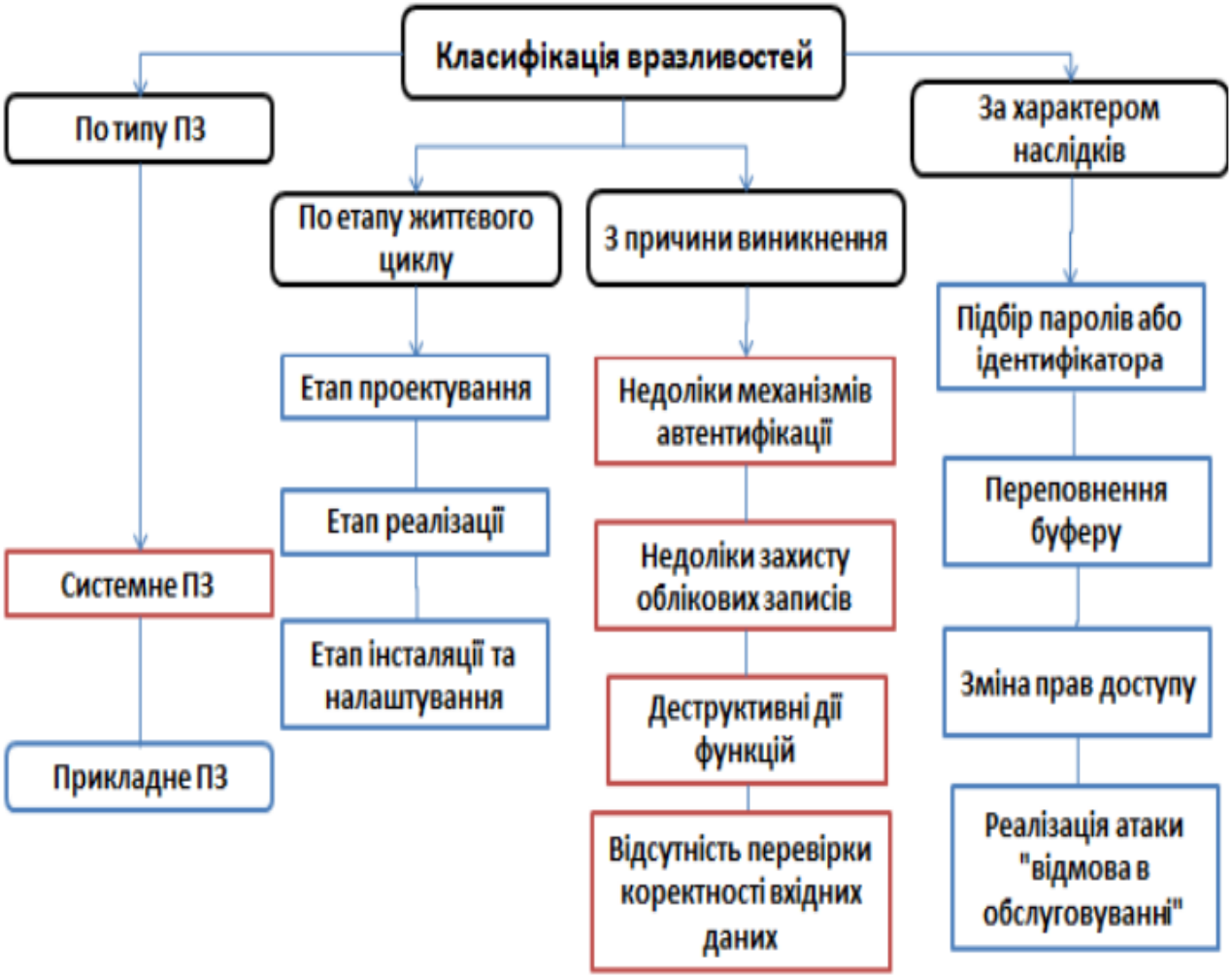


Рисунок 1.1 — Класифікація вразливостей

Прогнозування і своєчасне виявлення та усунення загроз це коли система повинна передбачати можливі загрози інформаційній безпеці банку, а також швидко виявляти їх і приймати відповідні заходи для їх усунення.

Створення механізму та умов оперативного реагування на загрози являє собою реалізовані ефективні процедури та шляхи оперативної реакції на інформаційні загрози, щоб запобігти їхньому негативному впливу на безпеку банку.

Ефективне припинення посягань на інформаційні ресурси означає те, що система повинна використовувати правові, організаційні та технічні заходи та

засоби для ефективного припинення будь-яких посягань на інформаційні ресурси банку.

Ці завдання допомагають забезпечити ефективну інформаційну безпеку банку, захистити конфіденційність, цілісність та доступність його інформаційних ресурсів [4].

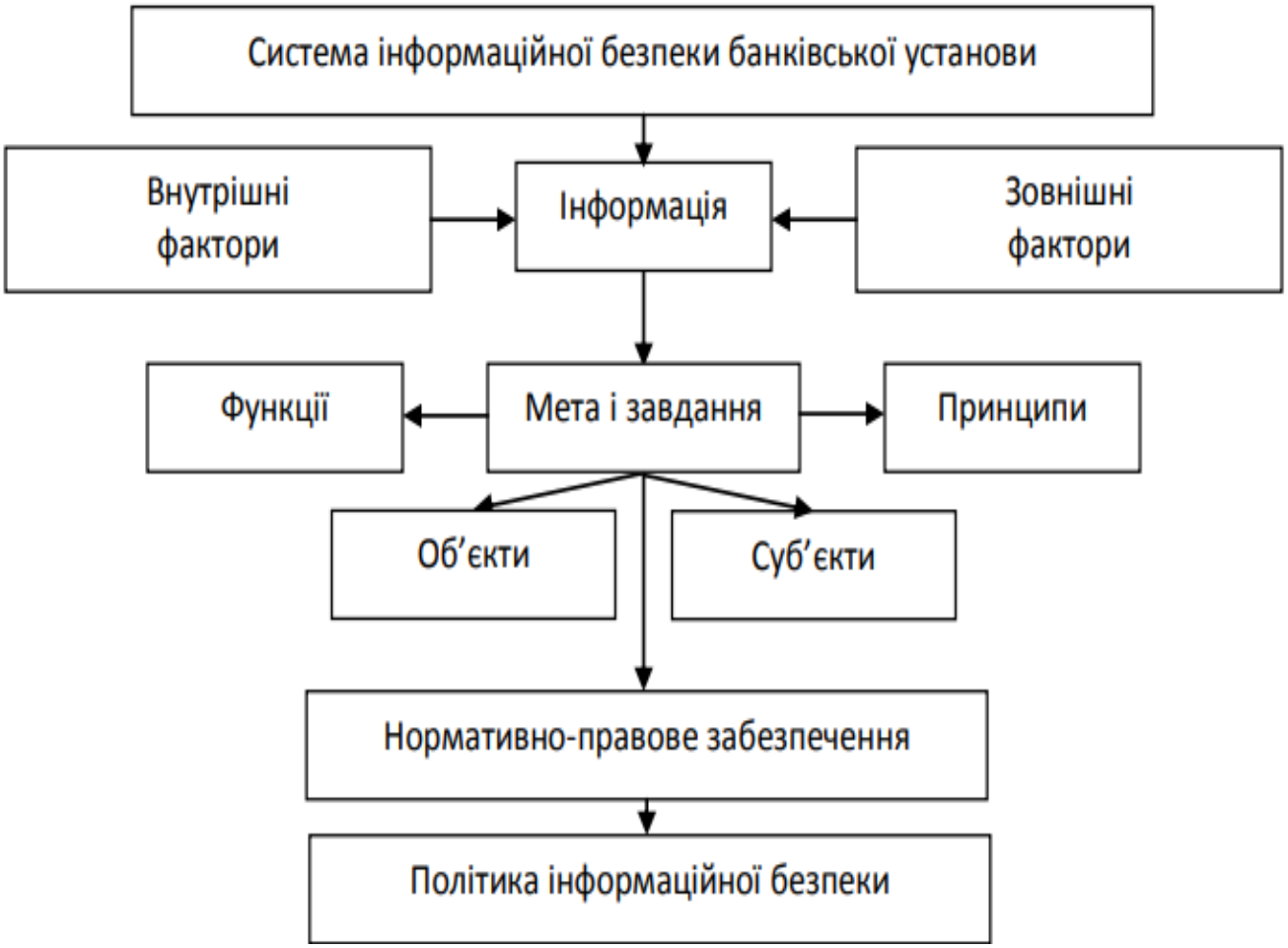


Рисунок 1.2 — Схема системи інформаційної системи для банківських установ

Об'єкти, які підлягають захисту з метою забезпечення інформаційної безпеки банку, включають:

— Інформаційні ресурси (вся інформація, що зберігається, передається та обробляється в банку, включаючи конфіденційну, фінансову та клієнтську інформацію)

— Інформація про персонал (дані про співробітників банку, їхні ідентифікаційні дані, фінансові записи та інші особисті дані, які потребують захисту)

— Програмне забезпечення (всі програми та системи, які використовуються в банку для обробки, збереження та передачі інформації, які повинні бути захищені від несанкціонованого доступу та зловживання)

— Процеси обробки інформації (всі кроки та процедури, пов'язані з обробкою та передачею інформації в банку, які повинні бути захищені від порушень та несанкціонованого доступу)

— Обладнання автоматизованої системи (сервери, комп'ютери, мережеве обладнання та інші технічні засоби, що використовуються для зберігання, обробки та передачі інформації)

— Приміщення (фізичний доступ до приміщень банку також підлягає захисту і потребує впровадження контролю доступу до робочих просторів, захист приміщень від несанкціонованого вторгнення та зловмисних дій) [5].

Серед суб'єктів інформаційної безпеки банку можна виділити:

— Державні органи — органи державного управління, які встановлюють нормативно-правову базу та регулюють діяльність банків з питань інформаційної безпеки.

— Державні інститути — організації, які займаються дослідженнями та розробками в галузі інформаційної безпеки, надають консультаційну підтримку та експертну оцінку.

— Національний банк України (НБУ) — відповідає за забезпечення стабільності фінансової системи та здійснює контроль за дотриманням правил і стандартів інформаційної безпеки банків.

— Керівники банків — відповідають за розробку та реалізацію політики інформаційної безпеки в своїй установі.

— Окремі структурні підрозділи банку — включають в себе відділи з інформаційної безпеки, які відповідають за планування, впровадження та забезпечення заходів з інформаційної безпеки в банку.

— Юридичні та фізичні особи — зовнішні спеціалісти, консультанти або партнери банку, які займаються практичними діями забезпечення інформаційної безпеки або мають договірні відносини з банком.

Принципи організації системи інформаційної безпеки банку включають:

— Комплексність — система інформаційної безпеки повинна охоплювати всі аспекти діяльності банку та всі об'єкти, що підлягають захисту. Це означає, що система повинна враховувати як технічні, так і організаційні аспекти інформаційної безпеки.

— Своєчасність — заходи забезпечення інформаційної безпеки повинні бути впроваджені та підтримуватися в актуальному стані з урахуванням нових загроз та технологічних ризиків.

— Безперервність — система інформаційної безпеки повинна працювати неперервно, забезпечуючи захист інформації в будь-який момент часу і в умовах можливих аварій або інцидентів.

— Активність — система інформаційної безпеки повинна виявляти, моніторити та реагувати на загрози та вразливості в реальному часі. Це включає в себе застосування проактивних заходів для запобігання потенційним загрозам.

— Законність — система інформаційної безпеки повинна дотримуватися відповідних нормативно-правових актів та регуляторних вимог, що стосуються безпеки і конфіденційності інформації.

— Обґрунтованість — заходи забезпечення інформаційної безпеки повинні бути обґрунтовані на основі аналізу ризиків та врахування особливостей банківської діяльності.

— Спеціалізація — система інформаційної безпеки повинна бути адаптована до специфіки банківського сектора та враховувати особливості його діяльності.

— Взаємодія — система інформаційної безпеки повинна забезпечувати співпрацю та взаємодію між всіма елементами системи.

— Удосконалювання — система інформаційної безпеки повинна постійно вдосконалюватись і оновлюватись з урахуванням нових загроз, технологій та найкращих практик в галузі інформаційної безпеки.

— Централізація управління — в установі має бути централізована система управління інформаційною безпекою, що забезпечує координацію, моніторинг та контроль за всіма аспектами інформаційної безпеки.

— Економічна доцільність — заходи забезпечення інформаційної безпеки повинні бути раціональними з економічної точки зору, забезпечуючи оптимальне використання ресурсів і досягнення балансу між витратами та ризиками.

Крім того, у контексті банківських установ, також доцільними є принципи компетентності та конфіденційності:

— Компетентність — система інформаційної безпеки повинна базуватись на компетентності та кваліфікації спеціалістів, які відповідають за розробку, впровадження та управління заходами забезпечення безпеки.

— Конфіденційність — система інформаційної безпеки повинна забезпечувати конфіденційність інформації, що обробляється та зберігається в банку, а також забезпечувати захист персональних даних клієнтів та інших конфіденційних відомостей.

Нормативно-правове забезпечення інформаційної безпеки банківських установ визначається законодавчими актами держави. Ці акти регулюють правила використання, опрацювання та передачі інформації обмеженого доступу та встановлюють ступінь відповідальності за порушення цих правил. Нормативна база може включати закони, постанови, накази, стандарти та інші документи, які визначають вимоги до інформаційної безпеки банківських установ [6].

Політика інформаційної безпеки банку визначає загальні принципи, цілі та стратегію забезпечення безпеки інформації. Вона повинна бути узгоджена з місією та стратегічними цілями банку і включати в себе положення щодо організації, структури, відповідальності, процедур і технічних заходів забезпечення інформаційної безпеки.

Система інформаційної безпеки банку повинна функціонувати як комплексний механізм, який включає в себе різноманітні заходи технічного, організаційного та адміністративного характеру. До основних функцій системи інформаційної безпеки можна віднести:

— Ідентифікація та класифікація інформації — встановлення процедур і правил для ідентифікації та класифікації інформації за її важливістю та рівнем конфіденційності.

— Аутентифікація та авторизація — встановлення процедур і механізмів для перевірки і підтвердження ідентичності користувачів та надання їм відповідних прав доступу до інформації.

— Захист від несанкціонованого доступу — використання технічних засобів і заходів безпеки для запобігання несанкціонованому доступу до інформації, включаючи встановлення мережевих фаерволів, шифрування.

— Захист від вторгнень — встановлення систем захисту від вторгнень (Intrusion Detection Systems - IDS) та систем захисту від вторгнень інформаційних систем (Intrusion Prevention Systems - IPS) для виявлення та блокування спроб несанкціонованого доступу до мережі та систем банку.

— Забезпечення цілісності інформації — застосування механізмів контролю цілісності даних, таких як цифровий підпис, хеш-функції, контрольні суми тощо, для забезпечення недоступності, втрати або зміни інформації під час передачі та зберігання.

— Резервне копіювання та відновлення даних — регулярне проведення резервного копіювання інформації та розробка планів відновлення даних для забезпечення доступності та інтегритету даних в разі виникнення аварійних ситуацій чи катастроф.

— Моніторинг та аудит — систематичне спостереження за діяльністю мережі та інформаційних систем банку, виявлення аномальних подій та інцидентів, а також проведення аудиту системи інформаційної безпеки з метою виявлення потенційних вразливостей та покращення безпеки.

— Свідомість та навчання персоналу — проведення навчань, тренінгів та інформаційних кампаній з питань інформаційної безпеки для підвищення обізнаності персоналу щодо загроз, процедур та політики безпеки, а також встановлення дисципліни використання інформаційних ресурсів та засобів.

Ці принципи та функції системи інформаційної безпеки спрямовані на забезпечення конфіденційності, цілісності та доступності інформції для банку. Конфіденційність означає, що інформація має бути доступна лише авторизованим користувачам та захищена від несанкціонованого доступу. Цілісність передбачає, що інформація має бути збережена у своєму первісному, недокорегованому стані та захищена від непередбачуваних змін або втрати. Доступність означає, що інформація повинна бути доступною та функціональною для авторизованих користувачів у потрібний момент часу.

Для ефективного функціонування системи інформаційної безпеки банку необхідно враховувати як внутрішні, так і зовнішні фактори. Внутрішні фактори включають персонал банку, його структуру, процеси та ресурси, які впливають на безпеку інформації. Зовнішні фактори можуть включати загрози з боку зловмисників, зміни в законодавстві, технологічні ризики тощо.

Крім того, система інформаційної безпеки банку має бути комплексною, своєчасною, безперервною, активною, законною та обґрунтованою. Це означає, що система повинна охоплювати всі аспекти безпеки інформації, бути орієнтованою на сучасні технології та відповідати вимогам, що змінюються та загрозам. Вона має працювати неперервно, забезпечуючи захист протягом усього часу. Активність передбачає постійне вдосконалення системи, виявлення та реагування на загрози та інциденти безпеки. Законність означає додержання вимог нормативно-правової баз и та виконання всіх необхідних правил і процедур забезпечення інформаційної безпеки. Обґрунтованість вимагає наявності чіткого обґрунтування і підходу до вибору заходів забезпечення безпеки, які відповідають конкретним потребам та загрозам банку.

При організації системи інформаційної безпеки банку також важливо враховувати принципи компетентності та конфіденційності. Компетентність передбачає наявність кваліфікованого персоналу, здатного ефективно впоратися з

викликами та завданнями інформаційної безпеки. Конфіденційність означає забезпечення конфіденційності інформації, особливо у випадку з фінансовою інформацією клієнтів та банківськими даними [7].

Нормативно-правове забезпечення інформаційної безпеки банківських установ визначається законодавчими актами держави. Ці законодавчі акти регулюють правила використання, опрацювання та передачі обмеженого доступу інформації та встановлюють ступінь відповідальності за порушення цих правил. Банк повинен дотримуватися вимог законодавства щодо інформаційної безпеки та приймати всі необхідні заходи для їх виконання [8].

1.3 Постановка задачі

Отже, комплексний підхід є важливим для забезпечення ефективної інформаційної безпеки в банківських установах. Він передбачає використання всіх доступних засобів захисту і методів на всіх етапах роботи з інформацією. Це може включати технічні заходи, які використовуються для захисту інформаційних ресурсів, такі як шифрування даних, використання міцних паролів, фізичний контроль доступу до обладнання і приміщень, а також заходи забезпечення безпеки програмного забезпечення та мережі.

Також важливим аспектом є постійне оновлення і удосконалення системи захисту залежно від змін у внутрішніх і зовнішніх умовах. Технології швидко розвиваються, а загрози інформаційній безпеці постійно змінюються, тому необхідно забезпечувати актуальність і ефективність заходів безпеки шляхом регулярного аудиту, оновлення програмного забезпечення, навчання персоналу і впровадження новітніх методів захисту.

Щодо перспектив подальших досліджень, детальна конкретизація запропонованих елементів системи інформаційної безпеки банківських установ дозволить побудувати ще більш ефективну і адаптовану до потреб банківського сектору систему захисту. Дослідження можуть спрямовуватись на вдосконалення

методів інтеграції різних засобів захисту, виявлення і аналіз нових загроз, розробку та впровадження новітніх технологій захисту і вдосконалення процедур управління інформаційною безпекою. Аби створити хорошу систему управління інформаційною безпекою банків, я буду покращувати конкретні аспекти уже готової системи, аби вона краще протистояла різним загрозам, особливо тим, які у останні роки набрали обертів через розвиток технологій.

2 ПОБУДОВА СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ (СУІБ)

2.1 Графічна модель СУІБ

З наведених вище переліків всього потрібного для створення дійсно захищеного банку я зробила висновок, що нам потрібна система ABBA.

Конструкція ABBA дотримується модульного підходу, щоб забезпечити можливість майбутніх розширень, зокрема додавання нових агентів та/або визначення нових правил поведінки, що регулюють агентів відповіді. ABBA реалізовано в NetlLogo, спеціалізованому багатоагентному моделюванні середовища (Wilensky, 1999).

У ABBA банки демонструють усі чотири характеристики та кваліфікуються як агенти. Заощаджувачі є гетерогенні та демонструють просту адаптивну поведінку, але не змінюють її та не демонструють автономію. Кредити та міжбанківські позики позбавлені всіх характеристик, крім неоднорідності. Заощаджувачі, позики та міжбанківські позики - це те, що називають протоагентами. Для простоти ми називаємо агентами і протоагентів, і агентів.

Агенти живуть у світі, розділеному на різні регіони. У цьому світі і заощадники, і кредити рівномірно розподілені по регіонах. На початковому етапі кожен регіон є домінує регіональний банк, який збирає вклади вкладників і надає кредити корпорації. На наступних етапах банки можуть почати залучати депозити та видавати кредити різні регіони. Це припущення не має вирішального значення для аналізу ризиків у банківській системі, але створює необхідну основу для розуміння динаміки транскордонної банківської діяльності.

Банки є найскладнішими агентами в ABBA. Банкам потрібно залучати депозити, розгортати їх депозити для фінансування ризикованих позик, водночас створюючи резерви на очікувані збитки.

Банки також повинні визначити суму власного капіталу та резервів, необхідних для задоволення мінімуму регулятивний капітал і резервні вимоги. Платоспроможні банки не відповідають вимогам може зменшити борг або провести оптимізацію ваги ризику, щоб збільшити свої резерви капітал до активів,

зважених на ризик. Незабезпечені міжбанківські позики від банків із надлишковими резервами може служити для задоволення резервних вимог. На рисунку 2.1 є ілюстрація різних рішень які банк повинен взяти на себе і свою взаємодію з іншими агентами в системі.

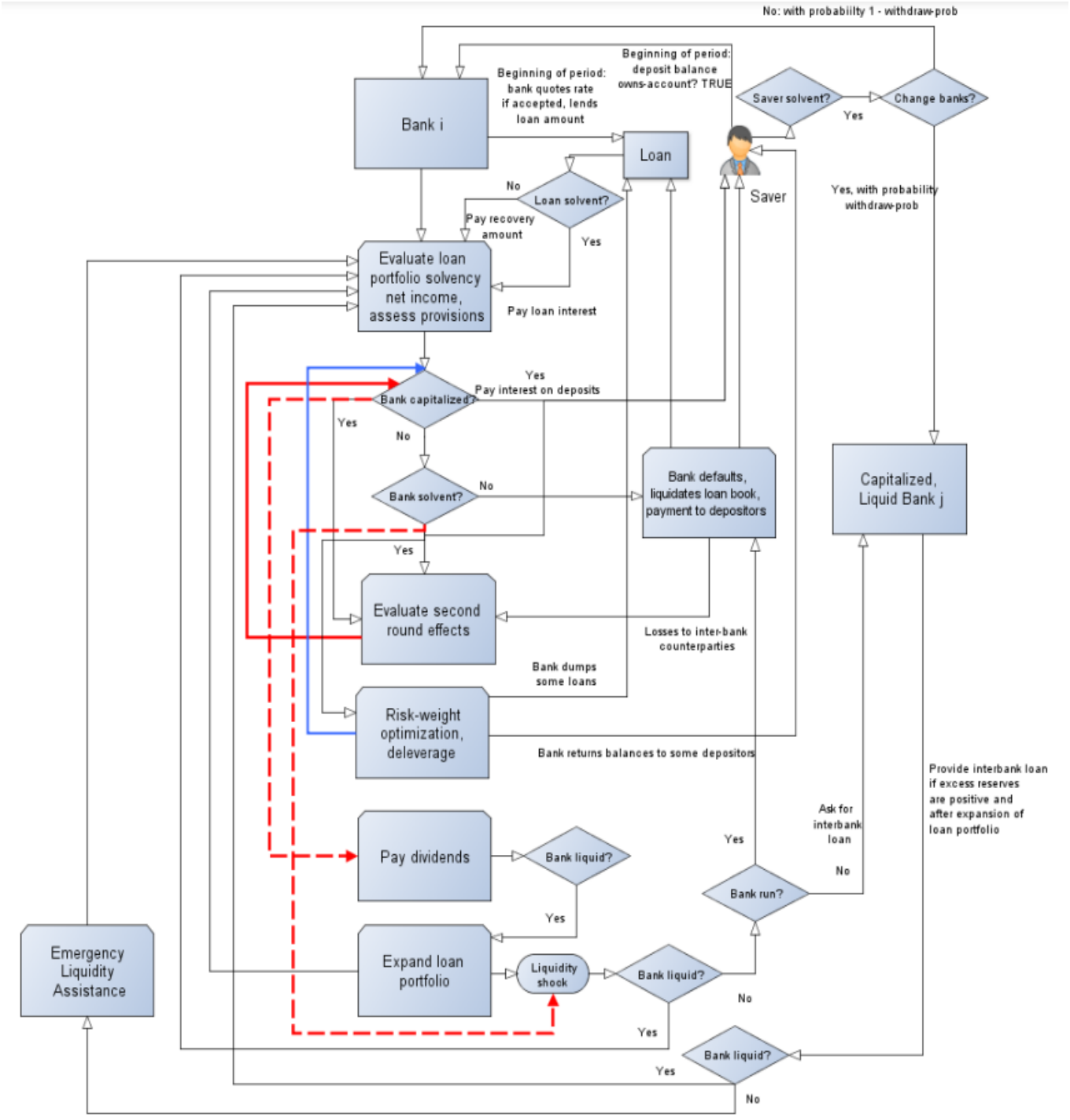


Рисунок 2.1 — Дії Банку та взаємодія з іншими агентами

За допомогою цього рисунку ми можемо чітко бачити усі процеси, які проходять в банку, від найменших, до найбільших, і почати розробляти систему захисту [9].

Система управління інформаційної безпеки банку — це набір основних інструментів і процесів, які дозволяють банкам та їхнім кредитним установам виконувати усі свої функції. Компоненти цієї СУІБ банку можуть відрізнятися залежно від банку, проте загалом система включає у себе базову банківську систему для керування основними транзакціями, кредитами, іпотекою та платежами, доступними через банкомати, мобільний банкінг і працюючі відділення. Іншими компонентами, які можуть бути включені, є системи CRM, системи управління ризиками, системи управління людськими ресурсами та системи бізнес-аналітики. CRM (Customer Relationship Management) — управління взаємовідносинами з клієнтами — це технологія для управління всіма відносинами та взаємодією вашої компанії з клієнтами та потенційними клієнтами.

Вимоги до СУІБ банку забезпечують повний опис поведінки системи та ґрунтуються на очікуваннях бізнесу. Функціонування системи має відповідати законам і нормативним актам країни.

Ключові вимоги, які має запропонувати СУІБ банку, можна класифікувати на функціональні та нефункціональні вимоги.

Функціональні вимоги описують послуги, які має пропонувати система управління банківською діяльністю, вони підрозділяються на три рівні доступу: режим адміністратора, режим касира (працівника) та режим клієнта:

— Клієнт:
  – Можливість увійти під логіном і паролем
  – Змога оновлення особистих даних у кабінеті
  – Можливість змінити пароль
  – Доступ до перегляду балансу на рахунку
  – Можливість перегляду особистої історії проведених транзакцій
  – Можливість переказувати гроші

– Змога відмінити ту чи іншу транзакцію

– Можливість подачі готівки

— Касир:

– Можливість увійти під логіном і паролем

– Можливість змінити пароль

– Дозвіл на реєстрацію нових клієнтів банку

– Можливість перегляданння інформації про клієнта

– Змога керування рахунками клієнтів

— Адміністратор:

– Можливість увійти під логіном і паролем

– Можливість перегляду інформації про касирів (працівників) та клієнтів

– Додавання або оновлення реквізитів відділення банку

– Додавання або оновлення даних касирів (працівників)

Пандемія надихнула користувачів досліджувати цифрові гаманці для здійснення платежів. Це варіант безконтактного мобільного банкінгу, який дозволяє завершити транзакцію практично з будь-якого пристрою iOS або Android. Він також пропонує компаніям персоналізований клієнтський досвід без дорогих і трудомістких розробок. На рисунку 2.2 зображена схема того, якими функціональними вимогами має володіти система управління банківською діяльністю.

Згідно з дослідженнями ринку, приблизно 4 мільярди людей використовуватимуть цифрові гаманці для оплати рахунків до 2024 року. Це вказує на те, що тенденції цифрового банкінгу необхідні установам, які хочуть виділитися.

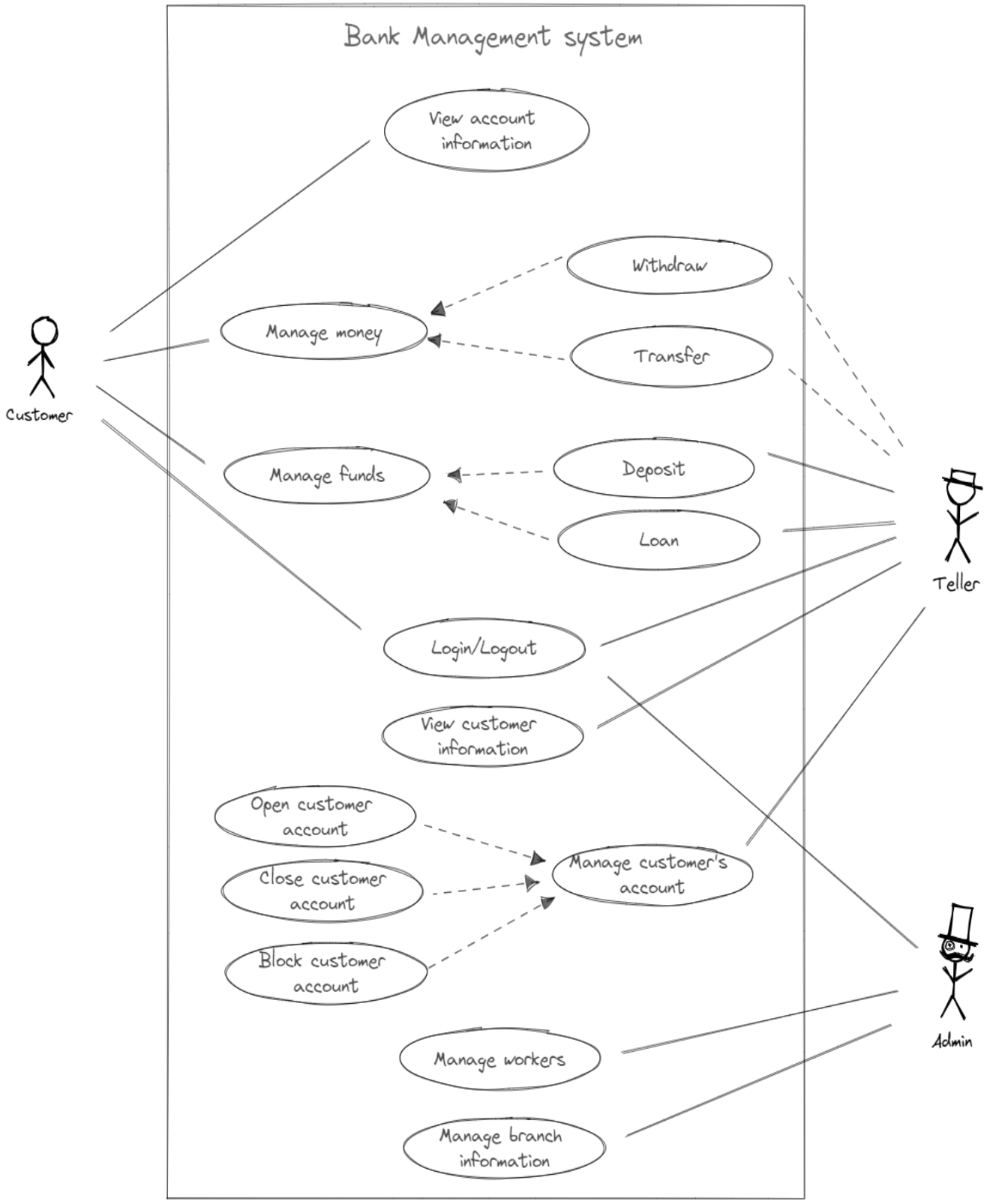


Рисунок 2.2 — Використання основних можливостей у СУІБ банку

Нефункціональні вимоги визначають критерії, за якими можна судити про роботу системи в цілому, а не про конкретну поведінку. Вони описують нові властивості, такі як безпека, продуктивність і доступність, і, на відміну від

функціональних вимог, які можна обійти, є важливими для виконання для придатної до використання системи. Оцінка того, чи відповідає продукт нефункціональній вимозі, зазвичай зводиться до логічної відповіді: так чи ні.

Для системи управління банком найважливіші нефункціональні вимоги включають безпеку, продуктивність, зручність використання та доступність.

Системи управління банками сумно відомі тим, що піддаються зловмисним атакам, тому безпека є головною вимогою до системи. Несанкціонований доступ до даних неприпустимий. Дані повинні щодня створюватися резервні копії та зберігатися в безпечному місці, на відстані від різних об’єктів системи.

Онлайн-транзакції та збережені цифрові файли мають бути зашифровані відповідно до 128-бітних або 256-бітних стандартів шифрування AES. Система також повинна використовувати програмне забезпечення брандмауера для захисту від мережевих атак.

Зі сторони клієнта система повинна забезпечувати автоматичний вихід із системи після періоду бездіяльності, приймати лише надійні паролі, які мають достатню довжину та неалфавітні символи, і блокувати спроби входу після кількох невдалих спроб.

СУІБ банку — це багатоклієнтська система, яка повинна досягати цільових показників часу відповіді для кожного з клієнтів під час одночасних дзвінків і повинна мати можливість виконувати цільову кількість транзакцій за секунду без збоїв. Система повинна ефективно використовувати апаратне забезпечення та енергетичні ресурси, щоб мінімізувати експлуатаційні витрати.

Система повинна забезпечувати різні графічні інтерфейси для клієнтів, касирів та адміністраторів. Усі інтерфейси системи мають бути зручними та простими для вивчення, включаючи допоміжні підказки та повідомлення та інтуїтивно зрозумілий робочий процес, особливо в інтерфейсі клієнта: клієнт повинен мати можливість швидко освоїти та використовувати інтерфейс без попереднього знання банківської термінології чи правил.

Інтерфейси повинні автоматично підлаштовуватися під пристрої з різними розмірами екрану та дозволяти змінювати розмір гарнітури та колірну схему для покращення читабельності.

Система повинна бути доступна в робочий час банку. Мобільний банкінг і банкомат мають бути доступними цілодобово з мінімальними витратами на обслуговування, досягаючи 99,999% часу доступності на рік.

Специфікація вимог до програмного забезпечення (SRS) - це опис програмної системи, яка буде розроблена, вона складається на останньому етапі аналізу, після функціональних і нефункціональних вимог. Набір інструментів і технологій програмування, які можуть бути застосовані до системи управління банком, залежить від того, чи використовується локальна, хмарна або гібридна модель обчислень.

Більшість великих фінансових інститутів мають свою основну банківську систему, яка працює на місці, що може бути забезпечено вимогою правової системи щодо полегшення серверів, які зберігають персональні дані на території країни.

Розробка системи базується на наступних технологіях:

— Сервери під керуванням ОС Windows Server/Linux, банкомат під управлінням Windows 10.

— Для серверної частини потрібна масштабована мова програмування, що підтримує багатопотоковість, наприклад Java, і Python потрібен для механізму аналізу даних і виявлення шахрайства.

— Сучасні зовнішні фреймворки, такі як React/AngularVue/jQuery для інтерфейсу користувача.

— Реляційна СУБД із механізмом, який підтримує транзакції ACID, як-от Microsoft SQL Server або Oracle RDBMS.

Після аналізу та узгодження вимог наступним етапом є опис архітектури системи на високому рівні.

Традиційним способом впровадження систем управління банком є монолітна архітектура, де різними завданнями керується єдиний уніфікований блок. Балансувальник навантаження рівномірно розподіляє завдання між серверами додатків, які запускають кілька копій додатка, а з іншого боку додаток керує запитами до бази даних. Балансувальник навантаження також виконує роль

внутрішнього брандмауера на додаток до зовнішнього брандмауера, який забезпечує захист першого рівня від мережевих атак.

Архітектура проста, тому її легко розробити та розгорнути, масштабування також відносно просте за допомогою балансувальників навантаження – ми можемо просто додати інший сервер додатків/баз даних, коли це необхідно [10].

Коли справа доходить до впровадження та підтримки основних банківських систем, то на думку приходять дві класичні архітектури, які конкурують одна з одною різними способами: моноліт проти мікросервісу(керована подіями), більш надійна проти більш гнучкої.

Монолітна архітектура — це традиційна модель програмного забезпечення, яка побудована як уніфікована одиниця, самодостатня та незалежна від інших програм. Слово «моноліт» часто приписують чомусь великому та льодовиковому, що не далеко від істини монолітної архітектури для розробки програмного забезпечення. Монолітна архітектура — це окрема велика обчислювальна мережа з єдиною кодовою базою, яка об’єднує всі бізнес-завдання. Щоб внести зміни в програму такого типу, потрібно оновити весь стек, отримавши доступ до бази коду та створивши та розгорнувши оновлену версію інтерфейсу служби. Це робить оновлення обмежувальними та забирає багато часу.

Моноліти можуть бути зручними на ранніх стадіях життя проекту для полегшення керування кодом, когнітивних витрат і розгортання. Це дозволяє звільнити все в моноліті одночасно.

Монолітні архітектури охоплюють усі основні банківські послуги в єдиному, повністю інтегрованому програмному забезпеченні. Важливо, що не потрібно розробляти інтерфейси між службами, оскільки, наприклад, такі речі, як платіжний додаток і додаток для збереження позицій, є частинами одного IT-рішення. А оскільки об’єктна модель узгоджується з усіма компонентами, немає потреби інвестувати в складне відображення між різними областями.

Вибір єдиного програмного забезпечення для виконання всіх функцій банку забезпечує привілейовані відносини з його постачальником, покращуючи їх підтримку. Таким чином, уся платформа є набагато міцнішою та стійкішою до одноточкової відмови, особливо під час оновлення.

Впровадження єдиного програмного забезпечення з відносно стандартною конфігурацією також відкриває двері до рішень програмного забезпечення як послуги (Software as a Service — SaaS). Дійсно, постачальники банківського програмного забезпечення SaaS майже напевно матимуть стандартну пропозицію з обмеженою кількістю готових розширень. Як правило, використання SaaS дозволяє істотно заощадити кошти на технічне обслуговування та оновлення, і навіть може забезпечити повний аутсорсинг бек-офісу, зберігаючи економічний бізнес і зосереджуючись на таких важливих сферах, як управління клієнтами. На рисунку 2.3 зображено спрощений алгоритм роботи монолітної системи банку.

Моноліти протягом тривалого часу були основною банківською системою, яку вибирали існуючі банки.

У монолітній архітектурі всі різні банківські компоненти об’єднані в одну окрему програму.

Це може здатися зручним, і в певному сенсі це так. З монолітною системою початкова розробка програмного забезпечення, тестування та розгортання відносно прості.

Однак моноліти також мають свої недоліки. Одним із найбільших недоліків є те, що вони не створені для конфігурації, що робить системи громіздкими та їх важко адаптувати до потреб вашого бізнесу та клієнтів у міру їх росту та розвитку.

Це означає, що будь-які оновлення вимагають кожного разу перерозгортання всієї системи. Це коштує вашому бізнесу часу та грошей, і якщо виникне така проблема, як вірус чи помилка, це може призвести до зупинки всієї системи, доки її не буде вирішено.

І останнє, але не менш важливе – це, мабуть, найбільша проблема з монолітними системами: вони просто не будуються з урахуванням майбутнього банківської справи. Оскільки нові технології продовжують революціонізувати банківський сектор, відсутність у моноліту можливостей інтеграції означає, що він завжди відставатиме від більш гнучких і конфігурованих рішень, доступних зараз на ринку.

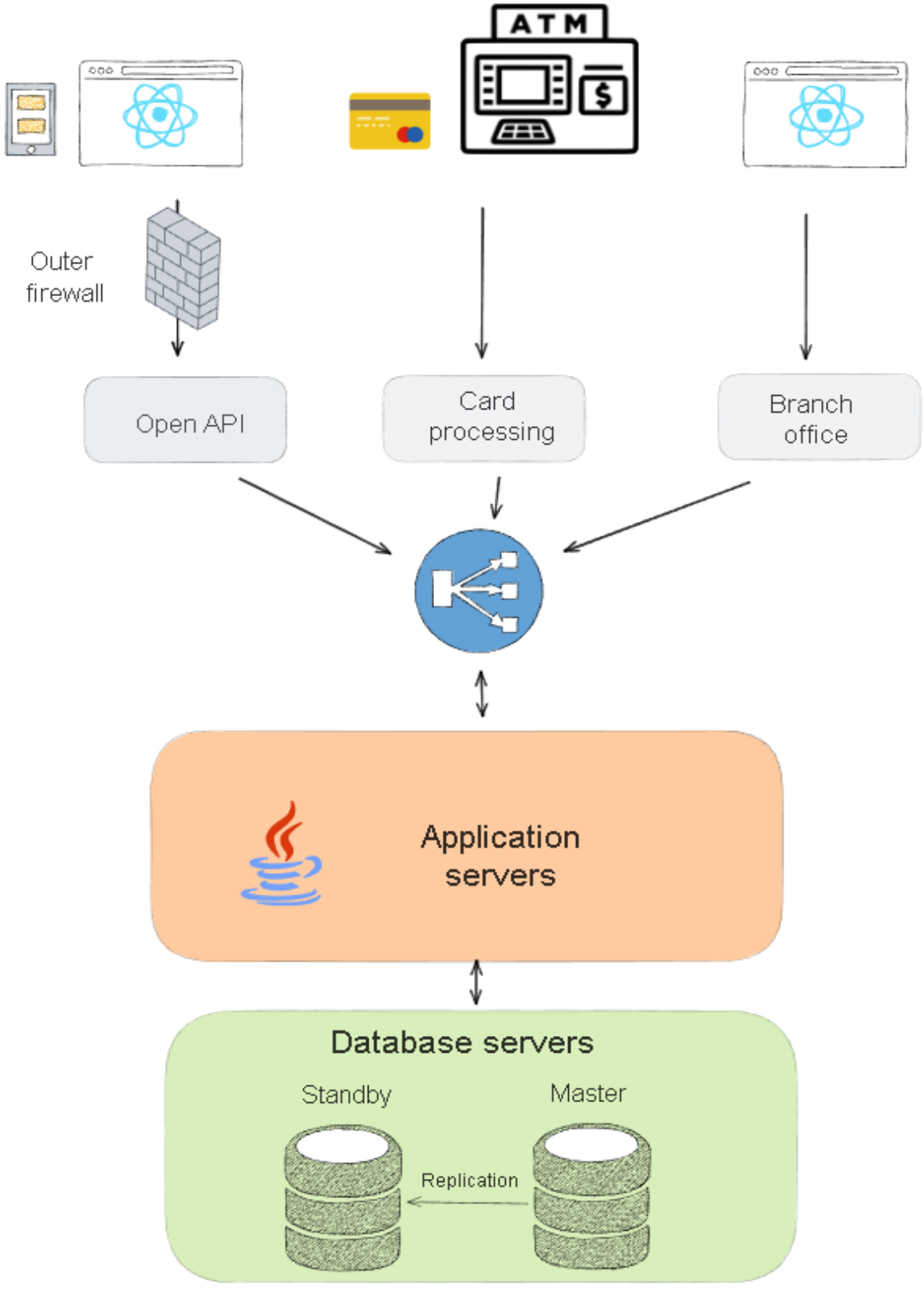


Рисунок 2.3 — Монолітна архітектура СУІБ банку

Як показано на рисунку вище, Java виконує різноманітні завдання, які надходять від філій, від обробки електронних карток до запитів до API, відкритого для інших банків і клієнтів.

Монолітну архітектуру найлегше реалізувати, але її важко підтримувати в довгостроковій перспективі, і дуже важко додавати нові функції або оновлювати старі. Крім того, з монолітною архітектурою важко вводити нові інструменти та фреймворки в стек, що розробляється, оскільки всередині монолітної структури немає точок для підключення нових технологій.

Архітектура, керована подіями, або її ще називають мікросервіс, є однією з альтернатив традиційній монолітній архітектурі, яка зосереджена навколо «подій», а не сутностей. Наприклад, події, коли офісний касир додає нового клієнта, коли клієнт натискає кнопку банкомату, щоб зняти гроші, або коли баланс рахунку стає нижчим за порогову суму. Усі вхідні події реєструються на рівні API та додаються до потоку Kafka.

Apache Kafka, розподілена платформа потокового передавання подій із відкритим вихідним кодом, розподіляє події між споживачами: завдання додатків, зберігання даних, збирачі статистики, процедури сповіщень і спеціальний механізм перевірки шахрайства. Перевірка шахрайства написана на Python для автоматичного виявлення та блокування підозрілих транзакцій, щоб запобігти відмиванню грошей та іншим порушенням.

Порівняно з монолітними архітектурами, програми мікросервісу порівняно неважкі в опануванні, з ними легко впоратися. Наприклад, є такий вираз, що безпека у кількості. Якщо один елемент виходить з ладу, команда може запровадити іншу послугу без необхідності змінювати всю архітектуру, що забезпечує швидшу доставку. Масштабувати, щоб задовольнити потреби певного елемента, також легше з невеликими компонентами. А оскільки програма може працювати незалежно під час внесення змін, можна впроваджувати швидкі та контрольовані оновлення без уповільнення або зупинки інших компонентів. Крім того, оскільки архітектура мікросервісів є більш гнучкою, команда може використовувати будь-яку мову чи структуру, яка підходить для роботи, що дозволяє їм виконувати такі завдання, як налаштування серверів, не перериваючи спілкування між службами.

Архітектури мікросервісів забезпечують таку необхідну гнучкість у секторі, відомому своєю відносною інертністю та стійкістю до змін. Невеликі команди

щодня розробляють нові цільові програми. А вибір правильної реалізації архітектури забезпечить швидку реакцію вашої основної банківської системи на зміни в нормативних актах, передових практиках і потребах клієнтів.

Будь-яку нову фінтех-програму з новим підходом до бізнесу можна швидко інтегрувати, забезпечуючи синергетичний розвиток і експлуатацію. Архітектури мікросервісів також сприяють дослідженню ринкових ніш, завдяки чому можна швидко, легко та доступно інтегрувати одноцільове програмне забезпечення, яке можна націлити на певні домени. На рисунку 2.4 зображено спрощений алгоритм роботи архітектури, керованою подіями.

В основному архітектура, керована подіями, використовує події для запуску та обміну даними між роз'єднаними службами. Це спосіб обміну та обміну даними через події. Подія — це зміна стану або оновлення, як-от списання коштів із поточного рахунку клієнта. Подія може ініціювати низку дій, як-от перевірка нової адреси клієнта або авторизація дебетової плати за п'ятидесяти гривневий латте з молоком.

Використання подій для обміну змінами в даних означає, що ви можете уникнути уповільнення роботи спільної бази даних, легко об'єднати дані та використовувати систему push, а не pull, щоб інформація, яка вам потрібна з даних, надходила до вас, коли вона вам потрібна.

Коли ви створюєте архітектуру потокової передачі подій для фінансових послуг, потрібно знати кілька важливих будівельних блоків.

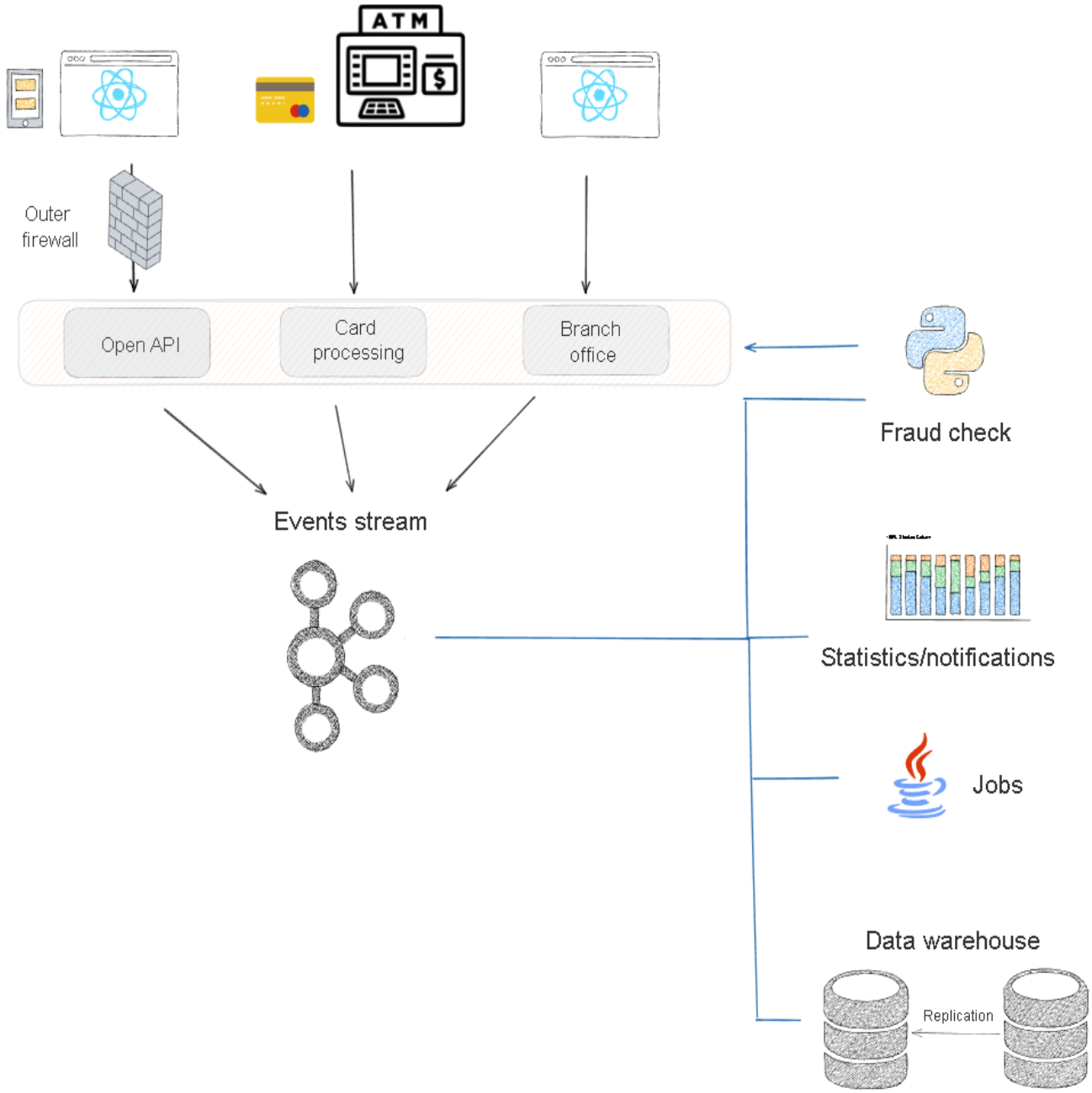


Рисунок 2.4 — Архітектура, керована подіями, СУІБ банку

Коли йде процес створення архітектуру потокової передачі подій для фінансових послуг, потрібно знати кілька важливих будівельних блоків.

— Сповіщення про події. Вони вказують на те, що, по суті, щось сталося. Це може бути, наприклад, нова адреса клієнта, яка потім ініціює подальші дії в програмі.

— Передача стану за допомогою події. Часто сповіщення про подію супроводжується сповіщенням про стан, яке містить відомості про фактичну

подію. У разі зміни адреси клієнта, наприклад, це міститиме фактичну адресу, на відміну від сповіщення про подію.

— Джерела подій. Це приносить повну історію змін стану. Наприклад, баланс рахунку – це низка депозитів і зняттів; щоб отримати доступ до поточного стану облікового запису, потрібно прочитати всі ці події — зміни стану, наприклад зміни адреси чи імені. Це важливо для запуску аналітики даних.

— Розподіл відповідальності за командні запити (CQRS). За допомогою шаблону CQRS ви створюєте окремий шлях для читання (команд) і запису (запитів) — асинхронний спосіб запису даних і отримання відповіді. Щоб зробити покупку, наприклад, команда або читання використовує дебетову картку, щоб купити каву. Для цього програма має пройти етапи перевірки балансу рахунку. За допомогою CQRS програма може слухати обидва канали, читання та запис, і чекати відповіді з тегами про те, що передача в порядку. Це потужний шаблон для використання та повторного використання у фінансових послугах.

Обидва підходи можуть бути узгоджені в ефективній банківській системі. Основні банківські дані та бек-офісні завдання можна інтегрувати в монолітну систему. Тоді дані можуть бути надані декільком мікросервісам, які виконують найсучасніші завдання. Один може займатися аналізом ризиків та оптимізацією портфеля, а інший піклуватися про електронний банкінг.

Оскільки архітектура, керована подіями, вимагає ретельного проектування на початкових етапах і, отже, потребує більше часу та ресурсів, витрачених на розробку, це хороший варіант для великих фінансових установ, які націлені на велику клієнтську аудиторію та надають низку різноманітних послуг.

Для нашої СУІБ ми виберемо архітектуру, яка керована подіями, аби мати у подальшому змогу швидко та без проблем впровадити нові зміни у системі, не порушуючи цілісність усієї системи.

Зв’язок між службами також є частиною платформи потокової передачі даних за допомогою команд, подій і запитів.

2.2 Поведінкова модель рішень СУІБ

Моя модель СУІБ буде працювати на основі циклу PDCA (Plan-Do-Check-Act). Цикл PDCA може допомогти відрізнити компанію від її конкурентів, особливо в сучасному корпоративному світі, де підприємства постійно шукають способи оптимізувати свої процеси, зменшити витрати, збільшити прибуток і підвищити рівень задоволеності клієнтів [11].

Багато менеджерів несвідомо застосовують цикл PDCA, щоб допомогти покращити систему захисту своєї організації, оскільки він охоплює основні принципи стратегічного планування. Чотири компоненти циклу PDCA є:

— Plan — чітко визначений план проекту забезпечує основу для майбутніх операцій. Важливо, щоб він відображав завдання та цінності організації. У ньому також має бути відображено цілі проекту та чітко вказано найкращий спосіб їх досягнення.

— Do — це крок, на якому план запускається. План був складений недаремно, тому працівникам важливо виконати його, як зазначено. Цей етап можна розбити на три підсегменти, включаючи навчання всього персоналу, задіяного в проєкті, фактичний процес виконання роботи та запис ідей або даних для майбутньої оцінки.

— Check — зазвичай у проекті повинно бути дві перевірки. По-перше, перевірки разом із реалізацією забезпечують досягнення цілей проекту. По-друге, більш повний аналіз проекту, який виконується після його завершення, розглядає успіхи та невдачі, щоб можна було внести коригування в майбутньому.

— Act — останнім кроком є вжиття коригувальних дій після виявлення та усунення попередніх помилок. Цикл PDCA повторюється і може бути перевизначений, можливо, для отримання кращих результатів згідно з новими рекомендаціями [12].

На рисунку 2.5 можна побачити цикл дії PDCA у системі.

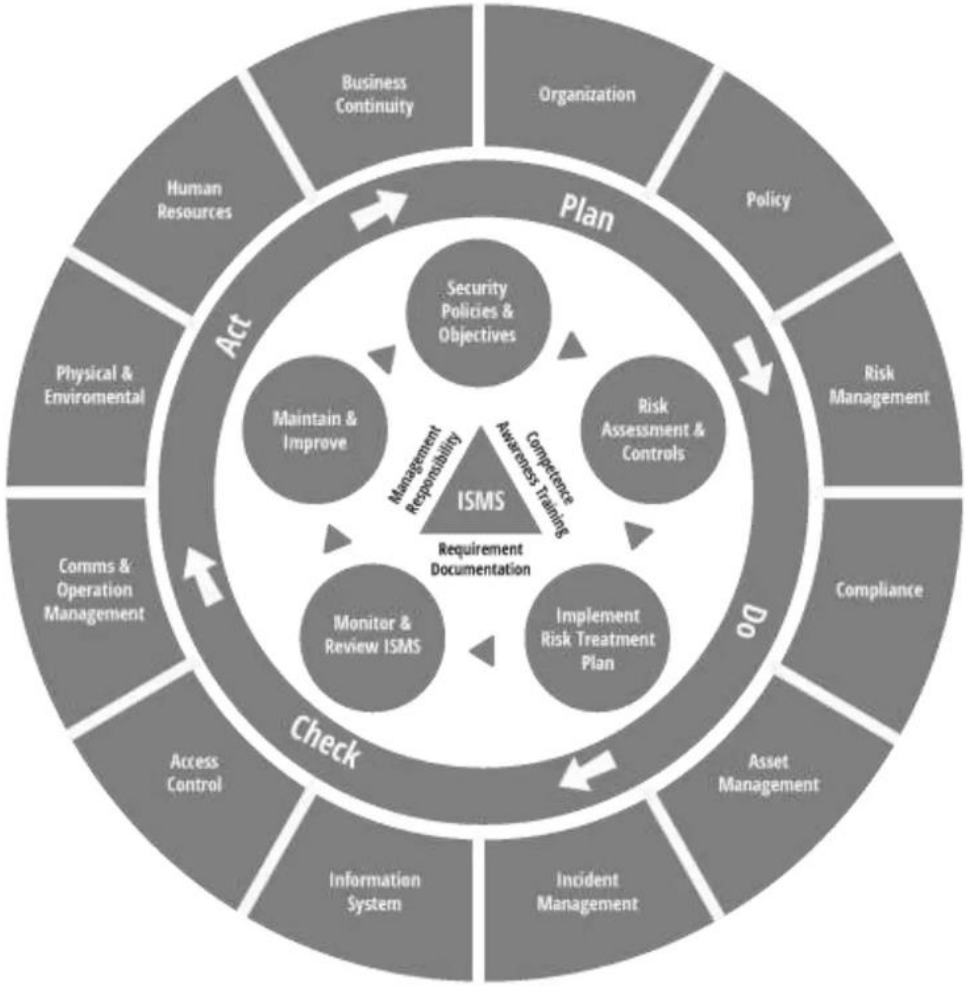


Рисунок 2.5 — Алгоритм дії циклу захисту

Проте лише одного алгоритму мало, для того щоб захистити настільки велику сітку інформації, яка є у банковій системі. Для покращення СУІБ нам потрібно також впровадити додатковий захист через програмне забезпечення (ПЗ).

PinCat — це уніфіковане рішення для керування загрозами, яке об’єднує численні функції безпеки на одній платформі для захисту вашої мережі, Інтернету, електронної пошти, програм і користувачів від розширених постійних загроз, атак DoS/DDoS, вірусів, шпигунського програмного забезпечення, програм-вимагачів і спаму.

Переваги PinCat є наступними:

— Захист від DDoS атак, які навантажують систему до 50 Гігабайтів на секунду

— Містить у собі наступне покоління фаєрволу

— Запобігає втраті даних

— Запобігає можливому просуненню програм-вимагачів

— Містить розширений захист проти спаму [13].

Для кращого розуміння, як саме діє PinCat на рисунку 2.6 є схема того, як діє це програмне забезпечення.

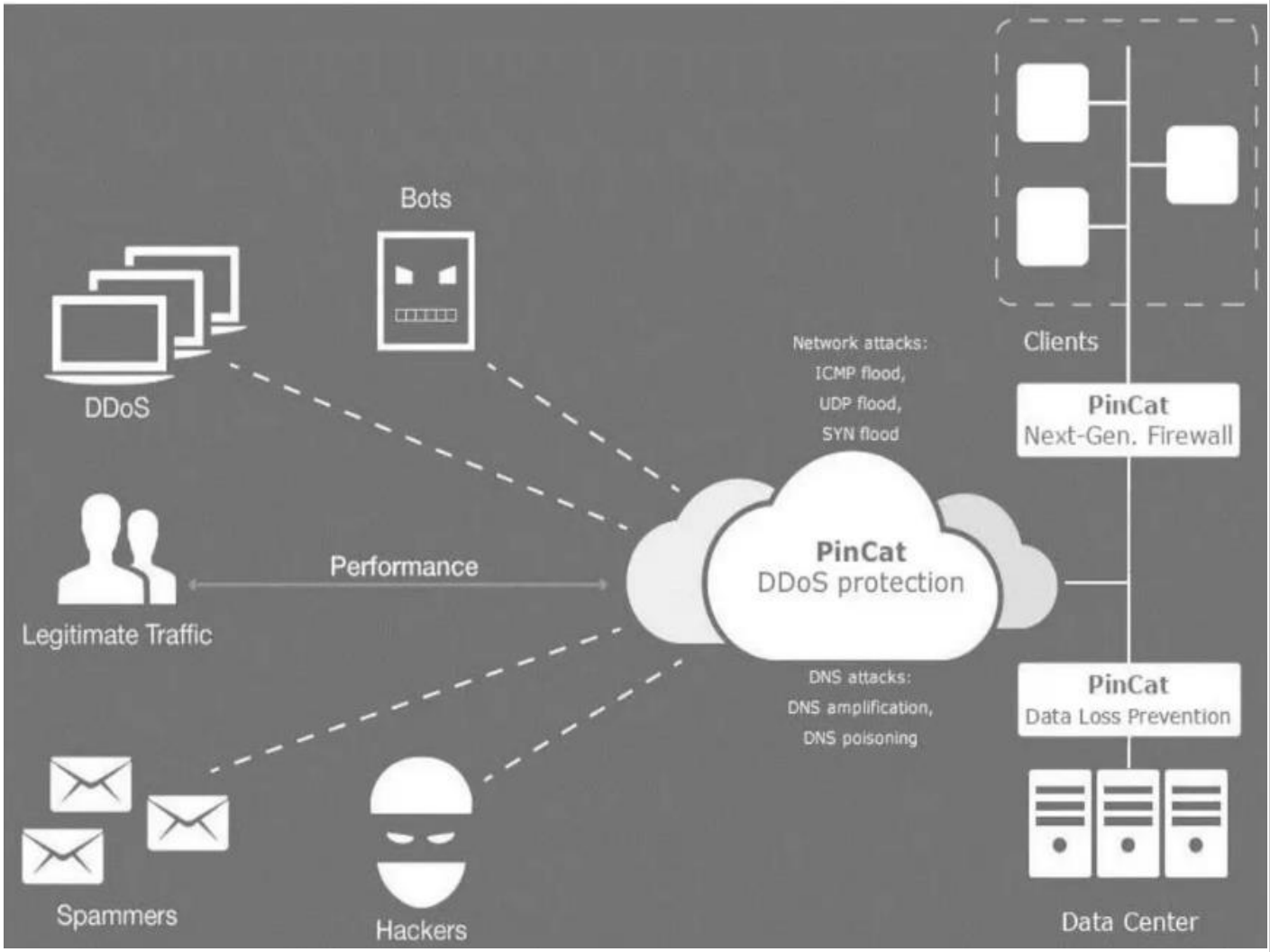


Рисунок 2.6 — Схема дії PinCat

Оскільки основою загрозою для СУІБ банківської системи є атаки типу DDoS, з метою перенавантаження мережі, то це програмне забезпечення зможе допомогти. Всі запити надходять до хмарного середовища, де сортуються за ступенем довіри, тобто перевіряється, чи трафік надходить саме від клієнтів, чи він генерується за допомогою спеціально запрограмованих ботів, спамерів, чи

хакерів, що намагаються проникнути в систему. Після того, як пройшла перевірка у хмарному середовищі, трафік надходить до фаєрволу, де перевіряється ще раз на предмет загроз, які система не виявила з першого разу, і тільки після цього запит доходить до клієнтів. В дата центрі ж зберігаються бек-апи, тобто резервні копії всіх даних на випадок пошкодження основного джерела збереження інформації.

Проте захист лише від перенавантаження системи був би неповний. Потрібно також впровадити алгоритм, який би почав нейтралізовувати загрозу в моменті її винекнення, і для цього нам потрібен ще один додаток. FireEye — платформа запобігання загрозам FireEye надає динамічний захист у реальному часі без використання сигнатур, для захисту організації навколо основного вектору загроз і різних стадій «життя» циклу атаки. За допомогою цієї системи ми можемо:

— Залишатися на крок попереду від усіх потенційних загроз, які можуть становити загрозу для банківської системи

— Ідентифікувати та блокувати невідомі кібер-загрози, які не були помічені традиційними методами захисту інформації у системах банківських транзакцій

— Запобігання потенційній крадіжці або ж спотворенню критично важливої інформації щодо проведення операцій та функціонування системи загалом [14].

Краще зрозуміти обсяг роботи, яку буде покривати FireEye допоможе зрозуміти рисунок 2.7.

Програмне забезпечення FireEye має можливість ідентифікувати, аналізувати та блокувати атаки, які надходять з мобільних телефонів. Це є дуже важливим у сучасному світі, адже з поширенням інтернет-банкінгу, кожен банк має додаток для смартфонів, аби облегшити клієнтам доступ до транзакцій.

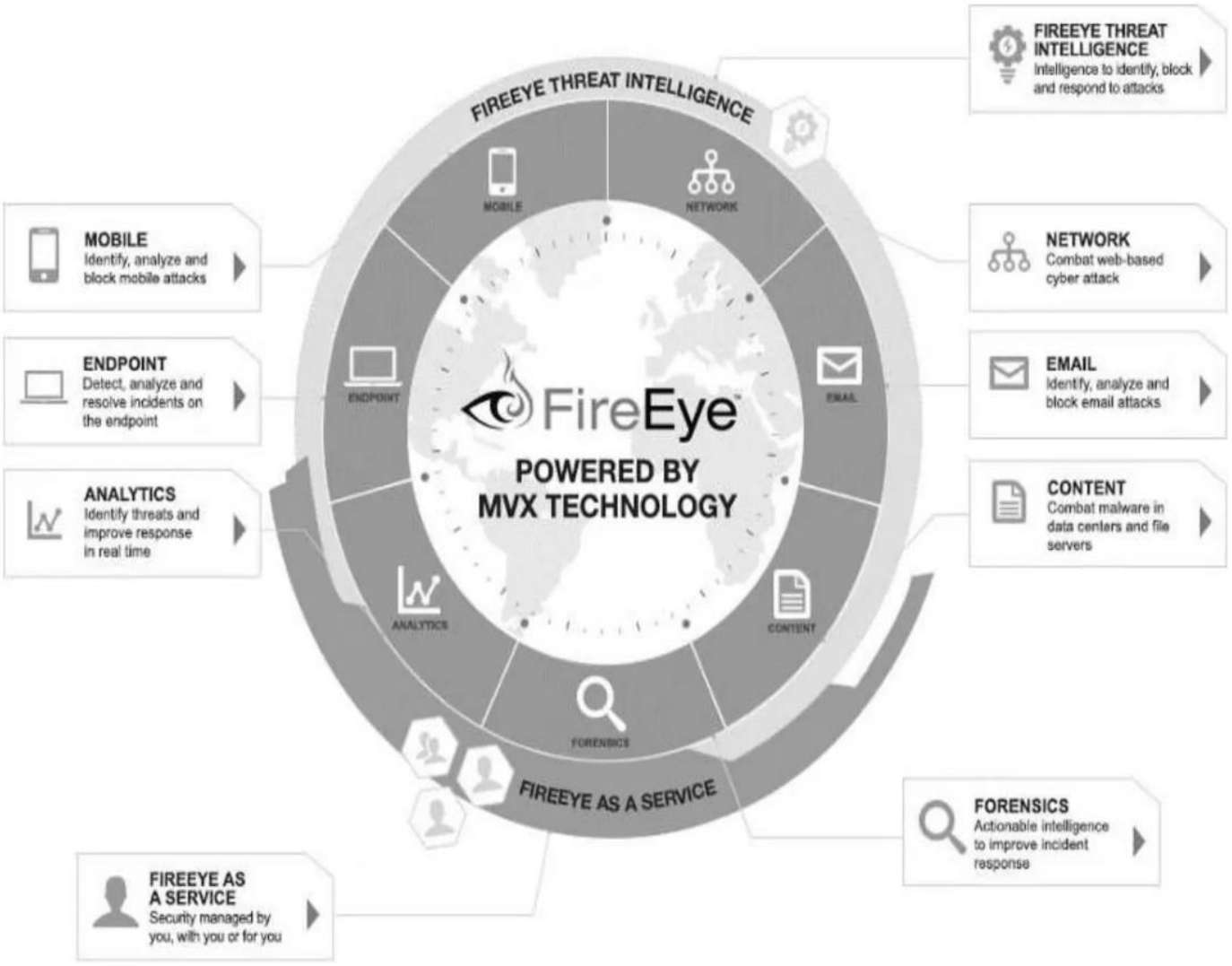


Рисунок 2.7 — Схема дії FireEye

Але смартфони набагато легше взломати, аніж комп’ютери чи ноутбуки, тому і потенційна загроза від них трохи вища. Якщо ж від телефону, чи ноутбуку, чи комп’ютеру надходить якийсь підозрілий трафік, то він блокується програмним забезпеченням і не пропускається далі по мережі, те ж саме відбувається і з підозрілими листами на електронну пошту. Крім цього програмне забезпечення може в режимі реального часу ідентифікувати загрозу та з кожним разом покращувати реакцію на неї, тобто, чим частіше однотипна атака здійснюється, тим швидше і якісніше на неї реагує система. Сам трафік і дані

також перевіряються системою у файлових серверах на предмет підозрілого вмісту, який може бути там прихований.

На випадок, якщо ж у нас попередні два ПЗ не зможуть впоратися із захистом, адже вони будуть направлені на більш вузькі спеціалізації, то потрібно взяти ще одне ПЗ, яке б виконувало більш важливу роль у нашій СУІБ банківської системи. Trend Micro — це скоординований захист від загроз, який є новим підходом до безпеки у сфері банкінгу, та який допомагає вирішити цю ситуацію. Він базується на традиційній тактиці, тобто покладається на комплексні контрзаходи на рівні домену, підкреслюючи додаткову потребу в:

— Широкій багатосторонній інтеграція між компонентами рівня домену та керування

— Всеохоплюючому аналізі, кореляції та візуалізації даних безпеки між доменами

— Додатковій глобальній розвідці про загрози

— Інтелектуальній координації та автоматизації основних можливостей реагування на загрози [15]

Схему роботи Trend Micro краще всього видно на рисунку 2.9.

Тобто, це програмне забезпечення працює більш на рівні доменів, захищаючи сервери, офісні комп’ютери, систему передачі даних всередині банку, а не тільки між клієнтами, а також забезпечує додаткове шифрування даних на серверах, для захищеності системи. Оскільки у нас перше програмне забезпечення, PinCat, працює через хмарне середовище, то Trend Micro покращить цей захист, адже він забезпечує захист гібридних та мультгібридних хмарних середовищ, а також хмарних додактів, у яких зберігається інформація.

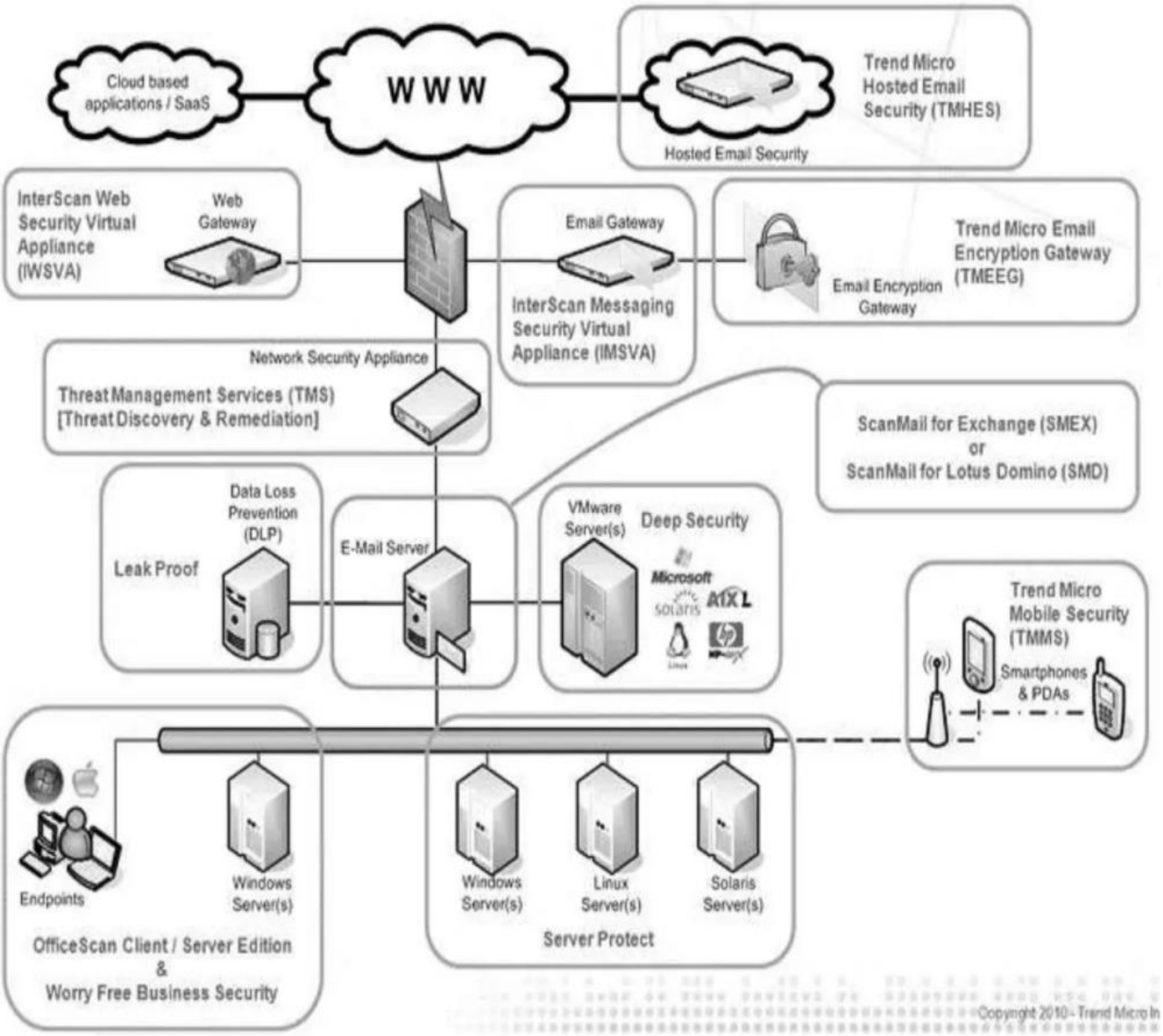


Рисунок 2.8 — Схема роботи Trend Micro

Саме через це, на мою думку, вони будуть мати гарну синергію, тобто, гарно взаємодіяти один з одним. Щодо взаємодії FireEye та Trend Micro, то тут можна вказати на перевагу того, що ці два ПЗ проводять аналіз трафіку постійно, і якщо одна система щось може пропустити повз, то друга вже підхопить. У системи інтернет банкінгу багато захисту не буває і потрібно бути дуже і дуже обережними, щоб не втратити важливих даних.

Останнім програмним забезпеченням, який дійсно зв’яже між собою нашу систему управління інформаційною безпекою, буде MaxPatrol. MaxPatrol дає неупереджену картину стану захисту на рівні системи, відділу, вузла та програми.

Пентестування, аудит і перевірка відповідності в поєднанні з підтримкою різноманітних операційних систем, баз даних і веб-додатків роблять MaxPatrol є ідеальним вибором для аудиту безпеки в режимі реального часу, постійно, на всіх рівнях корпоративної інформаційної системи. Це програмне забезпечення має такі переваги:

— Рішення «все в одному» забезпечує незмінні результати

— Багаторівневе звітування розповідає всю історію

— Попередні налаштування полегшують відповідність

На рисунку 2.9 зображено детальніше схему роботи MaxPatrol у системі управління інформаційною безпекою.

MaxPatrol забезпечить нам аудит безпеки системи. Для чого він нам потрібен? Із наведених вище особливостей організації системи захисту у банківських системах із розділу 1, я навела декілька найбільших загроз, однією з яких була загроза із середини банку. Тобто, навмисна людська шкода. Недобросовісний працівник, або ж підкуплений працівник, із певними правами доступу, може всю доступну йому інформацію «злити» у відкритий доступ.

Ця інформації може містити номери карток клієнтів банку, їхні ініціали, номери телефонів, дати виходу карток із обігу, та багато іншою конфіденційної інформації, яка може нашкодити не тільки втратою активів, а також зниженням рівня довіри до банку, а в результаті і зниження притоку нових клієнтів. Саме з цією проблемою нам допоможе аудит безпеки. Адміністратор безпеки буде бачити хто із авторизованих у системі працівників вносив правки до того чи іншого документу або ж частини інформації, коли заходив у систему і коли виходив.

Рисунок 2.9 — Схема роботи MaxPatrol

Також буде існувати звіт з безпеки, у якому будуть міститися усі ці записи. Це буде створене для того, аби у випадку того, що працівник захоче скачати всю базу даних і розповсюдити її у відкритому доступі, ці дії були задокументовані по годинам і хвилинам, з метою подальшого покарання, розмір якого буде залежати від втрат та шкоди, які були спричинені даним рухом і корелюватися від дисциплінарного зауваження до кримінальної відповідальності [16].

2.3 Висновки

Запропоновані мною рішення підвищать рівень захисту інформаційної системи банку, а також забезпечать список для внутрішнього аудиту безпеки, утворять стійку до зламів систему та дозволять реагувати на загрози в рази швидше. Кожна з цих програм діє по різному і покриває різні аспекти загроз. Проаналізувавши існуючі підходи та рішення я зробила висновок, що система управління інформаційною системою банку потребує комплексного рішення, а також переробки системи від монолітної архітектури до архітектури керованою подіями.

Багато проектів спочатку починаються як моноліт, а потім розвиваються в архітектуру мікросервісу. Оскільки до моноліту додаються нові функції, багато розробників, які працюють над єдиною кодовою базою, може стати громіздким. Конфлікти коду стають частішими, і ризик оновлень однієї функції вносить помилки в непов’язану функцію. Коли виникають ці небажані моделі, можливо, настав час розглянути можливість переходу на мікросервіси.

Проте, аби дізнатися точніше, чи ці рішення виправдають витрачених на них коштів, нам потрібно провести розрахунки ефективності прийнятих рішень, чому і буде присвячений третій розділ моєї роботи.

3 ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ СУІБ

3.1 Симуляція роботи СУІБ

У нас існувала до впровадження покращень до СУІБ загроза витоку інформації. Вона могла бути як зсередини компанії, через недобросовісних працівників, або ж їхній підкуп, через тих же працівників, проте випадково, по незнанню, або ж через самий недолік системи, наприклад, прогалину на сайті, якою можна скористатися, аби зайти з правами адміністратора, або ж працівника банку [17]. Для того, щоб виправити цю загрозу, ми впровадили два програмних засоби, які будуть діяти, як контрзаходи: FireEye і MaxPatrol. Перший програмний буде забезпечувати нам безпеку для сайтів та додатків на смартфонах, а другий програмний засіб, за допомогою реалізованого аудиту безпеки, дозволить нам переглянути, хто саме зробив шкоду із внутрішніх працівників, і яким чином їхні дії вплинули на систему. Впровадивши ці рішення для нашої СУІБ ми забезпечили безпеку таким активам як дані про установу (організація структури системи безпеки, дані про працівників, їхні посади, час роботи, обов'язки, філіали, дані про версію роботи сайтів, існуюче програмне забезпечення), дані про рахунки клієнтів (номери рахунків, кількість коштів, відкриті депозити та кредити, дані про діючи картки, наявність мобільних додатків, історію транзакцій, прив'язані номери телефонів, паспортні дані, ідентифікаційний код) та непрямий актив, такий як довіра клієнтів. Цей актив називається непрямим, тому що залежить від попередніх активів. Наприклад, якщо дані про клієнтів або ж про саму установу стануть відомими на загал, тобто будуть опубліковані у відкритому доступі, то рівень довіри клієнтів, як теперішніх, так і майбутніх, до цього банку знизиться, і банк втратить їх. Якщо банк втрачає клієнтів, то він втрачає потенційних вкладників, і прибуток банку зменшується, як результат, зменшується кількість грошей, які банк може видавати у якості кредиту, він починає працювати собі «в мінус», тобто витрати настільки великі, що не перекриваються прибутками, поки, в кінці-кінців, установчий фонд опустіє і банк оголосить себе банкротом, вкладники втратять свої вклади без можливості їх

повернути, а власники акцій не стануть володарями простих папірців. Звичайно ж, це не станеться за один вечір, тому що сучасні системи захисту інформації у банку комплексні і передбачають найгірші ситуації (саме тому ми ввели декілька програмних забезпечень, а не лише одне), проте ця загроза існує, теоретично, і від неї потрібно захистити системи [18].

Витік даних, який також називають малопомітною крадіжкою даних, передбачає несанкціоновану передачу електронних або фізичних даних від організації зовнішнім одержувачам або адресатам. Зловмисники часто збирають дані за допомогою облікових записів електронної пошти або Інтернету. Вони також можуть використовувати мобільні пристрої зберігання даних, такі як USB-ключі, ноутбуки та оптичні носії.

Витік даних може бути наслідком цілеспрямованих внутрішніх дій, спрямованих на нанесення шкоди організації, або як частина більшої схеми шахрайства з платежами. Це також може бути випадковим. Кіберзлочинці шукають різну інформацію у витоках даних, зокрема інформацію про клієнтів і комерційну таємницю. Обсяг і тип витоку визначає шкоду, яка була завдана організації [19].

На моделі загроз, на рисунку 3.1, детальніше зображено всі активи, загрози та запропоновані рішення на зменшення ризику виникнення сценарію загрози через певну вразливість.

Розголошення інформації про клієнтів може завдати шкоди як компанії, так і її клієнтам, завдати шкоди репутації та в багатьох випадках наражати компанію на порушення згоди та судові позови.

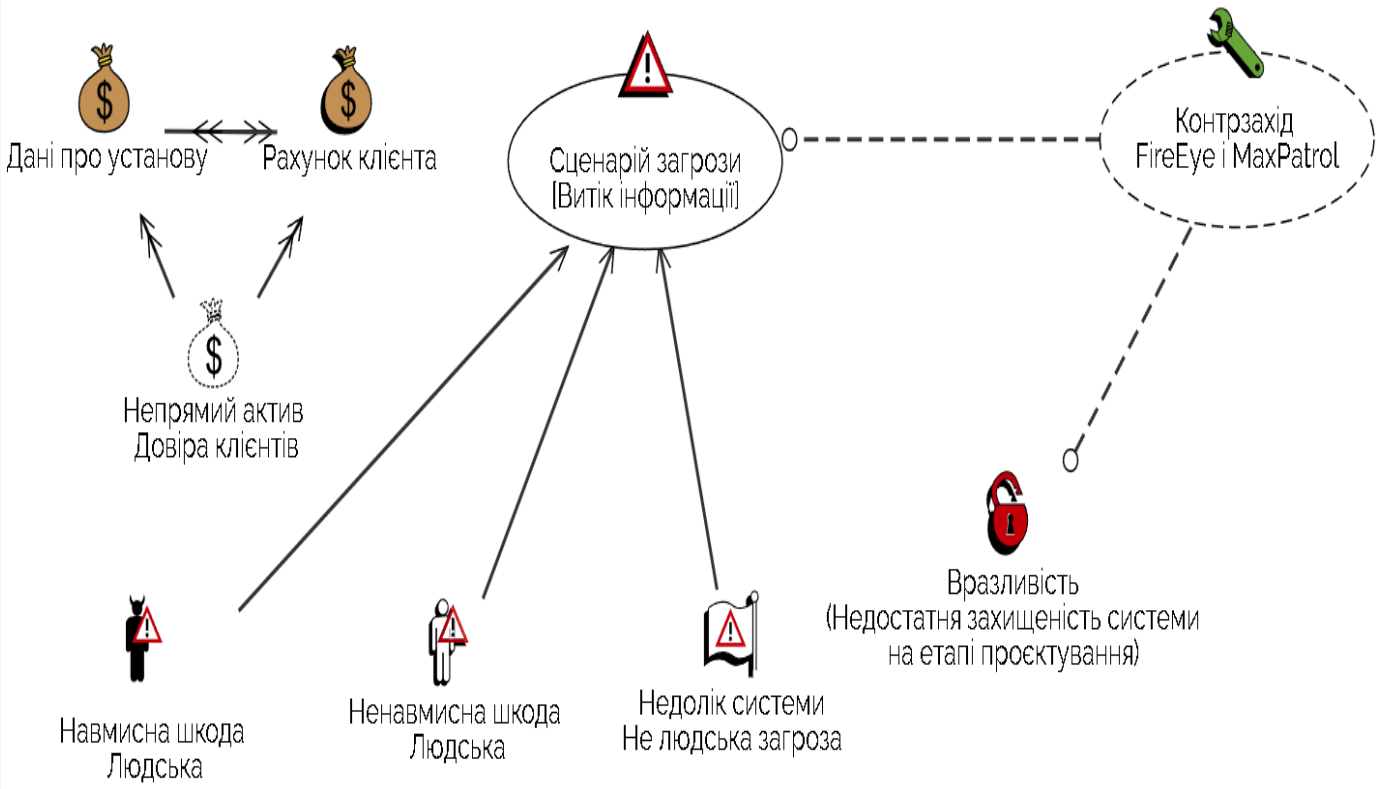


Рисунок 3.1 — Модель загрози витоку інформації у системі управління інформаційної безпеки банку

Далі у нас йде загроза фішингу, або ж соціальної інженерії. Фішинг є одним з поширених видів соціальної інженерії, який зазвичай здійснюється через електронну пошту, хоча також може використовуватись через телефонні дзвінки або повідомлення в соціальних мережах. У фішингових атаках зловмисники намагаються створити вигляд, що їхні листи або повідомлення походять від надійного джерела, такого як банк, компанія або сервіс, і просять отримати конфіденційну інформацію або виконати дії, які можуть вразити безпеку користувача. Це може включати введення паролів, номерів кредитних карток, соціального захисту або інших особистих даних. Соціальна інженерія в свою чергу є серйозною загрозою для інформаційної безпеки. Зловмисники, які використовують соціальну інженерію, ретельно планують свої атаки, використовуючи психологічні методи для маніпулювання людьми і отримання доступу до конфіденційної інформації або систем. Деякі поширені методи

соціальної інженерії включають підступні атаки по телефону або електронній пошті, виманювання інформації через підробку особи або використання прийомів впливу і маніпуляції, щоб змусити людей розкрити свої паролі, особисті дані або виконати небезпечні дії [20].

Основними атакми соціальної інженерії є:

— Bating (Цькування)

— Scareware (Відлякувальні програми)

— Pretexting (Претекстинг)

— Phishing (Фішинг)

Як випливає з назви, bating-атаки використовують фальшиві обіцянки, щоб викликати жадібність або цікавість жертви. Вони заманюють користувачів у пастку, яка викрадає їх особисту інформацію або заповнює їхні системи шкідливим програмним забезпеченням.

Найкритичніша форма bating-атаки використовує фізичні носії для розповсюдження зловмисного програмного забезпечення. Наприклад, зловмисники залишають приманку — як правило, заражені шкідливим програмним забезпеченням флеш-накопичувачі — на помітних місцях, де потенційні жертви напевно побачать їх (наприклад, у ванних кімнатах, ліфтах, парковці цільової компанії). Приманка має автентичний вигляд, наприклад, етикетка, яка представляє її як список заробітної плати компанії.

Жертви підхоплюють наживку з цікавості та вставляють її в робочий чи домашній комп’ютер, що призводить до автоматичної інсталяції зловмисного програмного забезпечення в системі [21].

Відлякувальне програмне забезпечення передбачає бомбардування жертв помилковими тривогами та фіктивними погрозами. Користувачі вводяться в оману, думаючи, що їхня система заражена зловмисним програмним забезпеченням, що спонукає їх інсталювати програмне забезпечення, яке не приносить реальної користі (окрім для зловмисника) або саме по собі є зловмисним програмним забезпеченням. Scareware також називають програмним

забезпеченням для обману, програмним забезпеченням для сканування шахраїв і шахрайським програмним забезпеченням.

Типовим прикладом страшного програмного забезпечення є звичайні спливаючі банери, які з'являються у вашому браузері під час перегляду веб-сторінок і містять такий текст, як «Ваш комп'ютер може бути заражений шкідливими шпигунськими програмами». Він або пропонує встановити інструмент (часто інфікований зловмисним програмним забезпеченням), або скеровує вас на шкідливий сайт, де ваш комп'ютер заражається.

Програмне забезпечення від страху також розповсюджується через спам, який розповсюджує фіктивні попередження або пропонує користувачам придбати шкідливі послуги [22].

За допомогою претекстингу зловмисник отримує інформацію за допомогою серії вміло сфабрикованих брехень. Шахрайство часто ініціюється зловмисником, який вдає, що йому потрібна конфіденційна інформація від жертви для виконання критично важливого завдання.

Зловмисники зазвичай починають із встановлення довіри зі своєю жертвою, видаючи себе за колег, поліцейських, банківських і податкових службовців або інших осіб, які мають право знати. Претекст ставить запитання, які нібито потрібні для підтвердження особи жертви, за допомогою якої вони збирають важливі особисті дані.

За допомогою цього шахрайства збирається різна відповідна інформація та записи, наприклад номери соціального страхування, особисті адреси та номери телефонів, телефонні записи, дати відпусток співробітників, банківські записи та навіть інформація про безпеку, пов'язана з фізичним підприємством [23].

Як один із найпопулярніших типів атак соціальної інженерії, фішингове шахрайство – це кампанії електронною поштою та текстовими повідомленнями, спрямовані на те, щоб викликати у жертв відчуття терміновості, цікавості чи страху. Потім він спонукає їх розкрити конфіденційну інформацію, натиснути посилання на шкідливі веб-сайти або відкрити вкладення, які містять зловмисне програмне забезпечення.

Прикладом може бути електронний лист, надісланий користувачам онлайн-сервісу, який сповіщає їх про порушення політики, що вимагає негайних дій з їхнього боку, наприклад необхідної зміни пароля. Він містить посилання на нелегітимний веб-сайт — майже ідентичний за зовнішнім виглядом своїй законній версії — спонукаючи нічого не підозрюючого користувача ввести свої поточні облікові дані та новий пароль. Після надсилання форми інформація надсилається зловмиснику.

Дуже часто зловмисники шукають дані, які самі по собі не є конфіденційними, але можуть розширити список потенційних жертв. Це створює серйозну загрозу безпеці даних, оскільки зловмисники можуть легко обдурити нічого не підозрюючих співробітників, запитуючи на перший погляд нешкідливу інформацію, таку як номери телефонів і номери соціального страхування.

Враховуючи, що ідентичні або майже ідентичні повідомлення надсилаються всім користувачам у фішингових кампаніях, виявити та заблокувати їх набагато простіше для поштових серверів, які мають доступ до платформ обміну загрозами [24].

Завдяки MaxPatrol і Trend Micro усі листи та підозрілі посилання перевіряються на достовірність, тобто здійснюється порівняння реальної адреси із тією, яка є у листі, а також перевіряється міст посилань і прикріплених файлів до електронних листів. Таким чином ми зменшили ризик крадіжки конфіденційної інформації, а також посилили нашу системи безпеки. Наші активи у безпеці, а загроза має тепер менший шанс на реалізацію. На моделі загроз, на рисунку 3.2, детальніше зображено всі активи, загрози та запропоновані рішення на зменшення ризику виникнення сценарію загрози через певну вразливість.

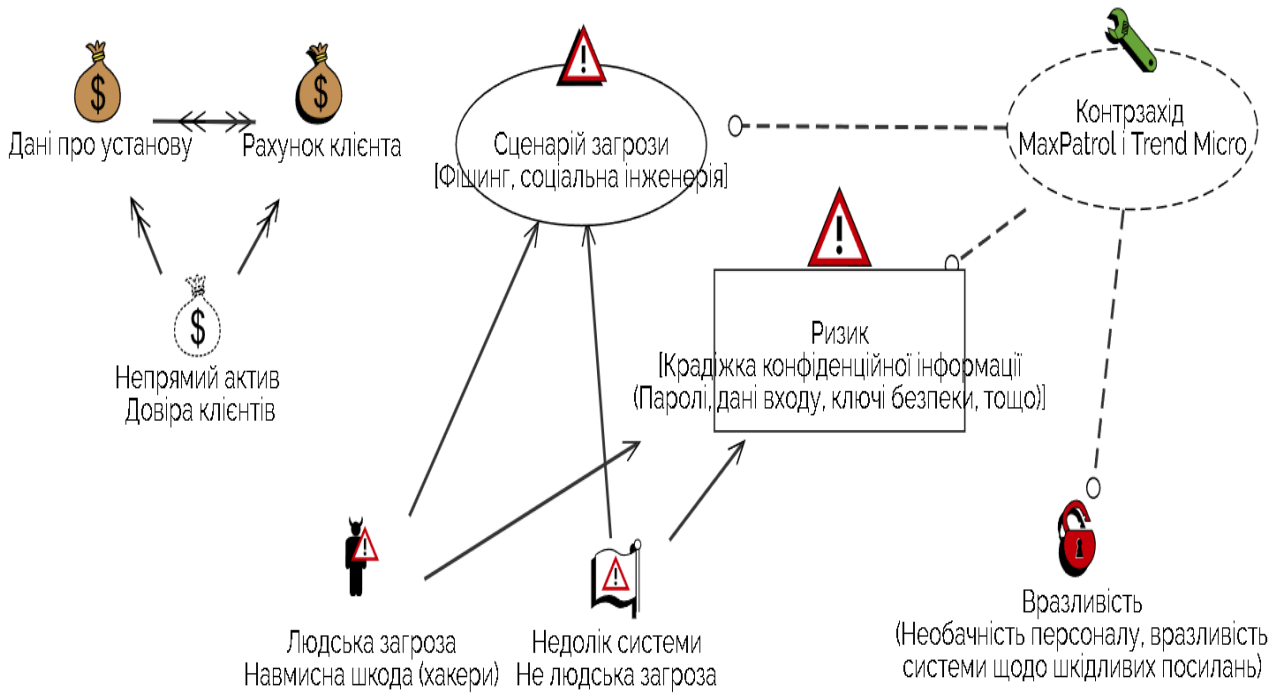


Рисунок 3.2 — Модель загрози фішингу та соціальної інженерії у системі управління інформаційної безпеки банку

Загрози впровадження вірусів, троянів, черв'яків у СУІБ була досить високою, адже за допомогою них могли постраждати більші активи. Ця загроза більш серйозніше тому що віруси, трояни і черв'яки можуть спотворити інформацію на серверах банку, або ж у хмарних середовищах, де ця інформація зберігається. Якщо ж інформація спотворена, то робота банку буде призупинена до тої пори, поки ці дані не стануть доступними. Зловмисники можуть їх зашифрувати, і на виявлення яким самим алгоритмом це було зроблено може піти не один день. Зловмисники можуть стерти частину інформації і залишити лише ті частинки інформації, які не матимуть сенсу, ускладнюючі роботу персоналу. Хакери таож можуть залишити вірус у системі, аби той «викачував» усі дані на інший носій або хмарне середовище, з ціллю шпіонажу та збирання данних про вкладників, транзакції, отримувачів та суми [25].

— Віруси — це комп'ютерні програми, які з'єднуються з іншим програмним забезпеченням або програмами, щоб завдати шкоди системі, тоді як

черв’яки дублюються, щоб уповільнити роботу комп’ютерної системи. З іншого боку, замість реплікації, троян зберігає важливі дані про комп’ютерну систему чи мережу.

— Вірус атакує виконуваний файл і приєднується до нього, щоб змінити файл, тоді як хробак атакує недоліки системи та програм. З іншого боку, троян виглядає корисною програмою, яка містить прихований код, який виконується для виконання небажаних або шкідливих операцій.

— Виконання та передача вірусу залежить від передачі заражених файлів, тоді як хробаки розмножуються без людських дій і використовують мережу для вбудовування в інші системи. З іншого боку, троян працює як допоміжне програмне забезпечення та виконується.

— Вірус не можна контролювати дистанційно. З іншого боку, хробаками та троянами можна керувати дистанційно.

— Вірус в основному використовується для зміни або стирання системних даних, тоді як хробаки використовуються для надмірного використання ресурсів системи та уповільнення її роботи. З іншого боку, трояни може бути використаний для викрадення даних користувача з метою отримання доступу до комп’ютерної системи користувача.

— Віруси можуть поширюватися повільно, тоді як глисти можуть поширюватися швидко. Навпаки, трояни також можуть поширюватися повільно [26].

MaxPatrol, Trend Micro та PinCat зменшують цю загрозу. PinCat, до прикладу, завжди робить back-up, або ж копію інформації та зберігає її у хмарному середовищу якраз на таких випадок, Trend Micro у нас захищає внутрішню систему банку, на випадок, якщо потрібно обмежити вірус лише у якійсь одній гілці мережі, FireEye порівнює сигнатури із внутрішньою системою та допомагає ідентифікувати який саме вірус, троян, або ж черв’як проникнув у систему, а MaxPatrol допоможе у виявленні слабких ланок у СУІБ, через яку стало можливим проникнення шкідливого програмного забезпечення у систему. На моделі загроз, на рисунку 3.3, детальніше зображено всі активи, загрози та

запропоновані рішення на зменшення ризику виникнення сценарію загрози через певну вразливість.

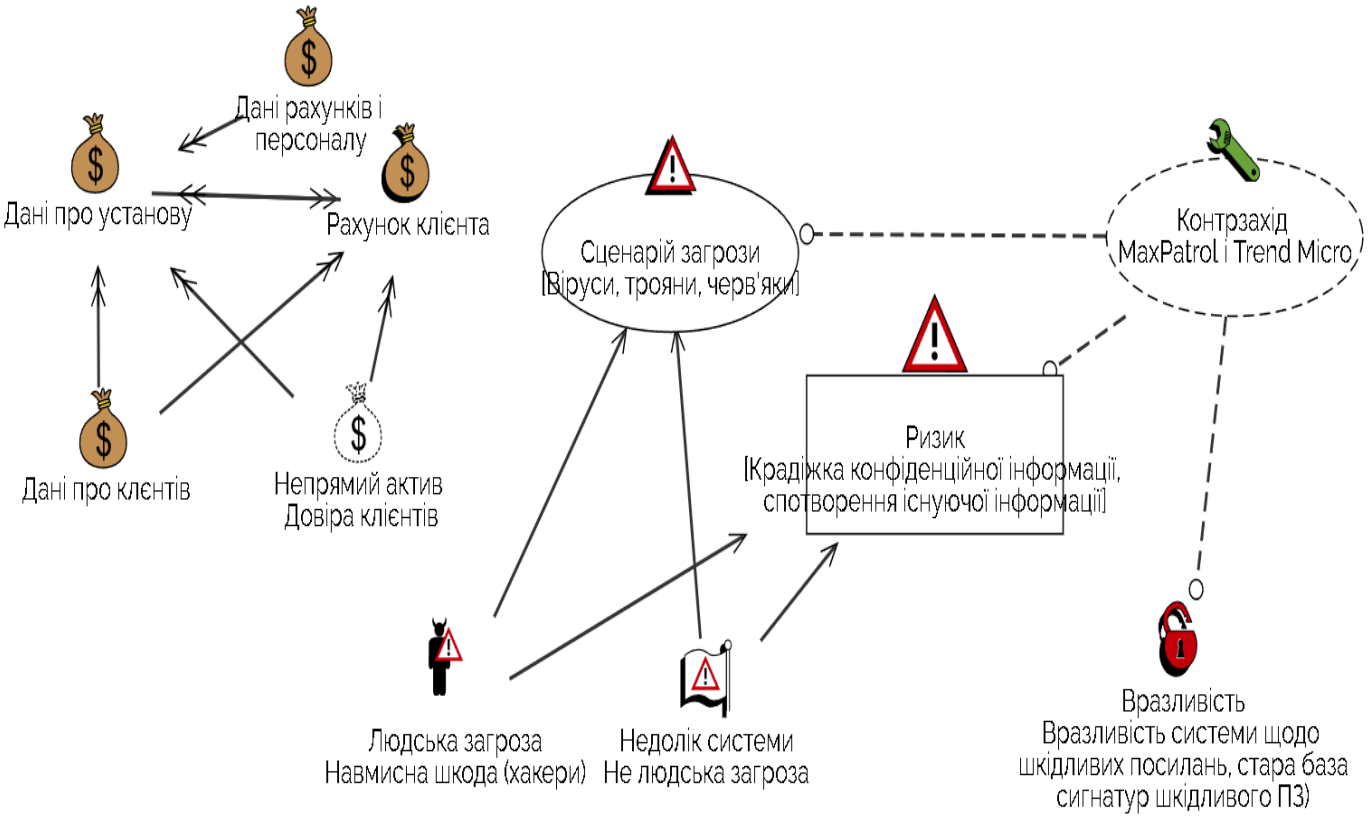


Рисунок 3.3 — Модель загрози проникнення у систему управління інформаційної безпеки банку вірусів, троянів, черв’яків

Атаки відмови доступу у системи інформаційної безпеки банків трапляються часто. Навіть ненавмисно, коли велика кількість запитів від клієнтів банків надходить до серверів одночасно, що сповільнює систему в рази, або ж навіть генерує настільки багато нових запитів, що система просто не справляється з цим та перестає відповідати. Навмисно ж ці атаки проводяться з ціллю відволікти увагу адміністраторів безпеки від справжньої атаки, яка проводиться із метою викрадення даних [27][28]. Щоб вирішити цю проблему я запропонувала два програмних забезпечення: PinCat і Trend Micro. PinCat у нас працює таким чином, що якщо за маленький проміжок часу з однієї і тієї ж самої адреси надходить велика кількість запитів за короткий проміок часу, ця адреса блокується на певний період часу, йде у так званий таймаут, і не може надсилати

запити протягом певного періоду часу. Можна встановити цей проміжок, до прикладу, якщо з однієї адреси надійшло десять запитів за долю секунди, то решта запитів із цієї адреси блокується, на п’ять хвилин. Trend Micro ж працює більш по доменам, тому він будет виконувати супровідні дії, забезпечуючи ті ж самі дії, але на мобільних додатках. Таким чином ризик перенавантаження системи зменшиться в рази і не буде обмежувати простих користувачів, адже наврядчи жива людина зможе створити таку велику кількість запитів з таких короткий проміжок часу [29] [30].

Остання атака, яка відбувалася на банк, після покращення СУІБ, проходила таким чином:

— Зловмисники використовували ботнет, який представляє собою сукупність заражених комп’ютерів та інших пристроїв, підключених до Інтернету, щоб розпочати атаку, яка генерувала понад 20 гігабіт на секунду обсягу на веб-сайт нашого банку.

— У цій атаці зловмисники використовували вразливий мережевий протокол часу, або сервери NTP. Вони надсилали дуже маленькі запити на сервер NTP, але сервери відповідали дуже великими відповідями. Зловмисники підробляли IP-адресу так, щоб виглядало, ніби веб-сайт банку надіслав запит. Потім відповідь, яка була дуже великою, була відправлена з NTP-сервера назад на сайт банку. Зокрема, зловмисники використовували команду monlist, яка містить останні 600 записів у пам’яті цього NTP-сервера. Отже, хоча розмір запиту був дуже малим, розмір відповіді був дуже великим порівняно з веб-сайтом цього банку.

— І так само, як NTP, вони також використовують уразливі сервери системи доменних імен (або DNS) для посилення атак і на веб-сайт банку. Зокрема, вони використовували розширення DNSSEC для посилення атаки, а також використовували позначку «Будь-який» в атаці DNS для надсилання великих відповідей жертві.

— Поки відбувалися ці flood-атаки, зловмисник також запустив творчу атаку, яка використовувала тунелі IPsec. Тунелі IPsec використовуються для

безпечного зв’язку між двома підключеними кінцевими точками в Інтернеті. Існує дві різні фази, які використовуються для налаштування тунелю IPsec. Фаза 1 використовується для налаштування деталей керування тим, як буде використовуватися тунель. Фаза 2 фактично є тунелем усередині цього тунелю, де протікає безпечний зв’язок. Отже, зловмисники використовували дані Фази 1 для зв’язку з веб-сайтом цього банку, але потім вони так і не завершили повністю тунель Фази 2. Це призвело до того, що веб-сайт банку залишився на ресурсах, споживаючи ресурси та чекав завершення тунелю Фази 2. Загалом ця атака згенерувала понад 20 гігабіт на секунду обсягу проти банку.

— Для пом'якшення цієї атаки було вжито кілька кроків. Першим кроком було закрити порти UDP для трафіку атаки. Вони також використовували завідомо хороші білі списки для відомо хорошого трафіку. Брандмауер, який має можливість дозволяти або забороняти певні номери портів, був налаштований на блокування конкретних портів, які використовуються цією атакою. І багато протоколів, які використовувалися, на той момент не потребували дозволу через брандмауер компанії, тому було прийнятно тримати їх закритими. Але інші потрібно було закрити на час атаки, а потім знову відкрити після завершення атаки, як, наприклад, DNS. Після цього затоплення IPsec було пом’якшено шляхом перевірки, чи було відкрито Фазу 1 будь-якою IP-адресою, але фаза друга не була завершена. А потім цю IP-адресу було заблоковано. Потім було складено відомий список порушників, оскільки ці IP-адреси блокувалися, і це дозволило банку запобігти майбутнім атакам цих відомих зловмисників.

— Загалом атаку вдалося зупинити, і банк зміг надавати послуги своїм клієнтам. Під час атаки клієнтський досвід трохи сповільнився, але повністю не припинився.

На моделі загроз, на рисунку 3.4, детальніше зображено всі активи, загрози та запропоновані рішення на зменшення ризику виникнення сценарію загрози через певну вразливість.

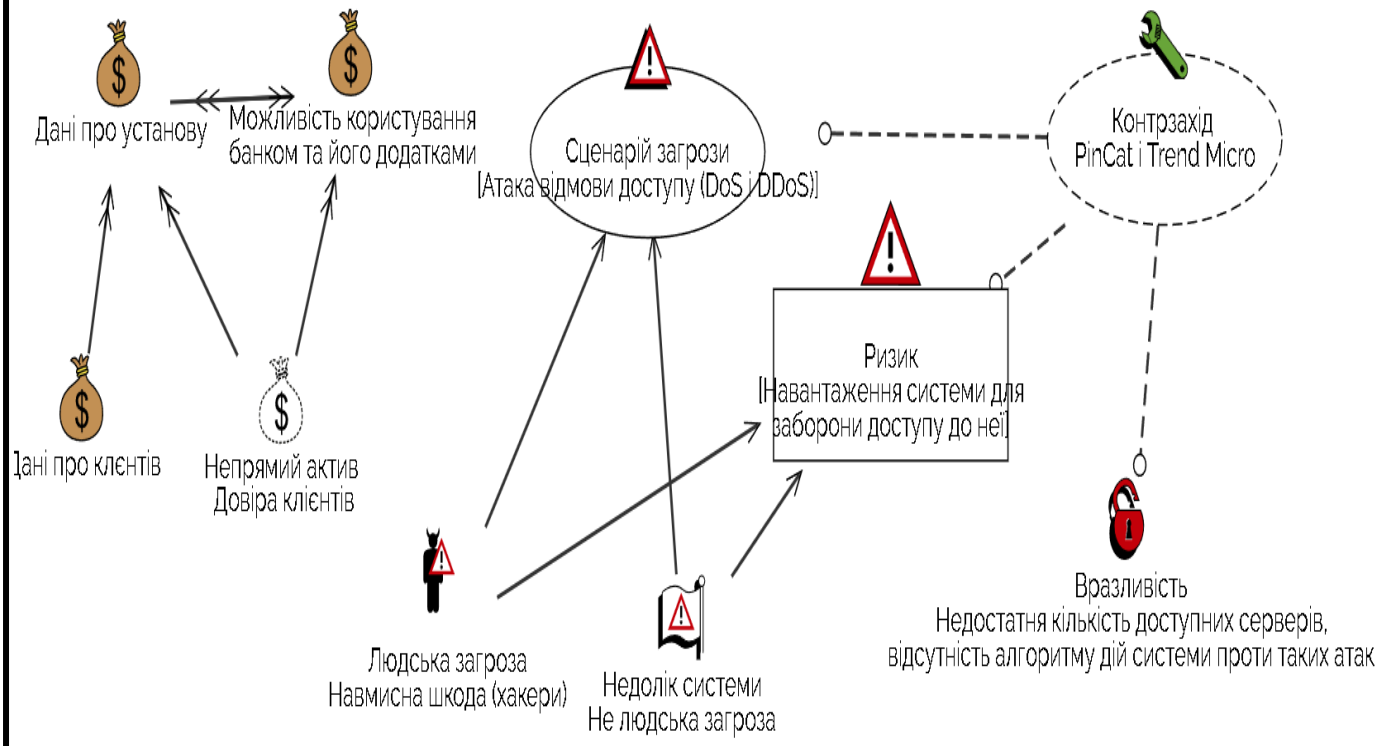


Рисунок 3.4 — Модель загрози атаками відмови доступу (DoS і DDoS) у системі управління інформаційної безпеки банку

Наступною великою загрозою є втрата даних через «злиття» її працівником установи. Дуже часто конфіденційну інформацію хакери отримують навіть без зламу системи безпеки, а просто підкупивши людину, яка там працює. Яскравим прикладом буде нещодавнє злиття даних Сбербанку. У архівах містилися гігабайти даних про працівників, їхні паспортні дані, номери телефонів, ініціали, ідентифікаційні коди, посади, та обов'язки. Проте вся ця інформація не була здобута шляхом грубого зламу систем захисту та викачки даних — вона була опублікована працівником із відділу безпеки банку, у якості акта протесту проти політики компанії [31][32]. Відповідно до останнього звіту Verizon, 82% порушень пов'язані з людським фактором, включаючи соціальні атаки, помилки та неправильне використання. Це означає, що співробітники можуть бути найслабшою ланкою в ланцюжку безпеки даних. За допомогою MaxPatrol наша система тепер має аудит безпеки, який записує дії користувачів на платформі у режимі реального часу, співставляючи всі дії із часом їхнього виконання. Це

допоможе зловити підкупленного або недобросовісного працівника до того, як він зможе вчинити шкоду. Адміністратор безпеки буде бачити, що певний користувач переглядає дуже багато сторінок і скачує ці дані, і зможе заблокувати доступ цьому користувачу до системи, аби обмежити його подальші дії. Цей аудит безпеки також згодиться з кримінальної точки зору, адже зловмисника буде можливо на основі інформації про його дії у системи банку притягнути до кримінальної відповідальності. Звичайно, можна підкупити самого адміністратора безпеки, який матиме доступ до цих даних, проте у системі управління інформаційної безпеки банку таких адміністраторів є декілька, і це мінімізує можливість саботажу з їхнього боку. На моделі загроз, на рисунку 3.5, детальніше зображено всі активи, загрози та запропоновані рішення на зменшення ризику виникнення сценарію загрози через певну вразливість.

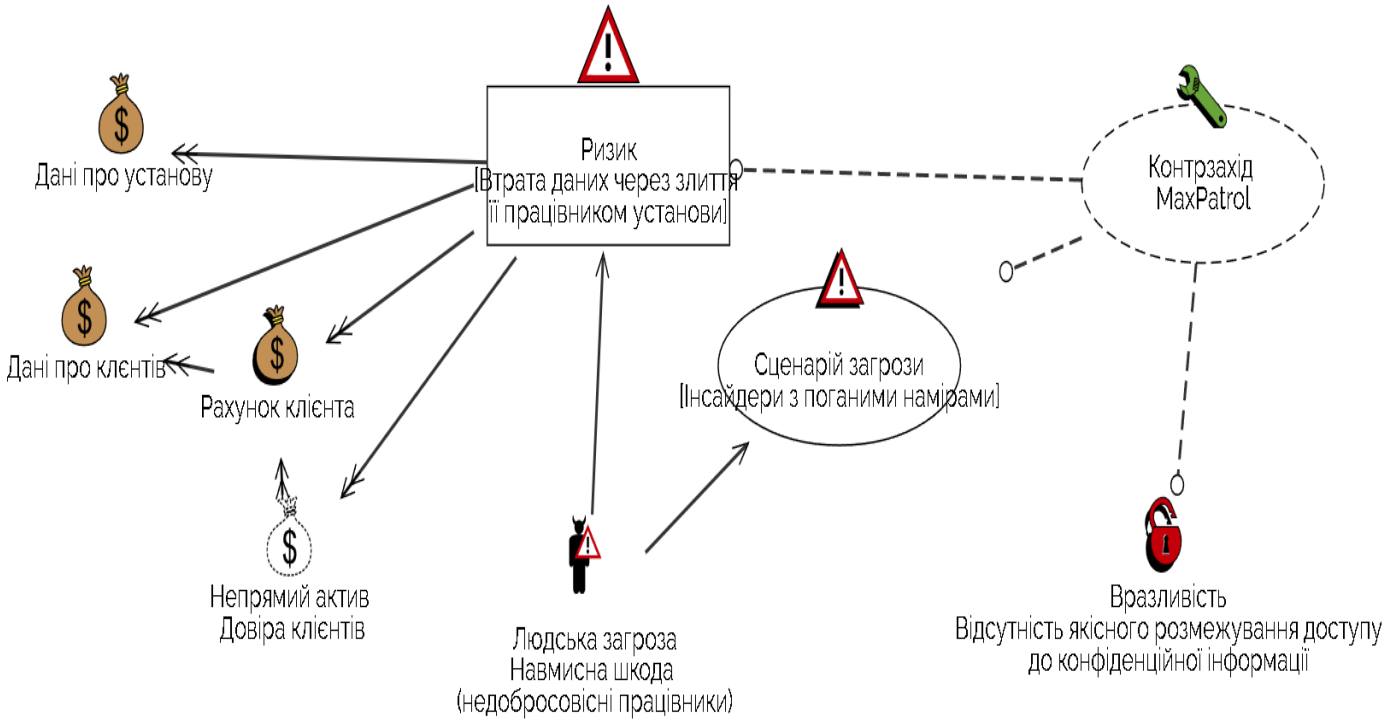


Рисунок 3.5 — Модель загрози втрати даних через її злиття працівником банку у системі управління інформаційної безпеки банку

Веб-атаки, також відомі як атаки на веб-додатки, є останньою великою загрозою, з якою може зіткнутися система управління інформаційної безпеки банку. Незважаючи на свої переваги, веб-програми викликають низку проблем

безпеки, що виникають через неправильне кодування. Серйозні недоліки або вразливості дозволяють зловмисникам отримати прямий і відкритий доступ до баз даних, щоб переробити конфіденційні дані – це відоме як атака веб-додатків. Наші бази даних містять цінну інформацію (особисті дані та фінансові деталі), що робить їх частими об'єктами атак. Хоча такі акти вандалізму (часто вчинені так званими сценаристами), як псування корпоративних веб-сайтів, все ще є звичним явищем, сьогодні зловмисники віддають перевагу отриманню доступу до конфіденційних даних, що зберігаються на сервері баз даних, через величезну вигоду від продажу результатів порушення даних [33][34].

Веб-сайти банку залежать від їхніх баз даних для доставки необхідної інформації клієнтам. Якщо веб-програми не захищені, тобто вразливі до принаймні однієї з різних форм хакерських методів, то вся банківська база даних конфіденційної інформації піддається серйозному ризику атаки веб-програми. Типи атак SQL Injection, спрямовані безпосередньо на бази даних, все ще є найпоширенішим і найнебезпечнішим типом уразливості. Інші зловмисники можуть вводити зловмисний код, використовуючи дані користувача вразливих веб-програм, щоб обманювати користувачів і перенаправляти їх на фішингові сайти. Цей тип атаки називається Cross-Site Scripting (атаки XSS) і може використовуватися, навіть якщо самі веб-сервери та механізм бази даних не містять уразливості. Він часто використовується в поєднанні з іншими векторами атак, такими як атаки соціальної інженерії. Існує багато інших типових атак, таких як обхід каталогу, включення локальних файлів тощо.

Останні дослідження показують, що 75% кібератак здійснюються на рівні веб-додатків. Веб-сайти та відповідні веб-додатки мають бути доступними 24 години на добу, 7 днів на тиждень, щоб надавати необхідні послуги клієнтам, співробітникам, та іншим зацікавленим сторонам [35].

Брандмауери та SSL не забезпечують захисту від атак веб-додатків просто тому, що доступ до веб-сайту має бути відкритим. До всіх сучасних систем баз даних (наприклад, Microsoft SQL Server, Oracle і MySQL) можна отримати доступ через певні порти (наприклад, порт 80 і 443), і будь-хто може спробувати пряме підключення до баз даних, фактично обходячи механізми безпеки, які

використовуються операційною системою. Ці порти залишаються відкритими, щоб забезпечити зв’язок із законним трафіком, і тому є основною вразливістю.

Веб-програми часто мають прямий доступ до серверних даних, таких як бази даних клієнтів, і, отже, контролюють цінні дані, і їх набагато складніше захистити. Ті, хто не мають доступу, матимуть певну форму сценарію, який дозволяє збирати та передавати дані. Якщо зловмиснику стане відомо про слабкі місця в такому сценарії, він може легко перенаправити ненавмисний трафік в інше місце та незаконно прибрати особисті дані [36].

За допомогою PinCat і FireEye у нас ці проблеми будуть мінімізовані. Ці два програмних засоби постійно шукають вразливості у системі, знаходяться у постійному режимі готовності до тієї чи іншої загрози, і також поширюють свій захист не тільки на бази даних банку, як на серверах, так у хмарних середовищах, а також у веб-додатках. На моделі загроз, на рисунку 3.6, детальніше зображено всі активи, загрози та запропоновані рішення на зменшення ризику виникнення сценарію загрози через певну вразливість.

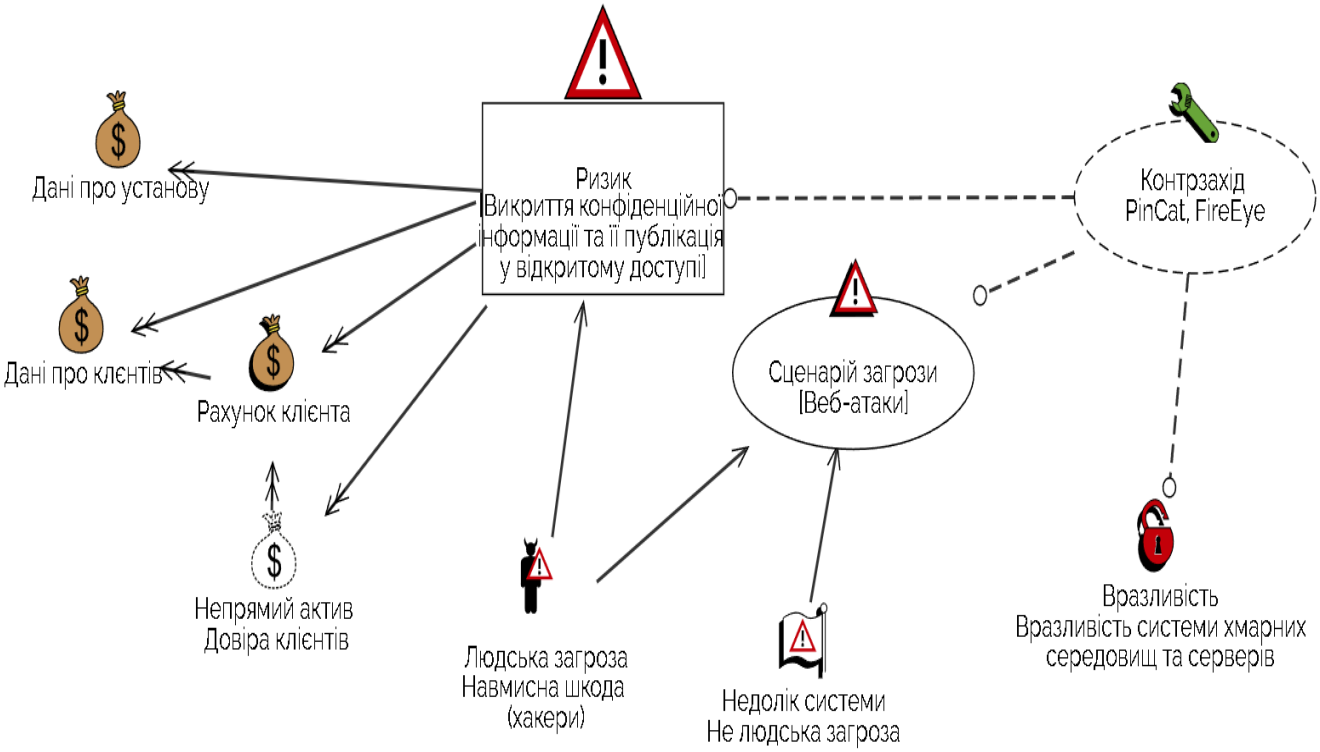


Рисунок 3.6 — Модель загрози веб-атак у системі управління інформаційної безпеки банку

3.2 Результати симуляції

Після впровадження рішень щодо покращення системи управління інформаційної безпеки банку рівень захисту значно покращився. Краще всього ці покращення можна помітити на рисунку 3.7, який наведено нижче.

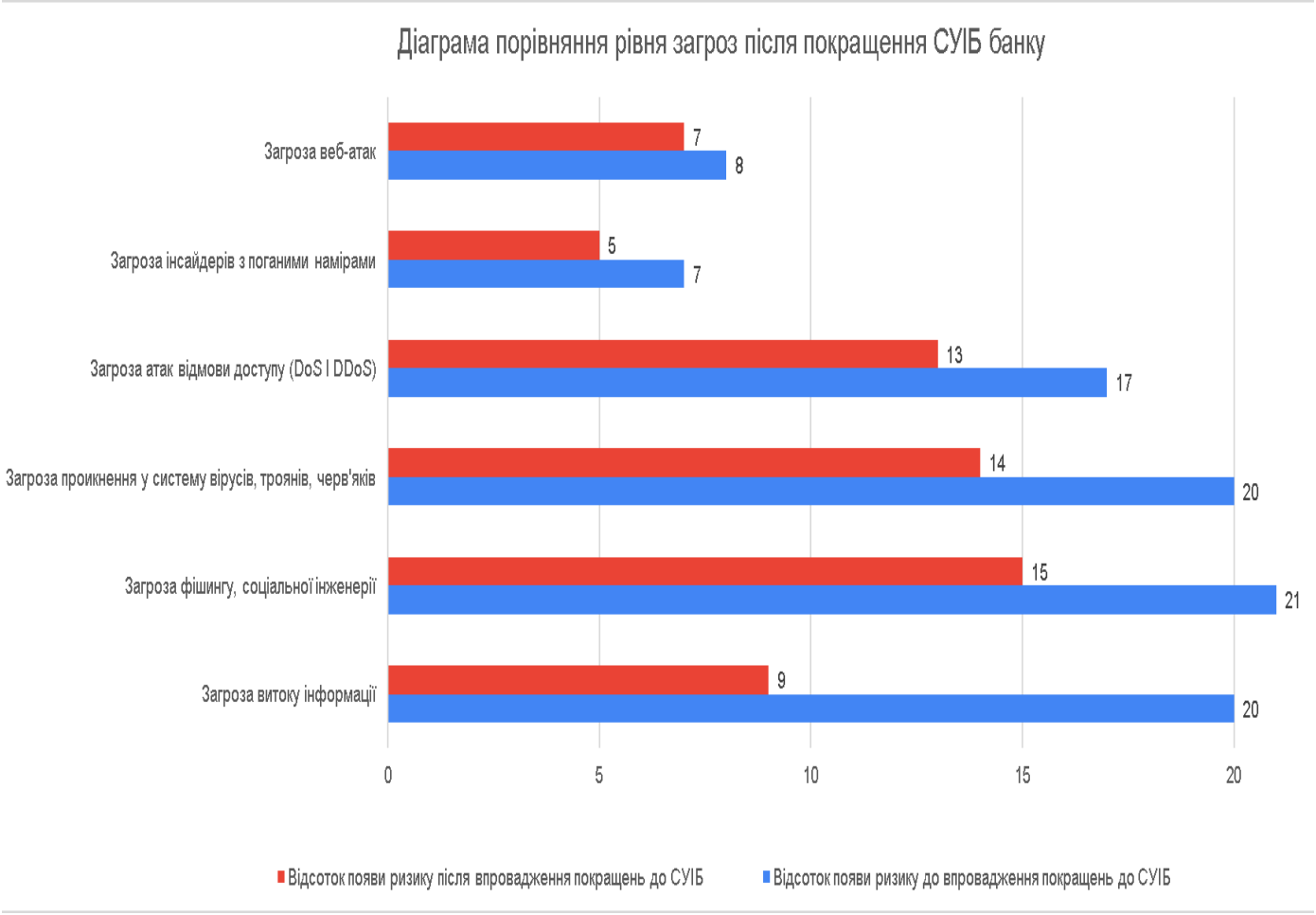


Рисунок 3.7 — Діаграма порівняння рівня загроз після введення покращень до системи управління інформаційною безпекою банку

Після введення чотирьох нових програмних засобів загроза витоку інформації зменшилася аж на 11%, маючи значення 9% замість 20%. Ефективність введення аудиту безпеки та моніторингу роботи працівників покращилася значно, що і видно на діаграмі. Загроза фішингу та соціальної інженерії зменшилася на 6%, впавши з 21% до 15% [38]. Перевірка адрес електронних листів, електронних підписів на документах та достовірної адреси

сайтів допомогла зменшити цей ризик. Загроза проникнення у систему управління інформаційної безпеки банку вірусів, троянів, черв'яків після тестування програмних засобів зменшилась на 6%, і тепер має значення в 14%, хоча до впровадження рішень мала 20%. Загроза атак відмови доступу DoS і DDoS зменшилася на 4%, з 17% до 13% [39]. Загроза інсайдерів з поганими намірами за період тестування проявлялась не так часто, але навіть із невеликою кількістю даних вже видно покращення, невелике, але покращення — ризик виникнення впав із 7% до 5%. Остання загроза, загроза виникнення веб-атак, також проявлялась за період тестування не так часто, але на діаграмі вино, що ж невелике покращення у вигляді 1%, з 8% до 7%. [40]

Ці дані були взяті за період роботи системи протягом одного місяця. Я впевнена, що якщо дати цій системі пропрацювати рік і більше, то результати і зміни у порівнянні з тим що було, проявляться більш явно.

3.3 Висновки

Після підрахування відсотків виникнення загроз після впровадження покращень до системи управління інформаційною системою банку, я можу з впевненістю сказати, що проведення інтернет-транзакцій стало більш безпечним. Ситуація із витоками даних, що конфіденційних, таких як подальші плани банку, так і не дуже конфіденційних, на прикладі особистих даних працівників, покращилася в рази. В довгостроковій перспективі цю систему можна покращувати і змінювати, в залежності від тих загроз і тих вразливостей, які буде реєструвати система захисту.

ВИСНОВКИ

У результаті виконання даної кваліфікаційної роботи, мною було проаналізовано і досліджено предметну область, теоретичну інформацію про проєктування систем управління інформаційної безпеки банку та її особливості в зв'язку з вимогами та чинним законодавством. Мною була спроєктована, розроблена та реалізована система управління інформаційної безпеки банку з ціллю налаштування системи захисту інформації банку від небажаного злому, витоків інформації, загроз атак відмови доступу, фішингу, соціальної інженерії, атак на веб-додатки банку, такі як сайт чи додаток на смартфон.

Заявлені і запропоновані завдання та вимоги до системи управління інформаційної безпеки банку виконано у повному обсягу. Розроблена система має широкий простір для подальшого удосконалення, доповнення, розширення та модернізації згідно з вимогами часу.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1) Поняття інформаційної безпеки банківської установи, Охорона банківської таємниці, правові засади : http://obt.inf.ua/page10.html (дата звернення 14.03.2023)

2) Система захисту інформації в банку, Посібники, статті та книги для студентів : https://posibniki.com.ua/post-sistema-zahistu-informaciyi-v-banku#:~:text=Система%20захисту%20інформації%20банку%20—%20це,і%20використання%20інформації%20в%20банку. (дата звернення 15.03.2023)

3) Модель та методи визначення проектних характеристик систем управління інформаційною безпекою. Монографія, ResearchGate : https://www.researchgate.net/publication/348788054_Model_ta_metodi_viznacenna_proektnih_harakteristik_sistem_upravlinna_informacijnou_bezpekou_Monografia (дата звернення 15.03.2023)

4) Забезпечення інформаційної безпеки банківських систем, FeelSecuredGlobaly : https://group-fs.com/zabezpechennya-informaczijnoyi-bezpeky-bankivskyh-system-osnovni-zasady-kiberbezpeky-bankiv/ (дата звернення 15.03.2023)

5) Кавун С. В. Інформаційна безпека. Навчальний посібник / С. В. Кавун, В. В. Носов, О. В. Манжай. – Харків: Вид. ХНЕУ, 2008. – 352 с.

6) Черевко О. В. Джерела виникнення загроз інформаційній безпеці банківських установ / О. В. Черевко, В. М. Андрієнко, І. Ю. Напора // Вісник Черкаського університету. Серія: Економічні науки. – 2016. – № 3. – С.120-127.

7) Чернадчук Т. Забезпечення інформаційної безпеки як один із напрямів банківської діяльності / Т. Чернадчук // Юридична Україна. – 2013. – №3. – С. 44-47

8) Сухонос В. В. Концептуальні організаційно-правові засади функціонування системи економічної безпеки банків / В. В. Сухонос // Правовий вісник Української академії банківською справи. – 2011. – № 1. – С. 64-66. – Режим доступу: http://www.nbuv.gov.ua/old_jrn/Soc_Gum/Pvuabs/2011_1/04_03_02.pdf.

9) ABBA: An Agent-Based Model of the Banking System, IMF Working Paper : https://www.imf.org/en/Publications/WP/Issues/2017/06/09/ABBA-An-Agent-Based-Model-of-the-Banking-System-44916 (дата звернення 20.03.2023)

10) System Design of Bank Management System, OpenGenus : https://iq.opengenus.org/system-design-of-bank-management-system/ (дата звернення 20.03.2023)

11) Рецепт приготування СУІБ в домашніх умовах : https://www.linkedin.com/pulse/рецепт-приготування-суіб-в-домашніх-умовах-yurii-yurchenko-1 (дата звернення 20.03.2023)

12) Що таке «планування-виконання-перевірка-дія» (PDCA)? : https://experience.dropbox.com/uk-ua/resources/pdca (дата звернення 21.03.2023)

13) PinCat Security System, PinCat : https://www.pincat.am/copy-of-pss (дата звернення 21.03.2023)

14) Combination of McAfee Enterprise and FireEye Complete, Trellix : https://www.trellix.com/en-us/about/newsroom/news/news-detail.html?news_id=141c899e-cc82-4aad-8d57-52eead86ab99 (дата звернення 21.03.2023)

15) Trend Micro, trendmicro: https://www.trendmicro.com/ru_ru/business.html (дата звернення 21.03.2023)

16) MaxPatrol, Positive Technologies : https://www.ptsecurity.com/ru-ru/products/mp8/ (дата звернення 21.03.2023)

17) Загрози витоку інформації технічними каналами : http://ni.biz.ua/9/9_2/9_23037_ugrozi-utechki-informatsii-po-tehnicheskim-kanalam.html (дата звернення 01.04.2023)

18) Захист від витоку інформації : http://integritysys.com.ua/security/dlp/ (дата звернення 01.04.2023)

19) Data Leakage: Understanding and Preventing the Threat : https://perception-point.io/guides/endpoint-security/data-leakage-understanding-and-preventing-the-threat/ (дата звернення 02.04.2023)

20) Avoiding Social Engineering and Phishing Attacks : https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks (дата звернення 10.04.2023)

21) Phishing and Social Engineering : https://www.unco.edu/cybersecurity/student-resources/phishing-social-engineering.aspx (дата звернення 11.04.2023)

22) Social Engineering : https://www.imperva.com/learn/application-security/social-engineering-attack/ (дата звернення 12.04.2023)

23) What is pretexting? : https://www.ibm.com/topics/pretexting#:~:text=the%20next%20step-,What%20is%20pretexting%3F,the%20organization%20they%20work%20for. (дата звернення 14.04.2023)

24) What is phishing | Attack techniques & scam examples : https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiw3-DKmqT_AhUGy4sKHeoGB_oQFnoECAwQAQ&url=https%3A%2F%2Fwww.imperva.com%2Flearn%2Fapplication-security%2Fphishing-attack-scam%2F&usg=AOvVaw35ccf1P0W-UgePDQIcTbOe (дата звернення 15.04.2023)

25) Difference between Virus, Worm, and Trojan horse : https://www.javatpoint.com/virus-vs-worm-vs-trojan-horse#:~:text=Viruses%20are%20computer%20programs%20that,computer%20system%20or%20a%20network. (дата звернення 18.04.2023)

26) Recovering from Viruses, Worms, and Trojan Horses, CISA : https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiZidjrmqT_AhVMposKHfavA6UQFnoECBEQAQ&url=https%3A%2F%2Fwww.cisa.gov%2Fnews-events%2Fnews%2Frecovering-viruses-worms-and-trojan-horses&usg=AOvVaw2ZWQL3jPpIjGfHtkSZ9kBc (дата звернення 20.04.2023)

27) DoS Attack vs. DDoS Attack: Key Differences? – Fortinet : https://www.fortinet.com/resources/cyberglossary/dos-vs-ddos (дата звернення 22.04.2023)

28) Dos vs DDoS Attacks: The Differences and How To Prevent Them : https://www.comparitech.com/net-admin/dos-vs-ddos-attacks-differences-prevention/ (дата звернення 23.04.2023)

29) DoS vs. DDoS Attacks: What's The Difference? | Microsoft 365 : https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/dos-vs-ddos-attacks-whats-the-difference (дата звернення 24.04.2023)

30) Denial-of-service attack : https://en.wikipedia.org/wiki/Denial-of-service_attack (дата звернення 25.04.2023)

31) What's the Difference Between a Data Leak and a Data Breach? : https://abnormalsecurity.com/glossary/data-leak (дата звернення 26.04.2023)

32) Biggest cause of data leaks: Human errors : https://www.smartlockr.io/en/blog/biggest-cause-data-leaks-human-errors (дата звернення 01.05.2023)

33) The 10 Most Common Website Security Attacks (and How to Protect Yourself) : https://www.tripwire.com/state-of-security/most-common-website-security-attacks-and-how-to-protect-yourself (дата звернення 03.05.2023)

34) Common Web Application Attacks : https://www.trustnetinc.com/web-application-attacks/ (дата звернення 06.05.2023)

35) Types of Cyber Attacks You Should Be Aware of in 2023 : https://www.simplilearn.com/tutorials/cyber-security-tutorial/types-of-cyber-attacks (дата звернення 07.05.2023)

36) 5 Ways in Which Banks Secure Their Data : https://www.endpointprotector.com/blog/ways-banks-secure-data/ (дата звернення 11.05.2023)

37) How Banks Can Achieve Compliance While Improving Security and Productivity : https://www.theglobaltreasurer.com/2007/02/12/how-banks-can-achieve-compliance-while-improving-security-and-productivity/ (дата звернення 14.05.2023)

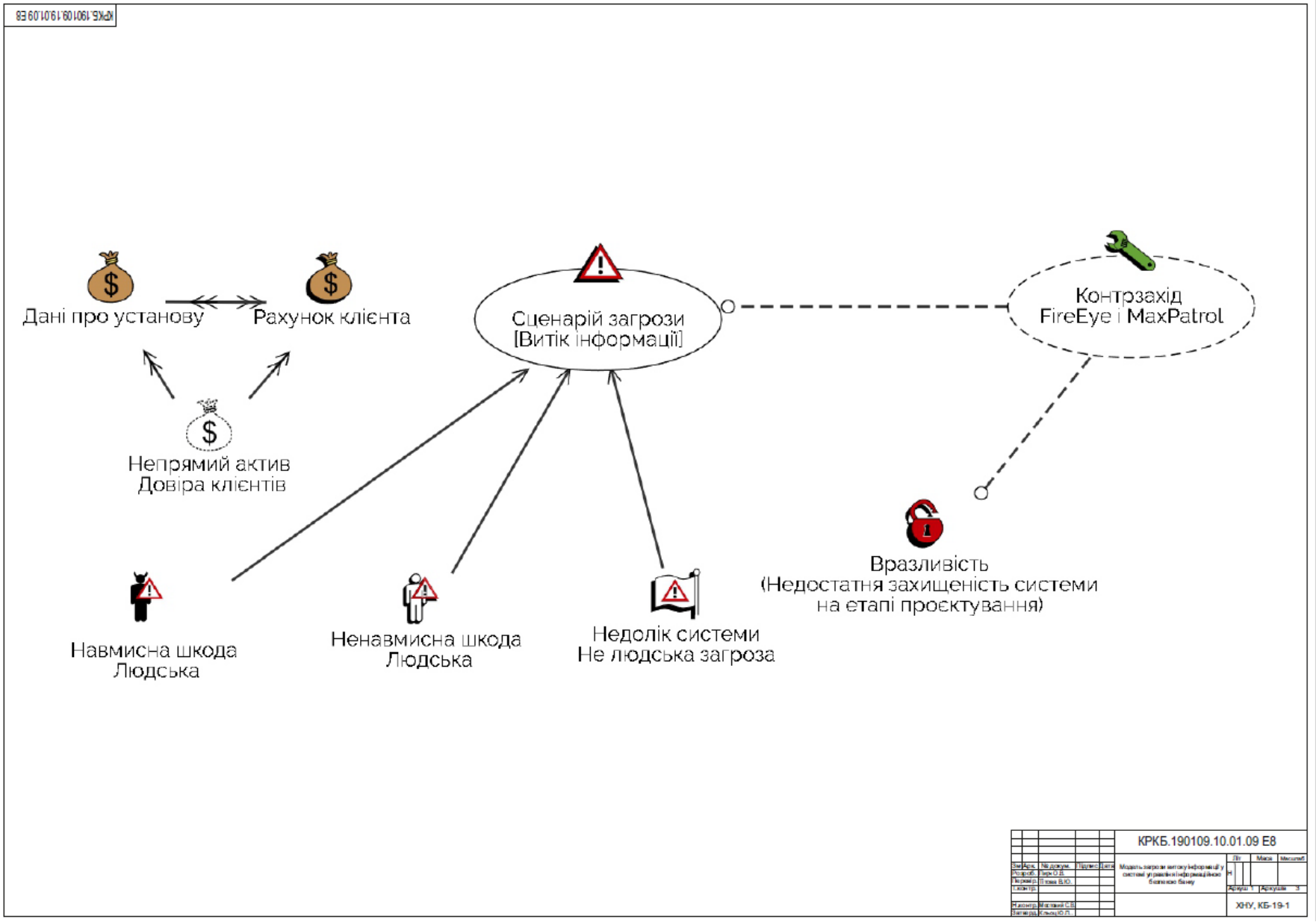
38) How To Improve The Mobile Banking App Security? : https://geniusee.com/single-blog/how-to-improve-the-mobile-banking-app-security (дата звернення 20.05.2023)

39) Information Systems Evolution in the Banking Industry https://studycorgi.com/information-systems-evolution-in-the-banking-industry/#:~:text=In%20connection%20with%20active%20operations,of%20credit%20and%20investment%20operations. (дата звернення 21.05.2023)

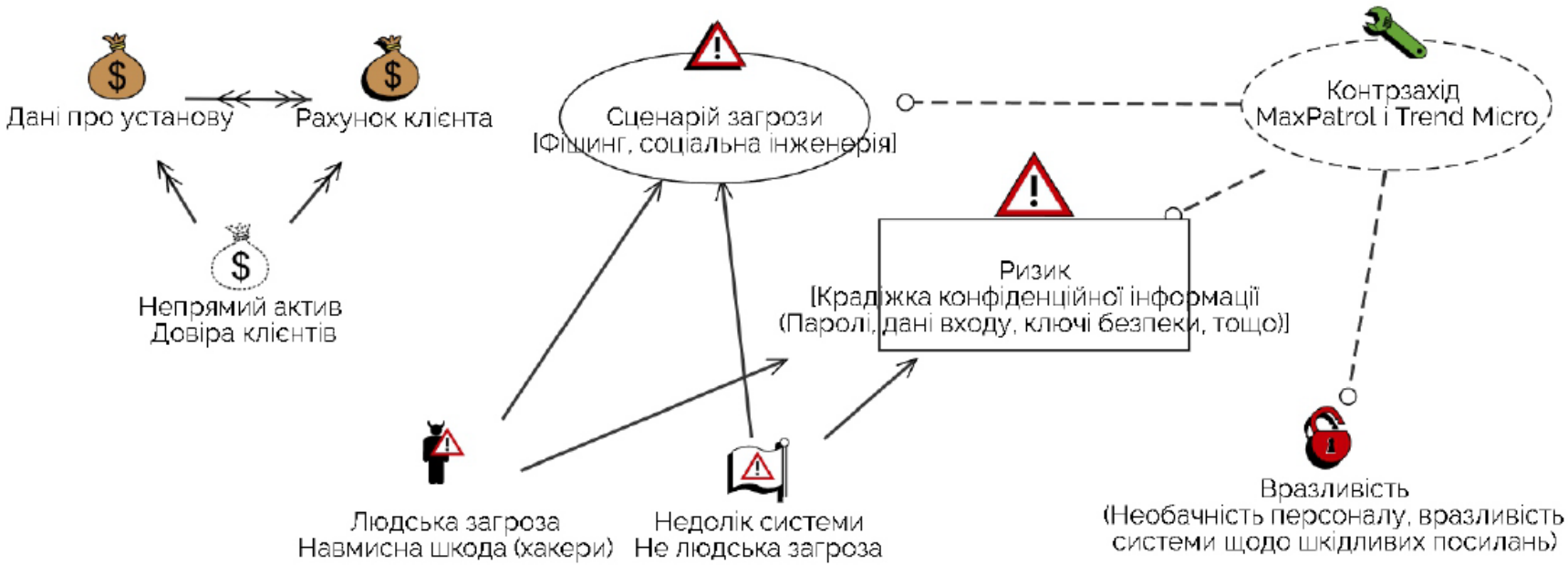
40) Data management in banking : https://learn.microsoft.com/en-us/azure/architecture/industries/finance/data-management-banking-overview (дата звернення 24.05.2023)

Додаток А

Графічна частина

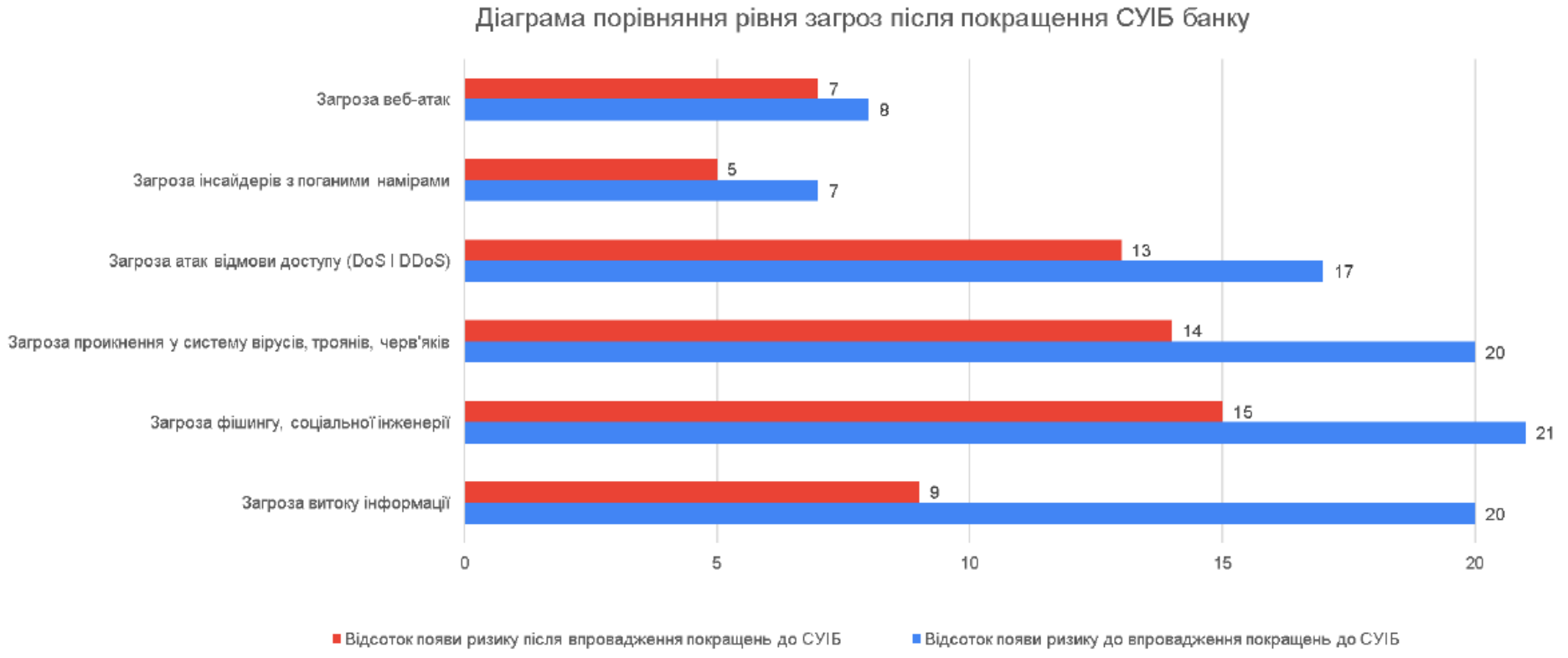


КРКБ.190109.10.01.09 Е8



					КРКБ.190109.10.01.09 Е8		
Зм.	Арк.	№ докум.	Підпис	Дата	Модель загроз фішингу та соціальної інженерії у системі управління інформаційною безпекою банку	Літ.	Маса	Масштаб
Розроб.		Іван О.В.				Н		
Перевір.		Попов В.Ю.						
Н.контр.						Аркуш 2	Аркушів 3	
Н.контр.		Мостовий С.В.				ХНУ, КБ-19-1		
Затверд.		Кільчик О.Л.						

КРКБ.190109.10.01.09 Е8



								КРКБ.190109.10.01.09 Е8	
Зм.	Арк.	№ докум.	Підпис	Дата					
Розроб.		Бєрх О.Д.			Діаграма порівняння рівня загроз у системі до та після покращення системи управління інформаційною безпекою банку		Літ.	Маса	Масштаб
Перевір.		Плаха В.Ю.					Н		
Т.контр.							Аркуш 9	Аркушів 9	
Н.контр.		Мостовий С.В.					ХНУ, КБ-19-1		
Затверд.		Кльоц Ю.Л.							

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 1.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 9%**

	Документ		Сумарний збіг по Базі Даних	
ID: 114648 Назва: Система управління інформаційною безпекою для підвищення ефективності захисту банківських транзакцій в системах інтернет-банкінгу Додано в БД: 2023-06-04 Автора: Пирч О.В. Керівники: Тітова В.Ю. Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	79280	1175	2052 (3%)	27 (2%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

UNICHECK

Ім'я користувача:
Кафедра кібербезпеки

Дата перевірки:
04.06.2023 21:04:39 EEST

Дата звіту:
04.06.2023 21:07:30 EEST

ID перевірки:
1015416603

Тип перевірки:
Doc vs Internet + Library

ID користувача:
100008300

Назва документа: **Пирч**

Кількість сторінок: **70** Кількість слів: **12763** Кількість символів: **99305** Розмір файлу: **2.76 MB** ID файлу: **1015079141**

Виявлено модифікації тексту (можуть впливати на відсоток схожості)

8.98%
Схожість

Найбільша схожість: **1.99%** з джерелом з Бібліотеки (ID файлу: **1011443724**)

8.31% Джерела з Інтернету	643	Сторінка 72
3.67% Джерела з Бібліотеки	223	Сторінка 76

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Підозріле форматування	13 сторінок

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітньо-кваліфікаційного рівня «бакалавр»

Студент Пирч Олена Вадимівна

Тема: «Система управління інформаційною безпекою для підвищення ефективності захисту банківських транзакцій в системах інтернет-банкінгу»

Галузь знань 12 «*Інформаційні технології*» Спеціальність 125 «*Кібербезпека*» Освітня програма «Кібербезпека»

Обсяг дипломної роботи освітньо-кваліфікаційного рівня «бакалавр»: кількість листів креслень 3; кількість сторінок записки 64;

1. Короткий зміст КР та прийнятих рішень Завданням кваліфікаційної роботи було покращення існуючої системи управління інформаційною безпекою, а також впровадження нових рішень, для забезпечення цілісності системи, як комплексної системи захисту від можливих загроз. В роботі використано комплексний підхід к забезпечення інформаційної безпеки комплексний підхід, що є важливим для забезпечення ефективної інформаційної безпеки в банківських установах

2. Висновок про відповідність КР завданню Кваліфікаційна робота у повній мірі відповідає поставленому завданню як в теоретичній так і у практичній частині роботи.

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі обґрунтовується актуальність теми роботи, її зв'язок з галуззю знань «Інформаційні технології» та спеціальністю «Кібербезпека», формулюється мета та основні завдання кваліфікаційної роботи. У першому розділі було проаналізовано і досліджено предметну область, теоретичну інформацію про проєктування систем управління інформаційної безпеки банку та х особливості в зв'язку з вимогами та чинним законодавством.. У другому розділі було спроектовано та реалізовано систему управління інформаційної безпеки банку з ціллю налаштування системи захисту інформації банку від небажаного злому, витоків інформації, загроз атак відмови доступу, фішингу, соціальної інженерії, атак на веб-додатки банку, такі як сайт чи додаток на смартфон. У третьому розділі проведено оцінку ефективності впровадженої системи, розраховано імовірність реалізації загроз після впровадження покращень до системи управління інформаційною системою банку.

4. Позитивні сторони кваліфікаційної роботи полягають у тому, що заявлені і запропоновані завдання та вимоги до системи управління інформаційної безпеки банку виконано у повному обсягу. Розроблена система має широкий простір для подальшого удосконалення, доповнення, розширення та модернізації згідно з вимогами часу.

5. Негативні сторони проекту: у роботі розглянуто не усі можливі загрози, які можуть мати місце в системі інтернет-банкінгу, тому, у випадку практичного використання запропонована система потребує часткового доопрацювання

6. Оцінка графічного оформлення та пояснювальної записки роботи. Графічне оформлення виконане відповідно до теми кваліфікаційної роботи із дотриманням усіх стандартів. У загальному графічне оформлення виконане на достатньому технічному рівні. Пояснювальна записка відповідає нормам для її оформлення та вимогам

7. Відгук про роботу в цілому В загальному кваліфікаційна робота заслуговує позитивної оцінки. Весь матеріал кваліфікаційної роботи структурований, чіткий та послідовний. Усі розділи роботи послідовні та логічні, що дозволяє чітко розуміти викладений матеріал в рамках тематики кваліфікаційної роботи. У пояснювальній записці багато наглядних пояснень. Графічний матеріал дозволяє наочно побачити доцільність та ефективність рішень, які були прийняті за основу для досягнення поставленої задачі проектування.

8. Інші зауваження -

9. Оцінка дипломної роботи Розглянувши позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що робота заслуговує оцінки «добре/ В (4,50)».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи) декан факультету інформаційних технологій, д.т.н., професор Савенко Олег Станіславович

« 5 » червня 2023 . (підпис)

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:
Назва: Система управління інформаційною безпекою для підвищення ефективності захисту банківських транзакцій в системах інтернет-банкінгу

Автор: Пирч Олена Вадимівна

Спеціальність: 125 – Кібербезпека

Освітня програма: освітньо-професійна

Науковий керівник: Тітова Віра Юріївна, к.т.н, доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою Unichek складає 91,02%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism v-15.257 складає 99%.

Згідно з Положенням про дотримання академічної доброчесності в Хмельницькому національному університеті (http://www.khnu.km.ua/root/files/01/10/03/0005.pdf) така авторська робота, обсяг оригінального тексту у відсотках до загального обсягу матеріалу в якій складає 90-100 %, визнається роботою з високою унікальністю тексту.

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1. Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості, складає 8.98%, з яких 1.99% є збігами з одним джерелом, зумовленими наявністю типових фразеологічних виразів предметної області, а також формулюваннями, які утворюють загальновживані фрази.
2. Інші три збіги є збігами в назвах використаних друкованих видань, розміщених в переліку джерел посилань

Керівник роботи _____ В. Ю. Тітова

Завідувач кафедри кібербезпеки _____ Ю. П. Кльоц