

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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

**«Технологія забезпечення кібербезпеки в банківських інформаційних
системах»**

зі спеціальності

125 Кібербезпека та захист інформації

(код, найменування спеціальності)

освітньо-професійної програми

Інформаційна та кібернетична безпека

(назва програми)

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

Владислав КУЧЕРЕНКО

(підпис)

Виконав: здобувач вищої освіти групи БСДМ-62

КУЧЕРЕНКО Владислав

(прізвище, ім'я)

Керівник

канд. техн. наук, доцент

БОРСУКОВСЬКИЙ Юрій

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

Рецензент

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

Київ 2025

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

Кафедра Систем та технологій кібербезпекиСтупінь вищої освіти МагістрСпеціальність 125 Кібербезпека та захист інформаціїОсвітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ

Завідувач кафедри

Систем та технологій
кібербезпеки

Галина ГАЙДУР
“___” жовтня 2025 року

**З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ**

Кучеренку Владиславу Юрійовичу

(прізвище, ім'я)

1. Тема кваліфікаційної роботи: «Технологія забезпечення кібербезпеки в
банківських інформаційних системах.»

керівник кваліфікаційної роботи

**БОРСУКОВСЬКИЙ Юрій канд. техн. наук,
доцент**

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

затверджені наказом Державного університету інформаційно-комунікаційних
технологій від «___» жовтня 2025 року № ____.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 25.12.2025 р.

3. Вихідні дані до кваліфікаційної роботи _____

інформаційні ресурси та інформаційні
системи банківської установи;

архітектура та інфраструктура банківських інформаційних систем;

наукова та технічна література, експлуатаційна документація, нормативні
документи, міжнародні стандарти.

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

1. Дослідження проблеми забезпечення кібербезпеки в банківських інформаційних системах.

2. Аналіз методів та засобів забезпечення кібербезпеки в банківських інформаційних системах.

3. Технологія забезпечення кібербезпеки в банківських інформаційних системах.

4. Перелік графічного матеріалу
Презентація PowerPoint.

6. Дата видачі завдання 01.10.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності проблеми забезпечення кібербезпеки в банківських інформаційних системах.	01.10.2025 р.	
2.	Аналіз наукової та технічної літератури з питань теми кваліфікаційної роботи.	12.10.2025 р.	
3.	Аналіз методів та засобів забезпечення кібербезпеки в банківських інформаційних системах.	27.10.2024 р.	
4.	Технологія забезпечення кібербезпеки в банківських інформаційних системах.	03.11.2025 р.	
5.	Розроблення рекомендацій щодо застосування технології забезпечення кібербезпеки в банківських інформаційних системах.	15.11.2025 р.	
6.	Оформлення результатів дослідження.	26.11.2025 р.	
7.	Подання роботи на плагіат. Підготовка доповіді до захисту.	25.12.2025 р.	

Здобувач вищої освіти

(підпис)

Владислав
КУЧЕРЕНКО

(ім'я, прізвище)

Керівник кваліфікаційної роботи

(підпис)

Юрій
БОРСУКОВСЬКИЙ

(ім'я, прізвище)

ВІДГУК РЕЦЕНЗЕНТА на кваліфікаційну роботу

здобувача КУЧЕРЕНКА Владислава

на тему: «Технологія забезпечення кібербезпеки в
банківських інформаційних системах.»

Актуальність: Сучасні банки впроваджують інформаційні технології для автоматизації фінансових операцій, дистанційного обслуговування клієнтів та підтримки внутрішніх бізнес-процесів. Разом із цим зростає кількість кіберзагроз, спрямованих саме на банківські інформаційні системи, що обробляють конфіденційні дані.

За таких умов питання побудови та впровадження ефективних технологій забезпечення кібербезпеки набуває особливої сенсу оскільки від цього залежить стабільність роботи банківських установ, фінансова безпека та довіра клієнтів. Саме тому обрана тема кваліфікаційної роботи є актуальною та своєчасною.

Позитивні сторони:

1. У роботі ґрунтовно розглянуто проблему забезпечення кібербезпеки банківських інформаційних систем, чітко визначено мету, завдання та основні напрями дослідження.
2. Проаналізовано сучасні методи та засоби забезпечення кібербезпеки, що застосовуються в банківській сфері.
3. Запропоновано технологію забезпечення кібербезпеки банківських інформаційних систем та надано рекомендації щодо її практичного застосування.
4. Матеріал викладено логічно та послідовно, сформульовано обґрунтовані висновки. Перелік використаних джерел свідчить про достатній рівень опрацювання наукової та технічної літератури.

Недоліки:

1. Доцільним було б більш детально продемонструвати застосування запропонованої технології на прикладі конкретної банківської установи.
2. Практичну реалізацію технології бажано було б проілюструвати на прикладі реальної банківської інформаційної системи.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку “**добре**”, а здобувач(ка) **КУЧЕРНКО Владислав** – присвоєння кваліфікації магістр з кібербезпеки за освітньо-професійною програмою інформаційна та кібернетична безпека.

Рецензент:

(науковий ступінь,
вчене звання)

(підпис)

(ім'я, прізвище)

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

**ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ**

Направляється здобувач КУЧЕРЕНКО до захисту кваліфікаційної роботи
Владилсав
(прізвище, ім'я)

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

на тему: «Технологія забезпечення кібербезпеки в
банківських інформаційних системах».

Кваліфікаційна робота і рецензія додаються.

Директор інституту

(підпис)

Свгенія ІВАНЧЕНКО

(ім'я, прізвище)

Висновок керівника кваліфікаційної роботи

Здобувач **КУЧЕРЕНКО Владислав** обрав тему роботи, метою якої було дослідити зміст технології забезпечення безпечної роботи гібридних працівників організації та розробка рекомендацій щодо її реалізації. Перелік використаних джерел свідчить про вміння здобувачем розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи **КУЧЕРЕНКО Владислав** показав добру теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача **КУЧЕРЕНКА Владислав** на оцінку “добре” та присвоїти йому кваліфікацію магістр з кібербезпеки за освітньо-професійною програмою інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи

Юрій
БОРСУКОВСЬКИЙ
(підпис) (ім'я, прізвище)
“ ” 2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач **КУЧЕРЕНКО Владислав** допускається до захисту даної кваліфікаційної роботи в Екзаменаційній комісії.

Завідувач кафедри Систем та технологій кібербезпеки
(назва)

(підпис)

Галина ГАЙДУР

(ім'я, прізвище)

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 67 сторінки, 4 рисунків, 4 таблиці, 16 джерел.

Об'єкт дослідження – забезпечення кібербезпеки банківських інформаційних систем.

Предмет дослідження – технологія забезпечення кібербезпеки в банківських інформаційних системах.

Мета роботи – розробити технологію забезпечення кібербезпеки банківських інформаційних систем та рекомендації щодо її впровадження і застосування.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Банківські інформаційні системи є складними багаторівневими системами, які контролюють отримання, зберігання та передачу фінансової інформації. У контексті тенденції до цифровізації банківського сектора та зростання кіберзагроз необхідно впроваджувати сучасні технології кібербезпеки, щоб забезпечити захист конфіденційності, цілісності та доступності банківських інформаційних ресурсів.

У цій роботі аналізується проблема забезпечення кібербезпеки банківських інформаційних систем, визначаються її мета та завдання. Проведено огляд існуючих підходів і технологій для забезпечення кібербезпеки в банківському секторі.

Далі вивчено методи та засоби захисту банківських інформаційних систем і визначено їх основні функціональні можливості. На основі проведеного дослідження запропоновано технологію забезпечення кібербезпеки банківських інформаційних систем та надано рекомендації для фахівців з кібербезпеки банків щодо їх впровадження та практичного застосування в діяльності банківських установ.

Галузь використання – кібербезпека банківських установ.

БАНКІВСЬКІ ІНФОРМАЦІЙНІ СИСТЕМИ, КІБЕРБЕЗПЕКА,
ІНФОРМАЦІЙНІ РЕСУРСИ БАНКУ, ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ
КІБЕРБЕЗПЕКИ, КІБЕРЗАГРОЗИ

ABSTRACT

Text part of the qualification work: 67 pages, 4 figures, 4 table, 16 sources.

Object of research – ensuring cybersecurity of banking information systems.

Subject of research – the technology for ensuring cybersecurity in banking information systems.

Purpose of the study – to develop a technology for ensuring cybersecurity of banking information systems and to provide recommendations for its implementation and practical application.

Research methods – analysis of scientific literature on the research topic, study of operational documentation, analysis and comparison of international standards.

Banking information systems are complex multi-level systems that control the acquisition, storage, and transmission of financial information. In the context of the digitalization of the banking sector and the growth of cyber threats, it is necessary to implement modern cybersecurity technologies to ensure the confidentiality, integrity, and availability of banking information resources.

This paper analyzes the problem of ensuring cybersecurity of banking information systems and defines its purpose and objectives. An overview of existing approaches and technologies for ensuring cybersecurity in the banking sector is conducted.

Furthermore, methods and tools for protecting banking information systems are examined, and their main functional capabilities are identified. Based on the conducted research, a technology for ensuring cybersecurity of banking information systems is proposed, along with recommendations for cybersecurity specialists of banks regarding its implementation and practical application in banking activities.

Field of application – cybersecurity of banking institutions.

BANKING INFORMATION SYSTEMS, CYBERSECURITY, BANK INFORMATION RESOURCES, CYBERSECURITY TECHNOLOGY, CYBER THREATS

ЗМІСТ

	Стор.
ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ	9
ВСТУП	10
1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В БАНКІВСЬКИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ	12
1.1 Дослідження проблеми забезпечення кібербезпеки в банківських інформаційних системах.....	12
1.2 Аналіз загроз та вразливостей банківських інформаційних систем.....	17
1.3 Аналіз існуючих підходів і рішень із забезпечення кібербезпеки банківських інформаційних систем.....	21
2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В БАНКІВСЬКИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ.....	29
2.1 Призначення та основні функції методів і засобів забезпечення кібербезпеки в банківських інформаційних системах.....	29
2.2 Архітектура системи кібербезпеки банківських інформаційних систем	35
2.3 Методи та засоби реалізації кібербезпеки в банківських інформаційних системах	38
3 ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В БАНКІВСЬКИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ.....	46
3.1 Архітектура технології забезпечення кібербезпеки банківських інформаційних систем.....	46
3.2 Варіанти архітектурних рішень забезпечення кібербезпеки банківських інформаційних систем.....	50
3.3 Технологія впровадження та застосування сучасних підходів до забезпечення кібербезпеки банківських інформаційних систем	55
3.4 Рекомендації щодо впровадження технології забезпечення кібербезпеки банківських інформаційних систем	59
ВИСНОВКИ	65
ПЕРЕЛІК ПОСИЛАНЬ	67
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)	

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

API – Application Programming Interface (інтерфейс програмування застосунків)

APT – Advanced Persistent Threat (розширена стійка кіберзагроза)

BYOD – Bring Your Own Device (використання власних пристроїв у корпоративній мережі)

DNS – Domain Name System (система доменних імен)

DTLS – Datagram Transport Layer Security (протокол захисту датаграмного трафіку)

IaaS – Infrastructure as a Service (інфраструктура як сервіс)

NAC – Network Access Control (контроль доступу до мережі)

NGFW – Next-Generation Firewall (міжмережевий екран нового покоління)

PaaS – Platform as a Service (платформа як сервіс)

SDN – Software Defined Network (програмно визначена мережа)

SDP – Software Defined Perimeter (програмно визначений периметр)

SIEM – Security Information and Event Management (управління подіями та інцидентами інформаційної безпеки)

VPN – Virtual Private Network (віртуальна приватна мережа)

WFA – Work From Anywhere (віддалений формат роботи)

ZT – Zero Trust (модель нульової довіри)

ZTA – Zero Trust Architecture (архітектура нульової довіри)

ZTNA – Zero Trust Network Access (доступ до мережі на основі Zero Trust)

ВСТУП

Актуальність дослідження.

Старий підхід до забезпечення інформаційної безпеки, який ґрунтувався на уявленні про чітко окреслений периметр мережі банківської установи, за якого користувачі та інформаційні ресурси перебувають усередині захищеного середовища, вже не відповідає сучасним умовам функціонування банківських систем. Активна цифровізація банківських послуг, широке використання хмарних технологій, дистанційних каналів обслуговування клієнтів та інтеграція з зовнішніми інформаційними системами суттєво ускладнюють архітектуру банківських інформаційних систем.

Після чого відбувається розмивання традиційного мережевого периметра, що зумовлює необхідність застосування нових підходів до контролю доступу, захисту даних і протидії сучасним кіберзагрозам. За таких умов використання ізольованих засобів захисту, зокрема брандмауерів, захищених веб-шлюзів, систем запобігання втраті даних (DLP) та інших точкових рішень, не завжди забезпечує належний рівень кібербезпеки в складних і динамічних банківських інформаційних системах.

Зростання кількості та складності кібератак, спрямованих на банківські установи, обумовлює потребу у впровадженні комплексних технологій кібербезпеки, здатних забезпечити захист конфіденційності, цілісності та доступності фінансової інформації на всіх рівнях її обробки. Особливого значення набуває розроблення та впровадження ефективних технологій забезпечення кібербезпеки банківських інформаційних систем, що враховують сучасні загрози, регуляторні вимоги та особливості функціонування банківської інфраструктури.

Вищевказане визначає актуальність теми даної кваліфікаційної роботи, основний зміст якої полягає у дослідженні та розробленні технології забезпечення кібербезпеки в банківських інформаційних системах.

Об'єкт дослідження – забезпечення кібербезпеки банківських інформаційних систем.

Предмет дослідження – технологія забезпечення кібербезпеки в банківських інформаційних системах.

Мета роботи – розробити технологію забезпечення кібербезпеки банківських інформаційних систем та рекомендації щодо її впровадження і застосування.

Наукові завдання:

дослідити сутність проблеми забезпечення кібербезпеки банківських інформаційних систем;

проаналізувати сучасні підходи до забезпечення кібербезпеки в банківському секторі;

проаналізувати існуючі технології та рішення із забезпечення кібербезпеки банківських інформаційних систем;

дослідити методи та засоби захисту банківських інформаційних систем;

розкрити порядок реалізації технології забезпечення кібербезпеки банківських інформаційних систем.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Практичне значення одержаних результатів: надає перевагу у використанні запропонованої технології забезпечення кібербезпеки банківських інформаційних систем та розроблених рекомендацій у діяльності фахівців з кібербезпеки банківських установ.

Результати кваліфікаційної роботи апробовані на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 27 жовтня 2023 року в Державному університеті інформаційно-комунікаційних технологій, м. Київ.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В БАНКІВСЬКИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

1.1. Дослідження проблеми забезпечення кібербезпеки в банківських інформаційних системах

Банківські інформаційні системи є важливим компонентом сучасної інфраструктури інформаційних систем в організації інфраструктури сучасних фінансових установ і автоматизують найпоширеніші банківські операції, від управління платіжними транзакціями та рахунками клієнтів, кредитно-депозитними послугами, дистанційними банківськими послугами та підтримкою внутрішнього адміністративного управління та аналізу. Через високий рівень фінансової та особистої інформації, що зберігається в банківських системах, банківська інформаційна система є однією з головних цілей, які експлуатуються хакерами.

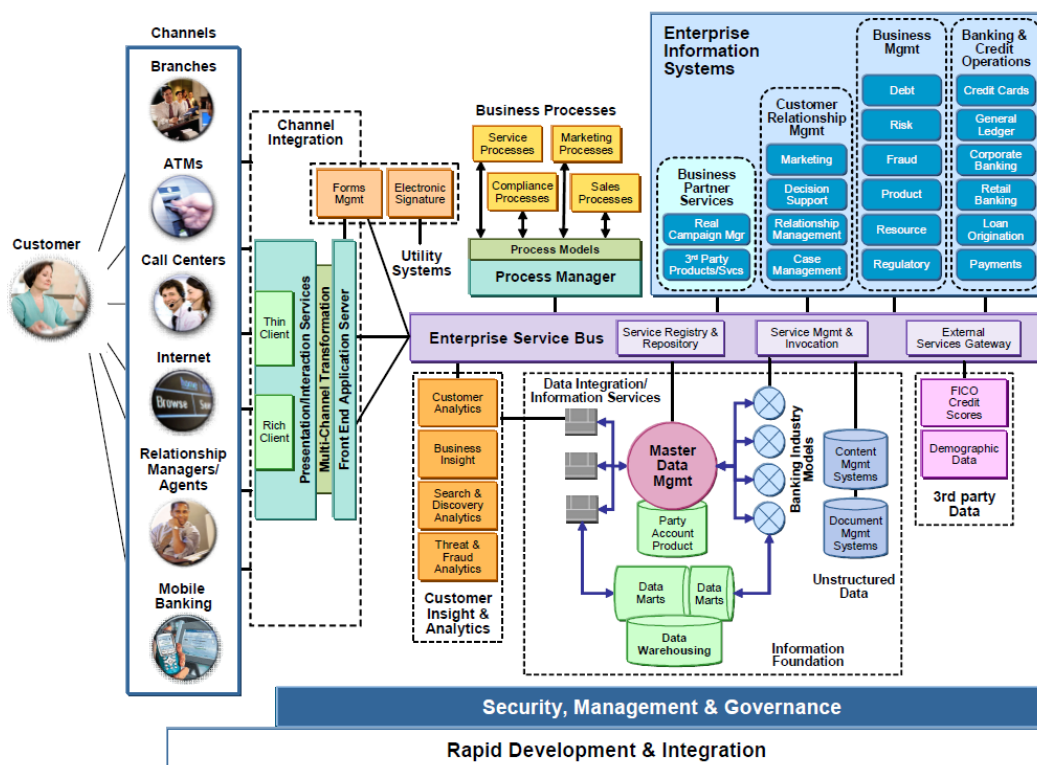


Рис. 1.1. Загальна структура банківської інформаційної системи

З огляду на поточний стан розвитку інформаційних технологій, банківський сектор перебуває в процесі значних змін завдяки цифровізації фінансових послуг, впровадженню хмарних технологій, мобільного та інтернет-банкінгу та інтеграції з зовнішніми платіжними та сервісними провайдерами. Ці зміни не лише сприяють більшому доступу та зручності банківських послуг, але й ускладнюють архітектуру банківських інформаційних систем і значно розширюють потенційний ландшафт кібербезпеки.

Одним з основних викликів для забезпечення кібербезпеки банківських інформаційних систем є втрата чітко визначеного мережевого периметра для захисту інформаційних мереж від атак на систему. Звичайні моделі захисту, які організовані на ідеї внутрішнього середовища, яке є належно довіреним разом із захищеним зовнішнім периметром, не виявляються достатньо ефективними у випадках розподіленої інформаційної системи, віддаленого доступу користувачів та активного використання користувачами хмарних сервісів. Існують середовища атак, де можуть бути прийняті як внутрішні, так і зовнішні вектори атак, що значно ускладнює виявлення та нейтралізацію загроз. На іншому рівні проблема ускладнюється зростаючою кількістю та складністю кіберзагроз для банківських установ.

Існує високий ступінь автоматизації, націленості та складних технічних методів атак у сучасних кібератаках.

Фішингові кампанії, шкідливе програмне забезпечення, атаки відмови в обслуговуванні, компрометація облікових даних та багатоступеневі атаки з акцентом на тривалу приховану присутність в інформаційній системі є різними техніками, які використовуються зловмисниками, спрямованими на подальше компрометування фінансових ресурсів банку.

Помилки персоналу, відсутність обізнаності про порушення кібербезпеки, слабкі методи аутентифікації, а також навмисні зловмисні дії можуть призвести до порушення конфіденційності, цілісності та доступності інформації.

Внутрішні загрози часто є натхненням, де складні кіберзагрози

використовуються як тригер для розгортання складних кібератак, у багатьох випадках ці внутрішні загрози допомагають керувати складними кібератаками.

Організаційні, правові і регуляторні фактори також відіграють значну роль у визначенні статусу загрози в кібербезпеці банківських інформаційних систем. Недостатня формалізація політик інформаційної безпеки, відсутність добре структурованого управління ризиками, відсутність систематичних контролів, нерегулярні аудити безпеки та тестування на проникнення послаблюють надійність технічної безпеки. Крім того, банки зобов'язані дотримуватися національних та міжнародних стандартів конфіденційності в сфері інформаційної безпеки, тому організації повинні постійно вдосконалювати процеси кібербезпеки.

Проблема захисту банківських інформаційних систем від кібератак є багатогранною, з багатовимірною перспективою від технічної, організаційної до регуляторної. Її вирішення вимагає систематичного підходу, заснованого на сучасних технологіях захисту ефективного контролю доступу в поєднанні з моніторингом поточних подій безпеки, підтримкою кібергігієни персоналу.

Перед можливістю надання надійних інфраструктурних рішень для задоволення сучасних вимог та загроз, для визначення ефективної технології для безпеки банківських інформаційних систем є необхідною передумовою.

Окремо слід відзначити, що ускладнення архітектури банківських інформаційних систем призводить до зростання залежності між різними компонентами інформаційної інфраструктури. Порушення безпеки одного з елементів системи може мати каскадний ефект і впливати на функціонування інших сервісів, що ускладнює локалізацію інцидентів та збільшує потенційні наслідки кібератак. У таких умовах традиційні підходи до побудови систем захисту, орієнтовані на окремі технічні засоби, втрачають свою ефективність.

Суттєвим фактором, який посилює проблему кібербезпеки банківських інформаційних систем, є постійна еволюція загроз. Зловмисники активно адаптують свої методи атак до нових технологій захисту, використовуючи автоматизовані інструменти, соціальну інженерію та комбіновані сценарії атак. У результаті навіть добре захищені інформаційні системи можуть залишатися

вразливими за умови відсутності системного та адаптивного підходу до кібербезпеки.

Крім того, складність забезпечення кібербезпеки банківських інформаційних систем зумовлена необхідністю поєднання високого рівня захисту з вимогами до безперервності та доступності банківських послуг. Будь-які збої в роботі інформаційних систем або надмірні обмеження доступу можуть негативно впливати на якість обслуговування клієнтів і репутацію банківської установи. Це вимагає пошуку збалансованих рішень, які забезпечують належний рівень безпеки без шкоди для бізнес-процесів.

У контексті зазначених проблем особливої актуальності набуває питання ефективного контролю доступу до інформаційних ресурсів банку. Саме доступ користувачів і сервісів до критичних даних є одним із найбільш уразливих елементів системи кібербезпеки. Недостатньо формалізовані механізми контролю доступу або надмірна довіра до внутрішніх користувачів створюють передумови для реалізації як зовнішніх, так і внутрішніх загроз.

Вищенаведене обґрунтовує необхідність подальшого аналізу сучасних підходів і методів забезпечення кібербезпеки в банківських інформаційних системах, що буде розглянуто в наступних підрозділах роботи, зокрема під час аналізу існуючих підходів і рішень у сфері захисту банківських інформаційних ресурсів.

Активна цифрова трансформація банківського сектору суттєво змінює підхід до організації та експлуатації банківських інформаційних систем. Впровадження мобільного банкінгу, дистанційного обслуговування клієнтів, інтеграція з фінансово-технологічними платформами та використання відкритих інтерфейсів доступу значно підвищують гнучкість і доступність банківських послуг. Водночас ці процеси призводять до істотного зростання складності інформаційної інфраструктури та створюють нові виклики у сфері кібербезпеки.

Розширення функціональних можливостей банківських інформаційних систем супроводжується збільшенням кількості компонентів, сервісів і точок взаємодії. Кожен додатковий елемент інформаційної системи потенційно може

стати об'єктом кібератаки або джерелом вразливості. У результаті формується багаторівневе середовище, у якому взаємозалежність між компонентами ускладнює як проєктування захисту, так і реагування на інциденти інформаційної безпеки.

Окремої уваги потребує проблема інтеграції банківських інформаційних систем із зовнішніми сервісами та партнерами. Сучасні банки активно взаємодіють із платіжними системами, державними реєстрами, фінансовими агрегаторами та іншими сторонніми організаціями. Такі інтеграції значно розширюють межі інформаційної системи банку та зменшують можливість повного контролю над усіма компонентами середовища. У цьому контексті класичне уявлення про «внутрішню безпечну мережу» втрачає практичне значення.

Додатковим чинником зростання кіберризиків є активне використання віддаленого доступу персоналом банківських установ. Працівники можуть підключатися до інформаційних ресурсів з різних географічних локацій, використовуючи різноманітні пристрої та мережі зв'язку. Це ускладнює контроль умов доступу та підвищує ймовірність використання скомпрометованих або недостатньо захищених кінцевих пристроїв. За таких умов традиційні механізми контролю доступу не завжди дозволяють адекватно оцінити реальний рівень ризику.

Зростання швидкості та обсягів фінансових операцій також впливає на характер загроз кібербезпеки. Банківські інформаційні системи дедалі частіше працюють у режимі реального часу, що скорочує час, доступний для виявлення та реагування на інциденти. Зловмисники, своєю чергою, використовують автоматизовані інструменти та сценарії атак, які дозволяють здійснювати складні кібератаки з мінімальним часовим інтервалом між етапами компрометації.

Важливою проблемою є необхідність підтримання балансу між рівнем безпеки та доступністю банківських послуг. Надмірно жорсткі заходи захисту можуть негативно впливати на ефективність роботи персоналу та знижувати зручність користування сервісами для клієнтів. У той самий час недостатній рівень контролю створює передумови для реалізації кіберзагроз і компрометації

інформаційних ресурсів. Це зумовлює потребу у впровадженні гнучких підходів до забезпечення кібербезпеки, здатних адаптуватися до змін у середовищі.

Окрім технічних аспектів, значний вплив на рівень кібербезпеки мають організаційні фактори. Відсутність чітко сформульованих політик безпеки, недостатня координація між підрозділами та нерегулярне оновлення процедур реагування на інциденти послаблюють загальну стійкість банківських інформаційних систем. У таких умовах навіть сучасні технічні засоби захисту можуть використовуватися неефективно.

Загалом аналіз проблеми забезпечення кібербезпеки банківських інформаційних систем свідчить про те, що традиційні підходи до захисту вже не відповідають сучасним вимогам. Зміна архітектури інформаційних систем, поява нових каналів доступу та динамічний характер кіберзагроз потребують переосмислення підходів до побудови системи безпеки. Це створює передумови для подальшого аналізу сучасних підходів і методів забезпечення кібербезпеки, які враховують контекст доступу, рівень ризику та необхідність постійного контролю взаємодії з інформаційними ресурсами банку.

1.2. Аналіз загроз та вразливостей банківських інформаційних систем

Через дуже важливу роль банківських інформаційних систем у фінансових операціях та обробці великих обсягів власних даних, ці системи постійно перебувають під загрозою різноманітних кіберзагроз. Такі системи, містять багато особистих даних, деякі з яких є конфіденційними, які вразливі до зловмисників, чий інтерес у порушенні потоку банківських операцій може призвести до значних втрат прибутку та поганої репутації банківської діяльності.

У практиці кібербезпеки зазвичай розрізняють зовнішні та внутрішні загрози. Зовнішні загрози - це типи загроз, які здійснюють кіберзлочинці, що виконують атаки в Інтернеті, використовуючи як технічні, так і соціальні інженерні методи, і пов'язані з їхньою діяльністю.

Внутрішні загрози виникають від співробітників банку, які можуть отримати

доступ до інформаційних ресурсів (і, отже, мають доступ до) інформаційних ресурсів лише у випадку, якщо вони здійснюють дію або помилку.



Рис. 1.2. Класифікація загроз та вразливостей банківських інформаційних систем

Найпоширенішими зовнішніми загрозами для банківських інформаційних систем є фішингові атаки, зараження шкідливим програмним забезпеченням та атаки відмови в обслуговуванні. Хоча хакерство є одним з найбільш впливових методів атаки, фішинг все ще вважається найбільш небезпечним методом атаки і найпростішим для осіб, щоб знайти облікові дані, які дозволяють зловмисникам отримати доступ до інформації, незважаючи на відсутність технічного захисту системи.

Шкідливе програмне забезпечення використовується для ексфільтрації фінансових даних, перехоплення платіжних даних або втручання в банківські операції.

Цільові атаки є найнебезпечнішими бо протягом цього періоду зловмисники хочуть залишатися невидимими в інформаційній системі банку протягом тривалого часу. Це може включати ескалацію ієрархічних привілеїв, аналіз внутрішньої інфраструктури та цільові порушення критичних ресурсів. Виявлення таких загроз

є складним завданням і вимагає постійного моніторингу подій безпеки.

У цьому контексті внутрішня загроза зазвичай стосується дотримання безпеки персоналом банку щодо вимог кібербезпеки та дотримання. Просте використання простих або вживаних паролів, передача пароля третій стороні, доступ до конфіденційної інформації також можуть бути пов'язані з витоком даних/відкритою системою без належних порушень безпеки.

Внутрішні загрози іноді розраховані і пов'язані з зловживанням посадою, яку використовує посадова особа (посадовець або функціонер). Існує широкий спектр вразливостей, які можуть розвиватися на різних рівнях, що впливають на профіль безпеки банківських інформаційних систем.

Технічні вразливості пов'язані з помилками конфігурації мережевого обладнання, застарілими програмними системами або недостатньою сегментацією мережі. Програмні вразливості виникають, коли в коді системи додатків є вразливість безпеки або оновлення безпеки встановлюється занадто пізно.

Організаційні вразливості зазвичай викликані нечіткими політиками кібербезпеки, відсутністю управління ризиками та поганим регулярним контролем безпеки.

Людський фактор також стає вирішальним – з хорошими сучасними технологіями для захисту систем, помилки користувачів можуть знищити їхні переваги.

Аналіз загроз і вразливостей вказує на те, що ефективність захисту кібербезпеки банківських інформаційних систем слід підходити не лише через індивідуальні технічні рішення. Необхідно вжити скоординованого підходу, щоб включити як апаратні засоби захисту, що забезпечують підтримку на рівні всієї організації, так і динамічний моніторинг безпеки. Це також є ключем до створення відповідного технологічного підходу для забезпечення кібербезпеки банківських комп'ютерних інформаційних систем.

Практичний аналіз кіберзагроз у банківських інформаційних системах свідчить про те, що більшість сучасних атак реалізуються не одноетапно, а у вигляді послідовного ланцюга дій, спрямованих на поступову компрометацію системи. Зловмисники, як правило, не намагаються одразу отримати повний контроль над інформаційними ресурсами банку, а використовують поетапний

підхід, який дозволяє залишатися непоміченими протягом тривалого часу.

Початковим етапом такої атаки зазвичай є збір інформації про банківську установу та її інформаційну інфраструктуру. Для цього можуть використовуватися відкриті джерела, соціальні мережі, публічні сервіси або технічні відомості, доступні через мережеві інтерфейси. Отримана інформація дозволяє зловмисникам сформулювати уявлення про архітектуру системи, типи використовуваних технологій і потенційні точки входу.

Наступним етапом часто стає отримання початкового доступу до інформаційної системи. Це може відбуватися через фішингові атаки, використання скомпрометованих облікових даних, експлуатацію програмних вразливостей або помилки конфігурації. У банківських інформаційних системах такий доступ може бути обмеженим за правами, однак навіть мінімальний рівень доступу створює передумови для подальшого розвитку атаки.

Після закріплення в системі зловмисники прагнуть розширити свої привілеї та отримати доступ до більш критичних ресурсів. На цьому етапі активно використовуються внутрішні вразливості, недостатня сегментація мережі та надмірні права доступу окремих облікових записів. Відсутність чіткого контролю внутрішніх переміщень у межах інформаційної системи значно полегшує виконання таких дій.

Особливу небезпеку становлять атаки, спрямовані на тривалу приховану присутність у банківській інформаційній системі. У таких випадках зловмисники намагаються мінімізувати свою активність, щоб уникнути виявлення засобами моніторингу. Це дозволяє їм накопичувати інформацію, спостерігати за поведінкою користувачів і готувати більш масштабні атаки на фінансові ресурси банку.

Аналіз загроз також показує тісний взаємозв'язок між різними типами вразливостей. Технічні вразливості часто посилюються організаційними недоліками, такими як відсутність чітких процедур реагування або несвоєчасне

оновлення систем. У свою чергу, людський фактор може стати вирішальним елементом, який дозволяє зловмисникам скористатися вже наявними слабкими місцями в системі захисту.

Наприклад, помилка користувача під час обробки електронного листа може призвести до компрометації облікових даних, після чого технічні вразливості та недостатній контроль доступу створюють умови для подальшого розвитку атаки. За відсутності оперативного виявлення та реагування такі інциденти можуть залишатися непоміченими протягом тривалого часу.

Слід враховувати, що сучасні загрози дедалі частіше мають комбінований характер. Зловмисники використовують одночасно кілька векторів атак, поєднуючи технічні методи з елементами соціальної інженерії. У банківських інформаційних системах це ускладнює процес виявлення загроз, оскільки окремі елементи атаки можуть не викликати підозр при ізольованому розгляді.

Дивлячись на вищевказане, аналіз загроз і вразливостей у банківських інформаційних системах демонструє, що ефективний захист не може базуватися лише на окремих технічних засобах або статичних правилах безпеки. Необхідним є підхід, який дозволяє враховувати динаміку атак, взаємозалежність вразливостей і контекст доступу до інформаційних ресурсів.

Узагальнюючи викладене, можна зробити висновок, що сучасні загрози для банківських інформаційних систем потребують адаптивних механізмів контролю, здатних реагувати на зміну умов функціонування системи та поведінки користувачів. Це створює підґрунтя для подальшого аналізу підходів і рішень із забезпечення кібербезпеки, які спрямовані на подолання зазначених обмежень і враховують особливості сучасного інформаційного середовища.

1.3. Аналіз існуючих підходів і рішень із забезпечення кібербезпеки банківських інформаційних систем

Забезпечення кібербезпеки банківських інформаційних систем традиційно

здійснювалося на основі периметрового підходу, за якого основна увага приділялася захисту мережевої межі банку. У межах такого підходу використовувалися міжмережеві екрани, системи виявлення та запобігання вторгненням, антивірусні засоби, а також контроль доступу до внутрішніх ресурсів. Вважалося, що користувачі та системи всередині корпоративної мережі є довіреними, тоді як зовнішнє середовище розглядалось як потенційно небезпечне.

Такий підхід протягом тривалого часу був ефективним, однак із розвитком цифрових технологій його обмеження стали очевидними. Використання хмарних сервісів, мобільного банкінгу, дистанційної роботи співробітників і інтеграції з зовнішніми системами призвело до того, що банківські інформаційні системи перестали мати чітко визначений мережевий периметр. У цих умовах класичні засоби захисту вже не забезпечують достатнього рівня безпеки, оскільки не враховують сучасні сценарії доступу та нові вектори атак.

Одним із поширених підходів до підвищення рівня захищеності банківських систем стало впровадження багаторівневого захисту, відомого як «захист у глибину». Цей підхід передбачає використання декількох рівнів контролю безпеки, зокрема мережевого, прикладного та користувацького рівнів. Його перевагою є зменшення ймовірності успішної атаки, проте ефективність такого підходу значною мірою залежить від правильності конфігурації та узгодженості між окремими засобами захисту.

Іншим важливим напрямом розвитку рішень із кібербезпеки є застосування систем централізованого моніторингу та аналізу подій безпеки. Такі системи дозволяють збирати інформацію з різних джерел, аналізувати її та виявляти потенційні інциденти. Для банківських установ це особливо важливо, оскільки дає змогу своєчасно реагувати на загрози та мінімізувати наслідки можливих атак. Водночас ефективність таких рішень залежить від якості налаштувань, рівня автоматизації та кваліфікації персоналу.

У сучасних умовах усе більшого поширення набувають підходи, орієнтовані на контроль доступу на основі ідентифікації користувачів і контексту їх дій. Замість довіри до розташування користувача в мережі увага приділяється перевірці його

автентичності, прав доступу та відповідності поточної поведінки встановленим політикам безпеки. Такий підхід дозволяє значно зменшити ризики, пов'язані з компрометацією облікових даних або несанкціонованим доступом до банківських ресурсів.

При аналізі існуючих підходів і рішень свідчить про те, що більшість із них вирішують окремі задачі кібербезпеки, але не завжди забезпечують цілісний і узгоджений захист банківських інформаційних систем. Фрагментарність засобів захисту, складність їх інтеграції та управління, а також залежність від застарілих моделей довіри знижують загальний рівень безпеки.

У зв'язку з цим у банківському секторі зростає потреба в застосуванні сучасних підходів до забезпечення кібербезпеки, які враховують особливості розподілених інформаційних систем, динамічний характер загроз і необхідність постійного контролю доступу. Одним із таких підходів є концепція Zero Trust, яка передбачає відмову від апріорної довіри до будь-якого користувача чи системи та базується на принципі постійної перевірки доступу.

Завдяки чому, результати аналізу існуючих підходів і рішень створюють передумови для обґрунтування доцільності застосування сучасної технології забезпечення кібербезпеки банківських інформаційних систем на основі принципів Zero Trust, що й буде розглянуто в наступних розділах кваліфікаційної роботи.

Таб.1.1 Порівняльна характеристика підходів до забезпечення кібербезпеки банківських інформаційних систем

Підхід до забезпечення кібербезпеки	Основна ідея	Переваги	Недоліки
Периметровий підхід	Захист мережевого периметра банку	Простота реалізації, зрозуміла архітектура	Неефективний у розподілених і хмарних середовищах
Захист у глибину	Багаторівневий захист на різних рівнях	Підвищена стійкість до атак	Складність управління та інтеграції
Контроль доступу на основі ролей	Обмеження доступу за ролями користувачів	Зменшення ризиків несанкціонованого доступу	Не враховує контекст і поведінку користувачів

Контекстно-орієнтований підхід	Оцінка дій користувача та середовища	Гнучкість, краща адаптація до загроз	Потребує складної аналітики
Zero Trust	Постійна перевірка кожного доступу	Високий рівень безпеки, відповідність сучасним вимогам	Складність впровадження

Практичний досвід використання описаних підходів у банківському секторі свідчить про те, що навіть за наявності значної кількості засобів захисту загальний рівень кібербезпеки часто залишається недостатнім. Причиною цього є те, що більшість існуючих рішень розроблялися для умов відносно стабільної мережевої архітектури та передбачуваних сценаріїв доступу. У сучасних банківських інформаційних системах, де доступ здійснюється з різних середовищ і за різних умов, такі припущення більше не відповідають реальності.

Додатковою проблемою є складність управління великою кількістю різнорідних засобів безпеки. Кожен із них може бути ефективним у межах власної функції, однак відсутність єдиного підходу до прийняття рішень щодо доступу та контролю призводить до зростання операційної складності. Це ускладнює адміністрування системи кібербезпеки, підвищує ризик помилок конфігурації та знижує оперативність реагування на інциденти.

Важливо також зазначити, що традиційні підходи до забезпечення кібербезпеки часто недостатньо враховують поведінкові аспекти доступу. Контроль доступу зазвичай базується на статичних правилах, які не змінюються залежно від контексту або поточної ситуації. У результаті система може дозволяти доступ у потенційно ризикованих сценаріях або, навпаки, надмірно обмежувати легітимних користувачів, що негативно впливає на ефективність банківських бізнес-процесів.

Ще одним обмеженням існуючих підходів є їх орієнтація переважно на зовнішні загрози. Внутрішні користувачі банківських інформаційних систем часто розглядаються як довірені, що створює значні ризики у випадку компрометації облікових даних або зловмисних дій персоналу. З огляду на це сучасні рішення повинні забезпечувати однаковий рівень контролю для всіх користувачів,

незалежно від їхнього статусу або місця знаходження.

При аналізі існуючих підходів і рішень показує, що подальший розвиток систем кібербезпеки банківських інформаційних систем має бути спрямований на подолання зазначених обмежень. Особливої актуальності набувають підходи, які дозволяють реалізувати безперервний контроль доступу, враховувати контекст і динамічно реагувати на зміну умов функціонування інформаційних систем.

Саме в цьому напрямі формується концепція Zero Trust, яка поєднує ідеї контекстно-орієнтованого доступу, мінімізації довіри та постійної перевірки безпеки. Результати проведеного аналізу створюють логічне підґрунтя для обґрунтування доцільності застосування технології забезпечення кібербезпеки банківських інформаційних систем на основі принципів Zero Trust, детальний розгляд якої здійснюється в наступних розділах кваліфікаційної роботи.

Практика використання існуючих підходів до забезпечення кібербезпеки в банківських інформаційних системах показує, що більшість із них формувалася в умовах відносно стабільної та замкненої інформаційної інфраструктури. У таких умовах ключовою задачею було захистити мережевий периметр і мінімізувати ризики зовнішніх вторгнень. Проте сучасні умови функціонування банківських установ суттєво відрізняються від середовища, у якому формувалися класичні моделі безпеки.

Однією з найголовніших проблем традиційних підходів є їх фрагментарність. Банківські установи часто використовують велику кількість окремих засобів захисту, кожен із яких вирішує вузьке коло задач. Міжмережеві екрани, антивірусні системи, засоби контролю доступу, системи моніторингу подій безпеки та інші компоненти функціонують як незалежні елементи, інтеграція між якими є обмеженою. У результаті формується складна екосистема засобів захисту, управління якою потребує значних ресурсів і високої кваліфікації персоналу.

Використання багаторівневого захисту, хоча й підвищує загальний рівень стійкості інформаційної системи, не завжди гарантує своєчасне виявлення складних атак. У багатьох випадках кожен окремий засіб захисту аналізує події у межах власного контексту, що ускладнює виявлення комплексних сценаріїв атак,

розтягнутих у часі. Для банківських інформаційних систем це створює ситуацію, коли окремі ознаки атаки не викликають підозр, але в сукупності можуть свідчити про серйозну загрозу.

Додатковим не менш важливим суттєвим обмеженням існуючих підходів є залежність від статичних правил і заздалегідь визначених політик доступу. Такі правила часто формуються на основі ролей користувачів або їх приналежності до певного сегмента мережі. У сучасних умовах, коли користувачі можуть змінювати місце роботи, використовувати різні пристрої та канали доступу, статичні моделі доступу не дозволяють адекватно враховувати контекст взаємодії з інформаційними ресурсами.

Особливо гостро проблема проявляється у випадках компрометації облікових даних. Традиційні підходи часто не здатні відрізнити легітимний доступ користувача від доступу, здійсненого зловмисником із використанням тих самих облікових даних. За відсутності аналізу поведінкових та контекстних факторів система безпеки розглядає такі дії як допустимі, що значно підвищує ризики внутрішніх загроз.

Складність інтеграції різних засобів захисту також створює так званий «технічний борг» у сфері кібербезпеки банківських установ. З часом інфраструктура безпеки стає перевантаженою застарілими рішеннями, які важко модернізувати або замінити без ризику порушення стабільності роботи інформаційних систем. Це обмежує можливості оперативного впровадження нових підходів і технологій захисту.

Централізовані системи моніторингу та аналізу подій безпеки значною мірою покращують ситуацію, проте і вони мають свої обмеження. Ефективність таких систем напряму залежить від повноти зібраних даних, якості кореляційних правил і рівня автоматизації процесів реагування. У реальних умовах значна частина аналізу залишається на рівні експертної оцінки фахівців з кібербезпеки, що ускладнює масштабування процесів захисту.

Новітні підходи до контролю доступу, орієнтовані на ідентичність користувача, є важливим кроком уперед порівняно з периметровими моделями.

Проте навіть такі рішення часто реалізуються у вигляді окремих компонентів, які не забезпечують комплексного управління ризиками доступу. За відсутності єдиного механізму оцінки ризику кожної сесії доступу прийняття рішень залишається частково суб'єктивним і залежним від попередньо заданих правил.

У результаті аналізу, можна зробити висновок, що більшість існуючих підходів і рішень у сфері кібербезпеки банківських інформаційних систем мають обмежену адаптивність і не повною мірою відповідають вимогам сучасного цифрового середовища. Вони здатні забезпечувати базовий рівень захисту, проте не завжди ефективно протидіють складним, багатоетапним атакам та внутрішнім загрозам.

Саме ці обмеження зумовлюють необхідність переходу до сучасних концепцій кібербезпеки, які базуються на відмові від апріорної довіри, постійному контролі доступу та оцінці ризиків у реальному часі. Такий підхід дозволяє подолати недоліки традиційних моделей і створює основу для побудови цілісної технології забезпечення кібербезпеки банківських інформаційних систем, орієнтованої на сучасні виклики та загрози.

Висновки про пророблену у першому розділі кваліфікаційної роботи: було досліджено проблему забезпечення кібербезпеки в банківських інформаційних системах у сучасних умовах цифровізації фінансового сектору. Аналіз показав, що банківські інформаційні системи є складними багаторівневими структурами, які обробляють значні обсяги фінансової та персональної інформації, що робить їх одними з найбільш привабливих цілей для кібератак.

У ході розгляду основних загроз і вразливостей встановлено, що кіберризики для банківських установ мають комплексний характер і охоплюють технічні, програмні, організаційні та людські фактори. Втрата чітко визначеного мережевого периметра, активне використання віддаленого доступу та хмарних сервісів суттєво ускладнюють застосування традиційних підходів до захисту інформаційних ресурсів. Аналіз існуючих підходів і рішень у сфері кібербезпеки банківських інформаційних систем засвідчив, що більшість із них зосереджуються на вирішенні окремих задач захисту та не забезпечують цілісного й узгодженого підходу до

управління доступом і реагування на загрози. Фрагментарність захисних механізмів та орієнтація на застарілі моделі довіри знижують ефективність таких рішень у сучасному середовищі. Отримані результати підтверджують необхідність пошуку та обґрунтування сучасної технології забезпечення кібербезпеки банківських інформаційних систем, яка враховує динамічний характер загроз, особливості розподілених архітектур і потребу в постійному контролі доступу.

2. АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В БАНКІВСЬКИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

2.1 Призначення та основні функції методів і засобів забезпечення кібербезпеки в банківських інформаційних системах

Методи та засоби впровадження кібербезпеки в банківських інформаційних системах є вирішальними для захисту інформаційних ресурсів банківських установ та підтримки стабільності функціонування їхніх інформаційних мереж. У сучасних умовах банківська індустрія значною мірою залежить від надійності інформаційних систем, оскільки практично всі основні функції банку пов'язані з їх роботою.

Діяльність банківських установ базується на використанні інформаційних систем, через які здійснюються фінансові транзакції, обслуговування клієнтів та підтримка внутрішніх бізнес-процесів. Порух функціонування таких систем становить суттєвий ризик для банку, оскільки може призводити не лише до прямих фінансових втрат, а й до зниження довіри клієнтів та виникнення репутаційних проблем. Особливо це актуально в умовах сучасного технологічно орієнтованого бізнес-середовища.

Методи та інструменти кібербезпеки в основному розробляються для забезпечення захисту інформаційних активів банку від несанкціонованого доступу, навмисного або випадкового спотворення, втрати чи знищення даних. При цьому рівень захисту має бути збалансований із зручністю використання інформаційних систем, оскільки надмірно жорсткі обмеження можуть негативно впливати на ефективність роботи персоналу та якість банківських продуктів і послуг.

Однією з основних функцій інструментів кібербезпеки є обмеження доступу до інформаційних систем, пов'язаних з банківською діяльністю. Контроль доступу включає ідентифікацію користувача, його автентифікацію та налаштування авторизації відповідно до наданих прав у системі. У банківській сфері це має

особливе значення, оскільки різні типи інформації доступні різним групам працівників і клієнтів.

У разі неправильного налаштування механізмів доступу можливе розкриття конфіденційних даних або виконання несанкціонованих операцій. Саме тому контроль доступу є одним із ключових елементів забезпечення кібербезпеки банківських інформаційних систем.

Важливим завданням методів і засобів кібербезпеки є захист мережевої інфраструктури банку. Банківські інформаційні системи, як правило, мають складну багаторівневу архітектуру, що включає внутрішні корпоративні мережі, центри обробки даних, зовнішні комунікаційні канали, хмарну інфраструктуру та засоби віддаленого доступу. Мережева безпека зосереджена на контролі трафіку, сегментації мережі, управлінні мережевими з'єднаннями та захисті від мережових атак.

Окрему увагу в банківських інформаційних системах приділяють захисту передавання даних. Для цього застосовуються надійні механізми шифрування, які використовуються під час передавання фінансової інформації між компонентами системи, а також між банком і клієнтами. Це дозволяє захистити чутливі дані навіть у разі перехоплення трафіку зловмисниками та зменшити ризики розкриття платіжної та персональної інформації.

Ще однією важливою функцією методів та інструментів кібербезпеки є виявлення та реагування на інциденти інформаційної безпеки. У реальних умовах повністю усунути всі загрози неможливо, тому ключовим завданням є своєчасне виявлення підозрілої активності та оперативне реагування на неї. Для банківських установ це означає можливість швидко ідентифікувати інцидент, локалізувати його, мінімізувати наслідки та відновити нормальну роботу інформаційних систем у найкоротші строки.

Значну роль відіграють також методи та засоби захисту прикладних систем, які безпосередньо забезпечують надання банківських послуг. До таких систем належать платіжні шлюзи, системи дистанційного банкінгу та внутрішні автоматизовані банківські системи. Їх захист передбачає контроль доступу до

функціональних можливостей, перевірку коректності виконання операцій та запобігання експлуатації вразливостей програмного забезпечення.

Ключовим аспектом управління кібербезпекою є моніторинг і аудит подій безпеки. Постійне спостереження за діями користувачів і станом інформаційних систем дозволяє своєчасно виявляти інциденти та оцінювати ефективність застосованих заходів захисту. Для банківських установ аудит подій безпеки також має важливе значення з точки зору дотримання нормативних вимог і внутрішніх політик безпеки.

Важливо зазначити, що методи та інструменти кібербезпеки в банківських інформаційних системах повинні застосовуватися комплексно. Окремі, неузгоджені між собою засоби захисту не забезпечують належного рівня безпеки. Лише поєднання технічних, організаційних і процедурних заходів дозволяє створити стійку систему кібербезпеки, здатну адаптуватися до змін у середовищі загроз.

Окрім визначення базових методів і засобів захисту, у банківських інформаційних системах особливе значення має узгодженість процесів кібербезпеки з управлінням ризиками на рівні організації. У цьому контексті методи забезпечення кібербезпеки повинні підтримувати безперервний цикл ідентифікації загроз, оцінювання ризиків, вибору заходів реагування та контролю їх ефективності. Такий підхід дозволяє не лише реагувати на вже відомі загрози, а й завчасно адаптувати систему захисту до потенційних змін у загрозовому середовищі.

Ключовою є також інтеграція методів кібербезпеки з процесами управління життєвим циклом інформаційних систем. Захисні заходи повинні враховувати етапи проєктування, впровадження, експлуатації та виведення з експлуатації банківських інформаційних систем. Це дозволяє мінімізувати ризики, пов'язані з появою нових вразливостей у процесі модернізації або масштабування інформаційної інфраструктури.

Додатково слід зазначити, що ефективність методів забезпечення кібербезпеки значною мірою залежить від рівня їх формалізації та документування.

Наявність чітко визначених процедур, регламентів і політик забезпечує однакове трактування вимог безпеки всіма учасниками процесу та зменшує ймовірність помилок у реалізації захисних заходів. У банківських установах це особливо важливо з огляду на складну організаційну структуру та значну кількість користувачів інформаційних систем.

Крім того, методи та засоби забезпечення кібербезпеки в банківських інформаційних системах повинні розглядатися не лише як набір окремих технічних рішень, а як частина цілісної системи управління ризиками та безпекою. Саме така інтегрована модель створює передумови для побудови ефективної архітектури кібербезпеки, яка буде детальніше розглянута в наступних підрозділах роботи.

Таб.2.1

Функція	Призначення	Приклад реалізації в банківських інформаційних системах	Результат застосування
Контроль доступу	Обмеження доступу до інформаційних ресурсів відповідно до ролей користувачів	Автентифікація користувачів, рольовий розподіл прав доступу	Зменшення ризику несанкціонованого доступу
Захист мережевої інфраструктури	Запобігання мережевим атакам і проникненню у внутрішню мережу	Фільтрація трафіку, сегментація мережі, контроль міжмережових з'єднань	Підвищення стійкості мережі до атак
Захист передавання даних	Забезпечення конфіденційності інформації під час передавання	Шифрування каналів зв'язку між компонентами системи	Захист фінансових і персональних даних
Захист прикладних систем	Запобігання несанкціонованому доступу до банківських сервісів	Контроль доступу до функцій систем дистанційного банкінгу	Зменшення ризиків компрометації прикладних систем

Виявлення інцидентів	Своєчасне виявлення підозрілої активності	Аналіз подій безпеки, контроль аномальної поведінки	Скорочення часу реагування на інциденти
Реагування на інциденти	Мінімізація наслідків кіберінцидентів	Блокування доступу, ізоляція скомпрометованих компонентів	Зниження фінансових і репутаційних втрат
Моніторинг та аудит	Контроль стану безпеки та дотримання політик	Реєстрація подій доступу та операцій користувачів	Підвищення прозорості та керованості безпеки

У сучасних умовах кібербезпека банківських інформаційних систем перестає бути виключно технічним завданням і дедалі більше розглядається як невід’ємна складова загальної стратегії управління ризиками банківської установи. Функції кібербезпеки безпосередньо пов’язані з фінансовою стійкістю банку, безперервністю його операційної діяльності та збереженням довіри клієнтів. Будь-яке порушення роботи інформаційних систем може мати не лише технічні, а й значні економічні та репутаційні наслідки.

Однією з ключових у системі кібербезпеки є забезпечення стабільності банківських бізнес-процесів. Банківські операції здійснюються у режимі реального часу, а зупинка або уповільнення роботи інформаційних систем може призвести до затримок платежів, втрати клієнтів та порушення договірних зобов’язань. У цьому контексті кібербезпека виконує не лише захисну, а й підтримувальну функцію, забезпечуючи безперервність роботи критично важливих сервісів.

Дуже важливим призначенням кібербезпеки є захист фінансових активів банку від прямих і непрямих втрат. Кібератаки можуть бути спрямовані як на викрадення коштів, так і на маніпулювання даними, що використовуються для прийняття фінансових рішень. Навіть незначні зміни в облікових або транзакційних даних можуть призвести до серйозних фінансових наслідків, якщо вони залишаються непоміченими протягом тривалого часу.

Функції кібербезпеки також тісно пов’язані з питаннями довіри клієнтів до банківських установ. У сучасному цифровому середовищі клієнти очікують не

лише зручних, а й безпечних фінансових сервісів. Інформація про витік персональних даних або компрометацію банківських систем швидко поширюється та може суттєво вплинути на репутацію банку. У цьому сенсі кібербезпека виконує роль інструменту підтримання іміджу та конкурентоспроможності банківської установи.

Окремою функцією кібербезпеки є забезпечення відповідності регуляторним і нормативним вимогам. Банківський сектор належить до найбільш регульованих сфер діяльності, де вимоги до захисту інформації визначаються національними та міжнародними стандартами. Система кібербезпеки повинна не лише запобігати інцидентам, а й забезпечувати можливість аудиту, контролю доступів і фіксації дій користувачів. Це дозволяє банкам підтверджувати дотримання вимог регуляторів та зменшувати ризики застосування санкцій.

Значну роль у системі кібербезпеки відіграє функція раннього виявлення загроз. Своєчасна ідентифікація підозрілої активності дозволяє зменшити масштаби інцидентів та запобігти їх ескалації. Для банківських інформаційних систем це особливо важливо, оскільки навіть короткочасна присутність зловмисника в системі може призвести до значних втрат. У цьому контексті кібербезпека виконує превентивну функцію, спрямовану на зниження ймовірності реалізації атак.

Функції кібербезпеки також охоплюють підтримку процесів управління доступом до інформаційних ресурсів банку. В умовах розподілених систем і віддаленої роботи персоналу контроль доступу стає складним багатовимірним завданням. Необхідно враховувати не лише роль користувача, а й контекст доступу, характер виконуваних операцій та поточний стан інформаційного середовища. Це потребує використання більш гнучких і адаптивних механізмів керування доступом.

Ще одним важливим призначенням кібербезпеки є підтримка процесів реагування на інциденти та відновлення після них. Навіть за наявності ефективних захисних механізмів повністю виключити можливість інцидентів неможливо. Тому система кібербезпеки повинна забезпечувати не лише виявлення та локалізацію

загроз, а й швидке відновлення працездатності інформаційних систем. Для банків це означає мінімізацію простоїв і збереження безперервності обслуговування клієнтів.

Слід також відзначити роль кібербезпеки у формуванні культури безпеки в банківських установах. Технічні засоби захисту є ефективними лише за умови належного рівня обізнаності персоналу. Функції кібербезпеки включають розробку процедур, інструкцій і рекомендацій, спрямованих на зменшення ризиків, пов'язаних із людським фактором. У цьому сенсі кібербезпека виступає не лише як технологічна, а й як організаційна функція.

Узагальнюючи викладене, можна зробити висновок, що призначення та функції кібербезпеки банківських інформаційних систем мають комплексний характер і охоплюють технічні, організаційні та управлінські аспекти. Система кібербезпеки повинна забезпечувати захист інформаційних ресурсів, підтримувати стабільність бізнес-процесів, відповідати регуляторним вимогам і адаптуватися до змін у середовищі загроз. Саме така багатофункціональність створює основу для подальшого аналізу архітектурних рішень і методів реалізації кібербезпеки, які розглядаються в наступних підрозділах роботи.

2.2 Основні компоненти та архітектура систем забезпечення кібербезпеки в банківських інформаційних системах

У процесі проєктування архітектури систем забезпечення кібербезпеки в банківських інформаційних системах особливу увагу приділяють питанням масштабованості та гнучкості. Банківські установи постійно розширюють спектр своїх послуг, впроваджують нові цифрові канали взаємодії з клієнтами та інтегруються з зовнішніми фінансовими й сервісними платформами. У таких умовах система кібербезпеки повинна бути здатною адаптуватися до змін без необхідності повної перебудови архітектури.

Важливим аспектом архітектури є розподіл функцій кібербезпеки між різними рівнями системи. Частина функцій реалізується безпосередньо на

мережевому рівні, інші — на рівні прикладних сервісів або користувацьких пристроїв. Такий розподіл дозволяє зменшити навантаження на окремі компоненти системи та підвищити загальну стійкість до відмов і атак. Крім того, багаторівнева архітектура спрощує локалізацію інцидентів і мінімізує їх вплив на роботу всієї банківської інформаційної системи.

Окрему роль в архітектурі систем кібербезпеки відіграє управління ідентифікацією та доступом користувачів. У сучасних банківських інформаційних системах користувачами є не лише співробітники банку, але й клієнти, партнери та зовнішні сервіси. Це ускладнює процеси контролю доступу та вимагає застосування більш гнучких і контекстно-орієнтованих механізмів автентифікації та авторизації.

Не менш важливим є питання інтеграції засобів кібербезпеки з існуючими інформаційними системами банку. У більшості випадків банківські установи експлуатують різноманітні інформаційні системи, створені в різні періоди та з використанням різних технологій. Архітектура системи кібербезпеки повинна забезпечувати сумісність із такими системами та підтримувати централізоване управління політиками безпеки без порушення роботи основних банківських сервісів.

Значний вплив на архітектуру систем кібербезпеки має також необхідність дотримання регуляторних і нормативних вимог. Банківські установи зобов'язані виконувати вимоги національного та міжнародного законодавства у сфері захисту інформації, що передбачає ведення журналів подій, забезпечення контролю доступу, резервне копіювання та можливість проведення аудитів. Це обумовлює включення до архітектури спеціалізованих компонентів, орієнтованих на забезпечення відповідності нормативним вимогам.

Крім того, сучасні архітектури систем кібербезпеки дедалі частіше враховують поведінкові аспекти роботи користувачів і систем. Аналіз поведінки дозволяє виявляти відхилення від нормальної діяльності, що може свідчити про потенційні загрози або компрометацію облікових даних. Включення таких механізмів до архітектури підвищує ефективність виявлення складних і

прихованих атак.

ТВарто зазначити, що при побудові архітектури систем забезпечення кібербезпеки в банківських інформаційних системах особливу увагу приділяють принципу розмежування доступу до ресурсів. Банківські системи обробляють різні типи інформації, що відрізняються за рівнем критичності та вимогами до захисту. Тому архітектура системи кібербезпеки повинна передбачати чіткий поділ ресурсів і сервісів за рівнями доступу, що дозволяє мінімізувати наслідки можливого компрометування окремих компонентів.

Важливим елементом архітектури є взаємодія між компонентами системи кібербезпеки та основними банківськими інформаційними системами. Захисні механізми не повинні працювати ізольовано, а мають бути інтегровані в загальну інформаційну інфраструктуру банку. Це дозволяє забезпечити єдину політику безпеки, централізоване управління доступом та узгоджене реагування на інциденти, що є особливо важливим для великих банківських установ із розгалуженою мережею підрозділів.

Окрему роль в архітектурі систем забезпечення кібербезпеки відіграє управління життєвим циклом користувачів і їхніх облікових записів. У банківських установах постійно відбуваються зміни в штаті персоналу, ролях і посадових обов'язках співробітників. Архітектура системи кібербезпеки повинна забезпечувати оперативне надання, зміну або відкликання прав доступу відповідно до поточного статусу користувача. Недотримання цих вимог може призводити до накопичення надмірних прав доступу та зростання ризиків внутрішніх загроз.

Значний вплив на архітектуру систем кібербезпеки має необхідність забезпечення високої доступності банківських інформаційних систем. Банківські сервіси повинні працювати безперервно, оскільки навіть короточасні збої можуть негативно впливати на фінансову діяльність банку та рівень довіри клієнтів. У зв'язку з цим архітектура захисних систем має передбачати резервування ключових компонентів, використання відмовостійких рішень та можливість швидкого відновлення працездатності у разі виникнення інцидентів.

Не менш важливим є врахування особливостей взаємодії банківських

інформаційних систем із зовнішніми контрагентами та сервісами. Сучасні банки активно співпрацюють з платіжними системами, фінтех-компаніями, державними інформаційними ресурсами та іншими організаціями. Це вимагає включення до архітектури систем кібербезпеки механізмів захисту зовнішніх інтерфейсів, контролю взаємодії через програмні інтерфейси та постійного моніторингу зовнішніх з'єднань.

Архітектура систем забезпечення кібербезпеки також повинна враховувати потребу в аналітичній обробці великих обсягів даних про події безпеки. У банківських інформаційних системах щоденно генерується значна кількість подій, пов'язаних із доступом до ресурсів, виконанням транзакцій і роботою прикладних систем. Ефективна архітектура має забезпечувати збирання, зберігання та аналіз цих даних з метою виявлення закономірностей, аномалій і потенційних загроз.

Крім того, сучасні архітектури систем кібербезпеки дедалі частіше орієнтуються на використання автоматизованих механізмів прийняття рішень. Автоматизація дозволяє скоротити час реагування на інциденти, зменшити навантаження на персонал і підвищити загальну ефективність захисту. Водночас архітектура повинна передбачати можливість контролю та втручання з боку фахівців з кібербезпеки у критичних ситуаціях.

Узагальнюючи, можна зазначити, що архітектура систем забезпечення кібербезпеки в банківських інформаційних системах є складною багатокомпонентною структурою, яка повинна враховувати технічні, організаційні та регуляторні вимоги. Її побудова потребує системного підходу та постійного вдосконалення відповідно до змін у банківській діяльності та середовищі кіберзагроз.

2.3 Порядок функціонування методів і засобів забезпечення кібербезпеки в банківських інформаційних системах

Порядок функціонування методів і засобів забезпечення кібербезпеки в банківських інформаційних системах базується на принципі безперервного та

комплексного захисту інформаційних ресурсів банку. У сучасних умовах кібербезпека не є окремою функцією, а інтегрується в усі процеси обробки, зберігання та передавання інформації. Це означає, що система захисту повинна працювати постійно, незалежно від режимів експлуатації банківських інформаційних систем.

Функціонування системи кібербезпеки починається з процесів ідентифікації та автентифікації користувачів. Кожна спроба доступу до інформаційних ресурсів банку супроводжується перевіркою облікових даних користувача, його прав доступу та відповідності встановленим політикам безпеки. У сучасних банківських інформаційних системах дедалі частіше враховується контекст доступу, зокрема тип пристрою, місце підключення та характер виконуваних операцій, що дозволяє зменшити ризики несанкціонованого доступу.

Після успішної автентифікації здійснюється авторизація, яка визначає перелік дозволених дій користувача в межах інформаційної системи. У банківській сфері це має критичне значення, оскільки доступ до фінансових операцій, персональних даних клієнтів і внутрішніх сервісів повинен бути чітко регламентований. У разі виявлення відхилень від типової поведінки користувача система може автоматично ініціювати додаткові перевірки або обмежувати доступ до окремих функцій.



Рис. 2.1. Загальна схема функціонування системи кібербезпеки банківської інформаційної системи

Захист мережевих з'єднань є наступним етапом у порядку функціонування системи кібербезпеки. Усі інформаційні потоки між компонентами банківської системи, а також між банком і зовнішніми користувачами, підлягають контролю та аналізу. Засоби мережевої безпеки виконують фільтрацію трафіку, виявлення аномальної активності та блокування потенційно небезпечних з'єднань.

Паралельно із захистом мережі здійснюється контроль роботи прикладних систем і захист даних. Банківські додатки обробляють критично важливу інформацію, тому всі операції перевіряються на відповідність встановленим правилам безпеки. У разі виявлення підозрілих дій або спроб несанкціонованого доступу система може автоматично застосовувати обмежувальні заходи.

Важливою складовою порядку функціонування системи кібербезпеки є постійний моніторинг подій безпеки. Інформація про дії користувачів, мережеві з'єднання та роботу прикладних компонентів збирається, аналізується та зберігається для подальшого використання. Це дозволяє своєчасно виявляти інциденти та реагувати на них.

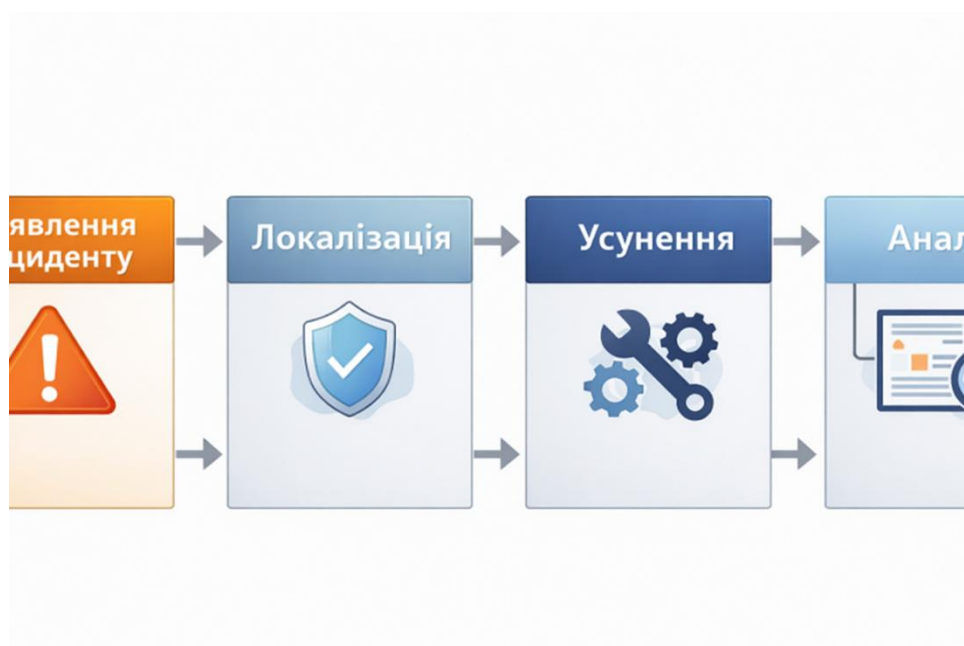


Рис. 2.2. Загальна схема функціонування системи кібербезпеки банківської інформаційної системи

Однією з ключових вимог до архітектури кібербезпеки є її багаторівневність. Захист банківських інформаційних систем не може бути ефективним у разі реалізації лише на одному рівні, наприклад, мережевому або прикладному. Архітектура повинна охоплювати мережеву інфраструктуру, серверні ресурси, прикладні сервіси, бази даних, а також кінцеві пристрої користувачів. Такий підхід дозволяє зменшити ризики компрометації системи навіть у разі обходу одного з рівнів захисту.

На мережевому рівні архітектура кібербезпеки зосереджується на контролі та сегментації мережевого трафіку. Банківські інформаційні системи, як правило, мають складну структуру з декількома зонами безпеки, що відрізняються за рівнем критичності. Сегментація мережі дозволяє обмежити можливість неконтрольованого переміщення між цими зонами та локалізувати наслідки потенційних інцидентів. Водночас надмірна сегментація без належного управління може ускладнити адміністрування та негативно вплинути на продуктивність систем.

Архітектура прикладного рівня передбачає захист програмних компонентів, що реалізують основні банківські сервіси. Особливу роль відіграє контроль доступу до прикладних інтерфейсів і бізнес-логіки систем. У банківських інформаційних системах прикладний рівень часто є основною цілью атак, оскільки саме тут обробляються фінансові транзакції та персональні дані клієнтів. Тому архітектура безпеки повинна враховувати специфіку прикладних взаємодій і забезпечувати захист від зловживань на рівні логіки бізнес-процесів.

Окрему роль в архітектурі кібербезпеки відіграє рівень управління ідентичністю та доступом. У сучасних банківських установах користувачі можуть взаємодіяти з інформаційними системами з різних локацій і з використанням різних пристроїв. Архітектура повинна забезпечувати централізований контроль ідентичності, при цьому підтримуючи можливість гнучкого управління правами

доступу відповідно до ролей і поточних умов роботи. Відсутність узгодженого управління доступом створює значні ризики внутрішніх загроз і несанкціонованого використання ресурсів.

Архітектура системи кібербезпеки також повинна включати механізми постійного моніторингу та аналізу подій. Банківські інформаційні системи генерують великі обсяги журналів і телеметричних даних, які можуть використовуватися для виявлення підозрілої активності. Ефективна архітектура передбачає збір, кореляцію та аналіз цих даних у режимі, близькому до реального часу. Це дозволяє своєчасно ідентифікувати інциденти та зменшити час реагування на загрози.

Важливим аспектом архітектури кібербезпеки є забезпечення масштабованості та адаптивності. Банківські інформаційні системи постійно змінюються: впроваджуються нові сервіси, збільшується кількість користувачів, з'являються нові канали доступу. Архітектура безпеки повинна підтримувати ці зміни без необхідності повної перебудови системи. Для цього застосовуються модульні підходи, які дозволяють додавати або змінювати компоненти захисту з мінімальним впливом на функціонування банківських сервісів.

Не менш важливим є питання продуктивності архітектури кібербезпеки. У банківських системах навіть незначні затримки можуть негативно впливати на якість обслуговування клієнтів і ефективність внутрішніх процесів. Тому під час проєктування архітектури необхідно враховувати компроміс між глибиною контролю та швидкістю обробки операцій. Оптимізація потоків даних і автоматизація процесів перевірки доступу дозволяють мінімізувати негативний вплив захисних механізмів на продуктивність.

Архітектура кібербезпеки повинна також забезпечувати можливість відновлення після інцидентів. Це включає резервне копіювання даних, планування сценаріїв відновлення та перевірку працездатності механізмів відновлення. Для банківських установ такі функції мають критичне значення, оскільки навіть короткочасна недоступність інформаційних систем може призвести до значних фінансових і репутаційних втрат.

Слід зазначити, що ефективна архітектура кібербезпеки не обмежується виключно технічними компонентами. Вона також включає організаційні процеси, політики та процедури, які визначають порядок взаємодії між різними підрозділами банку. Узгодженість технічних і організаційних елементів архітектури є необхідною умовою для досягнення належного рівня захищеності.

У разі виявлення інциденту активується процедура реагування, яка включає ідентифікацію джерела загрози, локалізацію інциденту та мінімізацію його наслідків. Для банківських установ швидкість реагування є критично важливою, оскільки дозволяє зменшити фінансові втрати та запобігти поширенню негативного впливу на інші компоненти системи.

Після завершення реагування проводиться аналіз причин інциденту та оцінка ефективності застосованих заходів захисту. Отримані результати використовуються для вдосконалення політик безпеки, оновлення налаштувань системи та підвищення рівня підготовки персоналу.

У практичній діяльності банківських установ порядок функціонування методів і засобів кібербезпеки формується з урахуванням специфіки фінансових операцій, високих вимог до надійності та необхідності безперервного обслуговування клієнтів. На відміну від багатьох інших галузей, банківська сфера не допускає тривалих збоїв у роботі інформаційних систем, тому процеси кіберзахисту повинні бути інтегровані в повсякденну діяльність банку та функціонувати у фоновому режимі.

Важливою особливістю функціонування систем кібербезпеки в банківських інформаційних системах є необхідність постійного узгодження заходів захисту з бізнес-процесами. Засоби безпеки не повинні перешкоджати виконанню фінансових операцій або знижувати швидкість обробки транзакцій, оскільки це безпосередньо впливає на якість банківських послуг. У зв'язку з цим процеси контролю доступу, перевірки операцій та моніторингу подій мають бути оптимізовані таким чином, щоб забезпечувати необхідний рівень захисту без створення надмірного навантаження на систему.

Окрему увагу в порядку функціонування методів і засобів кібербезпеки

приділяють управлінню змінами в інформаційній інфраструктурі банку. Впровадження нових інформаційних систем, оновлення програмного забезпечення, зміна конфігурацій мережевого обладнання або підключення нових сервісів можуть створювати додаткові вразливості. Тому кожна зміна повинна супроводжуватися аналізом потенційних ризиків і коригуванням налаштувань системи кібербезпеки.

Значну роль у функціонуванні системи кібербезпеки відіграє взаємодія між автоматизованими засобами захисту та фахівцями з кібербезпеки. Автоматизовані механізми дозволяють оперативно виявляти підозрілу активність і реагувати на типові інциденти, однак у складних або нетипових ситуаціях необхідне втручання спеціалістів. Саме поєднання автоматизації та експертного аналізу забезпечує ефективне функціонування системи кібербезпеки в довгостроковій перспективі.

У процесі функціонування методів і засобів кібербезпеки важливе місце займає накопичення та аналіз історичних даних про події безпеки. Такі дані дозволяють виявляти тенденції, оцінювати динаміку змін у середовищі загроз і прогнозувати можливі сценарії розвитку кібератак. Для банківських установ це особливо актуально, оскільки дозволяє переходити від реактивного підходу до проактивного управління кіберризиками.

Ще одним аспектом порядку функціонування системи кібербезпеки є навчання та підвищення обізнаності персоналу. Навіть за наявності сучасних технічних засобів захисту людський фактор залишається одним із найбільш уразливих елементів. Тому в банківських установах важливо впроваджувати регулярні заходи з навчання працівників, інструктажі з питань інформаційної безпеки та перевірки знань щодо правил роботи з інформаційними системами.

Крім того, функціонування методів і засобів кібербезпеки тісно пов'язане з процесами внутрішнього контролю та аудиту. Регулярна оцінка стану кібербезпеки дозволяє виявляти слабкі місця, перевіряти відповідність встановлених заходів вимогам нормативних документів і внутрішніх політик банку. Результати таких перевірок використовуються для вдосконалення системи захисту та підвищення її ефективності.

Узагальнюючи, можна зазначити, що порядок функціонування методів і засобів забезпечення кібербезпеки в банківських інформаційних системах є складним багаторівневим процесом, який охоплює технічні, організаційні та управлінські аспекти. Його ефективність залежить не лише від використання сучасних технологій, а й від здатності банківської установи адаптуватися до змін у середовищі загроз і постійно вдосконалювати підходи до кіберзахисту.

Висновки щодо проробленої роботи у другому розділі: було проаналізовано методи та засоби забезпечення кібербезпеки банківських інформаційних систем, а також їх призначення, функціональні можливості та обмеження. Дослідження показало, що ефективний захист інформаційних ресурсів банку можливий лише за умови поєднання технічних, програмних та організаційних заходів у межах єдиної системи кібербезпеки.

Розглянута класифікація методів і засобів захисту засвідчила, що жоден окремий механізм не може гарантувати повний захист банківських інформаційних систем. Найбільш ефективним є комплексний підхід, який поєднує контроль доступу, мережевий захист, моніторинг подій безпеки, захист прикладних систем і механізми реагування на інциденти. Особливу увагу в розділі приділено оцінці ефективності застосування засобів кібербезпеки. Встановлено, що надмірна концентрація на жорстких обмеженнях може негативно впливати на доступність і продуктивність банківських сервісів, тоді як недостатній рівень контролю створює передумови для реалізації кіберзагроз. Тому баланс між рівнем захисту та зручністю використання інформаційних систем є критично важливим. За результатами аналізу зроблено висновок, що сучасні банківські інформаційні системи потребують технологічного підходу до кібербезпеки, який забезпечує гнучке управління доступом, масштабованість і можливість адаптації до змін у середовищі загроз.

3. ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В БАНКІВСЬКИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

3.1. Архітектура технології забезпечення кібербезпеки банківських інформаційних систем на основі принципів Zero Trust

Архітектура технології забезпечення кібербезпеки банківських інформаційних систем на основі принципів Zero Trust формується з урахуванням сучасних умов функціонування банківського сектору, які характеризуються високим рівнем цифровізації, активним використанням віддаленого доступу та інтеграцією з численними зовнішніми сервісами. За таких умов традиційні підходи до побудови систем інформаційної безпеки, що базуються на концепції довіреного мережевого периметра, втрачають свою ефективність і не забезпечують належного рівня захисту інформаційних ресурсів банку.

Запропонована архітектура ґрунтується на принципі відсутності довіри за замовчуванням, відповідно до якого жоден користувач, пристрій або компонент банківської інформаційної системи не вважається безпечним лише на підставі свого розташування в межах корпоративної мережі. Кожна спроба доступу до інформаційних ресурсів підлягає обов'язковій перевірці, незалежно від того, чи здійснюється вона з внутрішньої мережі банку, чи з віддаленого середовища. Такий підхід дозволяє суттєво знизити ризики несанкціонованого доступу та компрометації банківських даних.

У межах розроблюваної архітектури основний акцент робиться на захисті інформаційних ресурсів і сервісів, а не на ізоляції мережевого середовища. Банківські інформаційні системи розглядаються як сукупність окремих сервісів, кожен з яких має власні вимоги до безпеки та рівня доступу. Це дозволяє реалізувати гнучку модель керування доступом, за якої права користувачів надаються відповідно до принципу мінімальних привілеїв і можуть динамічно

змінюватися залежно від прийняття рішення щодо надання доступу до інформаційних ресурсів банку доцільно формалізувати шляхом кількісної оцінки рівня ризику доступу. Для цього в межах розроблюваної технології пропонується використання інтегрального показника ризику, який враховує сукупність контекстних факторів доступу.

На основі розрахованого інтегрального рівня ризику доступу формується рішення щодо можливості взаємодії користувача з інформаційними ресурсами банку. У межах розроблюваної технології пропонується використання таких порогових значень:

$R < 0,3$ — доступ дозволяється без додаткових обмежень;

$0,3 \leq R < 0,6$ — доступ дозволяється з обмеженням функціональних можливостей;

$R \geq 0,6$ — доступ забороняється або сесія припиняється.

Такий підхід дозволяє реалізувати адаптивний механізм керування доступом, що відповідає принципам Zero Trust і забезпечує зниження ризиків несанкціонованого доступу.

Важливою складовою архітектури є механізми ідентифікації та автентифікації користувачів, які забезпечують перевірку особи перед наданням доступу до інформаційних ресурсів. У межах технології Zero Trust автентифікація розглядається не як одноразова процедура, а як безперервний процес, що може повторюватися протягом усього сеансу доступу. Це дозволяє своєчасно реагувати на зміну умов доступу та знижувати рівень довіри у разі виявлення підозрілої поведінки.

Архітектура технології також передбачає врахування характеристик пристроїв, з яких здійснюється доступ до банківських інформаційних систем. Стан пристрою, рівень його захищеності, наявність актуальних оновлень і відповідність внутрішнім вимогам безпеки розглядаються як важливі фактори під час прийняття рішення щодо надання доступу. Такий підхід дозволяє зменшити ризики, пов'язані з використанням незахищених або скомпрометованих пристроїв.

Однією з ключових особливостей архітектури Zero Trust є використання

централізованих політик доступу, які визначають правила взаємодії користувачів із банківськими інформаційними ресурсами. Політики формуються з урахуванням ролей користувачів, типу запитуваних ресурсів, часу доступу та інших контекстних параметрів. Завдяки цьому забезпечується уніфікований підхід до керування доступом і знижується ймовірність помилок, пов'язаних із ручним налаштуванням прав.

У архітектури значна увага приділяється сегментації доступу до інформаційних ресурсів банку. Кожен компонент інформаційної системи ізолюється на логічному рівні, що унеможливорює неконтрольоване переміщення між різними сегментами у разі компрометації окремого елемента. Така сегментація дозволяє локалізувати потенційні інциденти та обмежити масштаби їхнього впливу на діяльність банку.

Архітектура технології забезпечення кібербезпеки на основі принципів Zero Trust також передбачає постійний моніторинг дій користувачів і стану інформаційних систем. Дані про доступи, виконувані операції та мережеву активність збираються та аналізуються з метою виявлення аномалій і потенційних загроз. Моніторинг дозволяє не лише реагувати на вже реалізовані атаки, а й виявляти підготовчі етапи кібератак, що суттєво підвищує рівень захищеності банківських інформаційних систем.

У разі виявлення підозрілої активності архітектура Zero Trust передбачає можливість динамічного коригування рівня доступу або повного блокування сесії. Це дозволяє мінімізувати час перебування зловмисника в системі та зменшити потенційні наслідки інциденту. Такий підхід є особливо важливим для банківських установ, де навіть короткочасна компрометація інформаційних ресурсів може призвести до значних фінансових та репутаційних втрат.

Розроблювана архітектура також орієнтована на забезпечення безперервності банківських бізнес-процесів. Усі механізми контролю доступу та моніторингу впроваджуються таким чином, щоб не створювати надмірних затримок у роботі інформаційних систем і не впливати негативно на якість банківських послуг. Це досягається шляхом оптимізації процедур перевірки та автоматизації процесів

прийняття рішень.

У наслідку цього, архітектура технології забезпечення кібербезпеки банківських інформаційних систем на основі принципів Zero Trust являє собою цілісну, гнучку та адаптивну модель, яка забезпечує захист інформаційних ресурсів незалежно від місця їх розташування та способу доступу. Запропонований підхід створює надійну основу для подальшої реалізації варіантів архітектурних рішень і практичного впровадження принципів Zero Trust у діяльність банківських установ.

Додатково слід звернути увагу на те, що архітектура Zero Trust у банківських інформаційних системах повинна бути тісно пов'язана з процесами управління інформаційною безпекою на рівні всієї організації. Архітектурні рішення не можуть існувати ізольовано від політик безпеки, процедур управління ризиками та вимог регуляторних органів. У цьому контексті архітектура виступає не лише технічною моделлю, а інструментом реалізації стратегічних цілей банку у сфері кібербезпеки.

Практична цінність запропонованої архітектури полягає в можливості її поетапного впровадження без необхідності повної перебудови існуючої інформаційної інфраструктури. Архітектура Zero Trust дозволяє інтегрувати нові механізми контролю доступу та моніторингу поступово, починаючи з найбільш критичних сервісів і розширюючи їх застосування на інші компоненти банківської інформаційної системи. Такий підхід зменшує ризики порушення стабільності бізнес-процесів і забезпечує керованість процесу трансформації системи безпеки.

Важливим аспектом архітектури є її здатність адаптуватися до змін у технологічному середовищі та ландшафті загроз. Зростання кількості цифрових каналів обслуговування клієнтів, поява нових інтеграційних інтерфейсів і розширення функціональності банківських сервісів неминуче впливають на вимоги до безпеки. Запропонована архітектура Zero Trust враховує ці фактори за рахунок гнучкої системи політик і динамічного контролю доступу, що дозволяє швидко реагувати на появу нових ризиків.

Окремої уваги заслуговує питання взаємодії архітектури Zero Trust з існуючими системами банківської автоматизації. У більшості банків

використовуються комплексні та частково застарілі інформаційні системи, повна заміна яких є економічно недоцільною. Архітектура Zero Trust допускає інтеграцію з такими системами через стандартизовані механізми контролю доступу та моніторингу, що дозволяє підвищити рівень захищеності без радикальних змін у базовій інфраструктурі.

З урахуванням викладеного, архітектура технології забезпечення кібербезпеки банківських інформаційних систем на основі принципів Zero Trust формує цілісне середовище захисту, у якому поєднуються контроль доступу, оцінка ризиків, сегментація ресурсів і безперервний моніторинг. Такий підхід дозволяє не лише зменшити ймовірність успішних кібератак, а й обмежити їх наслідки у випадку реалізації загроз.

3.2. Варіанти реалізації Zero Trust у банківських інформаційних системах

Впровадження принципів Zero Trust для побудови банківських інформаційних систем може бути здійснено з використанням різних архітектурних філософій, вибір яких залежить від розміру банківської установи, особливостей дизайну та архітектури інформаційної інфраструктури, ступеня цифрової зрілості, а також рівня вимог до кібербезпеки. Незважаючи на спільну концептуальну основу, конкретні архітектурні рішення можуть суттєво відрізнятися за підходами до організації доступу, рівнем централізації управління та глибиною інтеграції механізмів контролю.

Централізована архітектура контролю доступу є одним із найбільш поширених варіантів застосування принципів Zero Trust у банківських інформаційних системах. Даний підхід передбачає проходження всіх запитів на доступ до інформаційних ресурсів банку через єдину контрольну точку, яка здійснює перевірку ідентичності користувача, аналіз контексту доступу та застосування політик безпеки.

Централізований підхід забезпечує єдині правила доступу для всіх

користувачів і сервісів, спрощує адміністративне управління та підвищує прозорість процесів кібербезпеки. Для банківських установ така архітектура є привабливою завдяки можливості швидкого впровадження та чіткого контролю доступу до критично важливих інформаційних ресурсів.

Водночас централізована архітектура може створювати додаткові виклики, пов'язані з навантаженням на контрольну інфраструктуру та затримками в обробці запитів доступу. У великих банківських установах із розгалуженою мережею філій і значною кількістю користувачів такі обмеження потребують оптимізації та масштабування відповідних компонентів системи.

Іншим архітектурним підходом є розподілена модель впровадження Zero Trust, у межах якої функції контролю доступу та перевірки контексту інтегруються безпосередньо в окремі сегменти банківської інформаційної системи. У такій архітектурі кожен сервіс або кластер сервісів реалізує власні механізми застосування політик Zero Trust.

Завдяки цьому мінімізується залежність від єдиної контрольної точки, а загальна стійкість системи кібербезпеки підвищується. Такий підхід є особливо актуальним для банківських установ, що використовують мікросервісні архітектури та хмарні технології.

Разом із тим розподілена архітектура вимагає більш високого рівня координації між компонентами системи та гармонізації практик безпеки. За відсутності належного централізованого управління може виникнути складність у контролі відповідності політик доступу та моніторингу подій безпеки.

На практиці найбільш доцільним для більшості банківських установ є гібридний архітектурний підхід, який поєднує елементи централізованої та розподіленої моделей. У межах такої архітектури ключові функції управління ідентичністю, політиками доступу та моніторингом подій безпеки зосереджуються в єдиному центрі, тоді як безпосереднє застосування політик здійснюється на рівні окремих сервісів і ресурсів.

Гібридний підхід дозволяє досягти оптимального балансу між керованістю, масштабованістю та гнучкістю системи кібербезпеки, що є критично важливим для

банківських інформаційних систем із високими вимогами до доступності та продуктивності.

Окрему категорію становлять архітектурні рішення Zero Trust, орієнтовані на підтримку активного віддаленого доступу. У таких сценаріях ключову роль відіграє контроль ідентичності користувача та стану пристрою, з якого здійснюється підключення. Архітектура повинна забезпечувати однаковий рівень захищеності як для внутрішнього персоналу банку, так і для зовнішніх користувачів, незалежно від місця їх підключення.

У сучасних банківських установах інформаційні системи часто розміщуються як у власних центрах обробки даних, так і в хмарних середовищах. Архітектура Zero Trust у таких умовах повинна забезпечувати послідовний захист інформаційних ресурсів незалежно від їх фізичного розташування. Це вимагає узгодження політик доступу, механізмів автентифікації та засобів моніторингу між різними інфраструктурними середовищами в режимі реального часу.

Практична реалізація Zero Trust у банківських інформаційних системах повинна здійснюватися поступово. Багато банківських установ використовують застарілі автоматизовані системи, повна заміна яких є економічно недоцільною. У таких випадках архітектура Zero Trust впроваджується поетапно, починаючи з найбільш критичних ресурсів і поступово охоплюючи інші компоненти системи.

Важливим аспектом архітектурних рішень є забезпечення сумісності Zero Trust із наявними системами керування доступом та інформаційної безпеки. У більшості банківських установ уже впроваджено певні механізми автентифікації, контролю доступу та моніторингу подій. Тому архітектура Zero Trust повинна інтегруватися з існуючою інфраструктурою без порушення стабільності її функціонування. Такий підхід дозволяє реалізувати принципи Zero Trust поступово, з мінімальними ризиками для операційної діяльності банку.

Окрему увагу в архітектурних рішеннях Zero Trust приділяють захисту внутрішніх користувачів банку, які мають доступ до критично важливих інформаційних ресурсів. У традиційних моделях безпеки внутрішні користувачі часто вважаються довіреними, що створює значні ризики внутрішніх загроз.

Архітектура Zero Trust усуває цю проблему шляхом застосування однакових правил контролю доступу як для внутрішніх, так і для зовнішніх користувачів, що істотно підвищує рівень загальної безпеки.

Ще одним напрямом архітектурних рішень є реалізація Zero Trust у контексті взаємодії банківських інформаційних систем із зовнішніми організаціями та сервісами. Банки активно обмінюються даними з платіжними системами, фінансовими партнерами та державними інформаційними ресурсами. У таких сценаріях архітектура Zero Trust повинна забезпечувати контроль кожного зовнішнього з'єднання, незалежно від рівня довіри до партнера, що дозволяє мінімізувати ризики компрометації інформаційних ресурсів через зовнішні канали.

Практика впровадження Zero Trust у банківських інформаційних системах також показує доцільність використання контекстно-орієнтованих архітектурних рішень. Контекст доступу включає не лише ідентичність користувача, а й поведінкові характеристики, історію доступів та поточні умови підключення. Архітектурні рішення, що враховують ці фактори, дозволяють реалізувати більш гнучку та адаптивну модель захисту, яка реагує на зміну рівня ризику в реальному часі.

Важливим чинником вибору архітектурного рішення є забезпечення масштабованості системи кібербезпеки. Банківські інформаційні системи постійно розвиваються, зростає кількість користувачів, сервісів і каналів доступу. Архітектура Zero Trust повинна бути здатною підтримувати це зростання без суттєвого ускладнення управління та зниження продуктивності. Тому архітектурні рішення мають передбачати можливість горизонтального масштабування та автоматизації процесів контролю доступу.

Окремо слід відзначити роль архітектурних рішень Zero Trust у забезпеченні відповідності банківських інформаційних систем регуляторним вимогам. Банківська діяльність регламентується численними нормативними документами у сфері захисту інформації та персональних даних. Архітектура Zero Trust, завдяки централізованому управлінню політиками доступу та детальному аудиту дій користувачів, створює передумови для виконання вимог регуляторів і спрощує

процедури контролю та звітності.

Переглянувши види архітектурних рішень реалізації Zero Trust у банківських інформаційних системах повинні розглядатися не як універсальні шаблони, а як гнучкі моделі, що адаптуються до специфіки конкретної банківської установи. Комплексний підхід до проєктування архітектури дозволяє поєднати високий рівень кібербезпеки з ефективністю банківських бізнес-процесів, що є ключовою вимогою сучасного фінансового сектору.

Реальний вибір варіанту реалізації Zero Trust у банківській інформаційній системі завжди пов'язаний із компромісом між рівнем безпеки, складністю впровадження та впливом на операційну діяльність банку. Жодна з розглянутих архітектурних моделей не може вважатися універсальною, оскільки ефективність її застосування визначається конкретними умовами функціонування банківської установи, структурою бізнес-процесів і ступенем інтеграції інформаційних систем.

Практика показує, що для великих банків із розгалуженою інфраструктурою та значною кількістю користувачів доцільно застосовувати комбіновані архітектурні рішення, які дозволяють поєднати централізований контроль із локальною автономією окремих сервісів. Такий підхід забезпечує керованість системи кібербезпеки на стратегічному рівні, водночас зберігаючи гнучкість і масштабованість на рівні окремих підсистем.

Для менших банківських установ або спеціалізованих фінансових організацій більш прийнятними можуть бути спрощені варіанти реалізації Zero Trust, зосереджені на ключових сервісах і критичних інформаційних ресурсах. У таких випадках основний акцент робиться на контролі доступу, автентифікації користувачів і моніторингу подій безпеки без надмірного ускладнення архітектури.

Суттєвим фактором під час вибору архітектурного рішення є рівень зрілості процесів управління інформаційною безпекою в банківській установі. За відсутності налагоджених політик, процедур і механізмів контролю навіть технічно досконалі рішення Zero Trust можуть не дати очікуваного ефекту. Тому архітектурні варіанти повинні підбиратися з урахуванням готовності організації до їх практичного застосування. Також варто враховувати, що архітектурні рішення

Zero Trust не є статичними. У процесі експлуатації банківської інформаційної системи архітектура може змінюватися, доповнюватися новими компонентами або трансформуватися відповідно до змін у бізнес-моделі банку та ландшафті кіберзагроз. Це означає, що обрана архітектура повинна мати потенціал для подальшого розвитку без необхідності кардинального перегляду базових принципів.

Узагальнюючи викладене, варіанти реалізації Zero Trust у банківських інформаційних системах слід розглядати як набір адаптивних моделей, що можуть комбінуватися та модифікуватися відповідно до потреб конкретної установи. Усвідомлений вибір архітектурного підходу створює передумови для ефективної практичної реалізації принципів Zero Trust, що потребує детального опрацювання технології впровадження та застосування цих принципів у реальному середовищі банківської інформаційної системи.

3.3 Технологія впровадження та застосування принципів Zero Trust у банківських інформаційних системах

У ході виконання даної кваліфікаційної роботи основну увагу було зосереджено на практичному опрацюванні технології впровадження та застосування принципів Zero Trust у банківських інформаційних системах. Необхідність такого підходу зумовлена тим, що сучасні банківські установи функціонують у складному інформаційному середовищі, де поєднуються внутрішні автоматизовані системи, віддалений доступ персоналу, інтеграція з зовнішніми сервісами та обробка значних обсягів конфіденційних даних. У таких умовах використання виключно традиційних механізмів захисту не забезпечує належного рівня кібербезпеки.

Розроблювана в межах роботи технологія Zero Trust розглядається як послідовний процес, що охоплює аналіз інфраструктури, формування політик доступу, оцінювання ризиків і постійне вдосконалення захисних механізмів. На першому етапі було проведено детальний аналіз інформаційної інфраструктури

банківської установи, який дозволив визначити склад і взаємозв'язки основних компонентів банківських інформаційних систем. У межах цього етапу здійснювалась ідентифікація користувачів, сервісів і ресурсів, а також каналів доступу до них.

Отримані результати аналізу дали змогу виділити найбільш критичні інформаційні ресурси, які потребують підвищеного рівня захисту. Особливу увагу було приділено ресурсам, що безпосередньо пов'язані з виконанням фінансових операцій, обробкою персональних даних клієнтів і забезпеченням безперервності банківських бізнес-процесів. Такий підхід дозволив сформувати основу для подальшого впровадження принципів Zero Trust без необхідності повної перебудови всієї інформаційної інфраструктури.

На наступному етапі в межах дослідження було здійснено класифікацію користувачів і ресурсів банківської інформаційної системи. Користувачі групувалися за функціональними ролями, рівнем доступу та характером виконуваних операцій. Паралельно інформаційні ресурси класифікувалися за ступенем критичності та чутливості. Така класифікація дала змогу реалізувати принцип мінімальних привілеїв і створити передумови для формалізованого керування доступом.

Важливим елементом практичної реалізації Zero Trust у даній роботі стало використання кількісного підходу до оцінки ризику доступу. У межах дослідження було запропоновано інтегральний показник ризику доступу, який дозволяє об'єктивно оцінювати безпечність кожної спроби взаємодії з банківською інформаційною системою. Такий підхід є особливо актуальним для банківської сфери, де рішення щодо доступу повинні прийматися швидко, але водночас бути обґрунтованими.

Інтегральний показник ризику доступу R було визначено як зважену суму основних контекстних параметрів доступу. У межах розроблюваної технології було обрано чотири ключові фактори: характеристики користувача, стан пристрою, локацію доступу та часові параметри. Формалізація цих факторів дозволила перейти від суб'єктивної оцінки до кількісної моделі прийняття рішень.

Інтегральний рівень ризику доступу R визначається за формулою:

Формула 3.1

$$R = w_1 \cdot U + w_2 \cdot D + w_3 \cdot L + w_4 \cdot T$$

Таб.3.1

Параметр	Діапазон	Практичний зміст
(U)	0–1	Роль користувача, історія доступів
(D)	0–1	Стан пристрою, оновлення, захист
(L)	0–1	Внутрішня / зовнішня локація
(T)	0–1	Робочий / неробочий час

У межах розроблюваної технології всі параметри нормуються в діапазоні від 0 до 1. Вагові коефіцієнти було визначено з урахуванням специфіки банківських інформаційних систем:

$$w_1=0,35;$$

$$w_2=0,30;$$

$$w_3=0,20;$$

$$w_4=0,15;$$

Нехай користувач має такі параметри доступу:

$$U=0,4;$$

$$D=0,5;$$

$$L=0,7;$$

$$T=0,2;$$

Тоді інтегральний рівень ризику доступу становить:

Формула 3.2

$$R = 0.35 * 0.4 + 0.30 * 0.5 + 0.20 * 0.7 + 0.15 * 0.2$$

$$R= 0.455$$

Отримане значення відповідає **середньому рівню ризику**, що в межах розробленої технології передбачає надання доступу з функціональними обмеженнями.

У межах роботи було визначено такі порогові значення інтегрального ризику:

$$R < 0.3$$

$$0.3 \leq R < 0.6$$

$$R \geq 0.6$$

Застосування таких порогів дозволяє реалізувати адаптивний контроль доступу відповідно до принципів Zero Trust.

Для оцінювання практичної ефективності впровадження запропонованої технології в роботі було використано показник зниження кількості інцидентів інформаційної безпеки. Ефективність визначалась за формулою:

Формула 3.3

$$E = \frac{(I_{\text{до}} - I_{\text{після}})}{I_{\text{до}}} * 100\%$$

$I_{\text{до}}$ — кількість інцидентів до впровадження Zero Trust;

$I_{\text{після}}$ — кількість інцидентів після впровадження.

Умовний приклад розрахунку.

До впровадження технології фіксувалося 120 інцидентів на рік, після впровадження — 45.

Формула 3.4

$$E = \frac{(120 - 45)}{120} * 100\% = 62,5\%$$

Отримане значення свідчить про суттєве підвищення рівня кібербезпеки банківської інформаційної системи внаслідок впровадження принципів Zero Trust.

У підсумку, виконання роботи було не лише описано технологію

впровадження принципів Zero Trust, а й здійснено її практичне опрацювання з використанням формалізованих методів оцінки ризиків і ефективності. Запропонована технологія може бути адаптована до умов конкретної банківської установи та використана як основа для побудови сучасної системи кібербезпеки.

3.4 Рекомендації щодо впровадження технології забезпечення кібербезпеки банківських інформаційних систем на основі Zero Trust

Під час виконання кваліфікаційної роботи та розробки технології забезпечення кібербезпеки банківських інформаційних систем на основі принципів Zero Trust було сформовано низку практичних рекомендацій, спрямованих на підвищення ефективності впровадження цього підходу в діяльність банківських установ. Рекомендації мають комплексний характер і охоплюють організаційні, технічні та процедурні аспекти побудови системи кібербезпеки.

Основною пропозицією є поетапне впровадження принципів Zero Trust у банківські інформаційні системи. Практика свідчить, що різка та повна трансформація існуючої інформаційної інфраструктури пов'язана зі значною технічною та економічною складністю. У зв'язку з цим доцільно розпочинати впровадження Zero Trust із найбільш критичних інформаційних ресурсів і сервісів, які забезпечують обробку фінансових транзакцій та персональних даних клієнтів. Такий підхід дозволяє поступово адаптувати персонал і технологічне середовище до нової парадигми безпеки.

Ключовою рекомендацією є впровадження прозорості та формалізованої практики управління ідентифікацією користувачів і доступом до інформаційних ресурсів. У межах концепції Zero Trust рішення щодо надання або обмеження доступу приймається з урахуванням не лише ідентичності користувача, а й контексту, у якому здійснюється доступ. Тому банківським установам рекомендується забезпечувати актуальність облікових записів, регулярно переглядати ролі користувачів та своєчасно вилучати надлишкові права доступу. Це дозволяє мінімізувати ризики внутрішніх загроз і несанкціонованого

використання облікових записів.

Особливу увагу в рекомендаціях приділено застосуванню формалізованого підходу до оцінювання ризиків доступу. Запропонована в дослідженні модель інтегрального індикатора ризику дозволяє автоматизувати процес прийняття рішень і зменшити вплив людського фактора. Рекомендується адаптувати вагові коефіцієнти моделі до специфіки конкретної банківської установи та періодично переглядати їх з урахуванням змін у загрозовому середовищі.

Важливою рекомендацією є забезпечення постійного моніторингу подій інформаційної безпеки та активності користувачів. У межах Zero Trust моніторинг розглядається не як допоміжний елемент, а як невід'ємна складова всієї технології. Банківським установам доцільно розробити механізми спостереження за діями користувачів, що дозволяють своєчасно виявляти аномальну активність і локалізувати кіберінциденти на ранніх стадіях.

Окремо рекомендується приділяти увагу навчанню та підвищенню рівня обізнаності персоналу банківських установ у сфері кібербезпеки. Навіть за наявності сучасних технічних засобів захисту ефективність системи безпеки значною мірою залежить від рівня підготовки користувачів. Регулярне навчання сприяє зменшенню кількості інцидентів, пов'язаних із соціальною інженерією та помилками персоналу, а також формує відповідальне ставлення до питань інформаційної безпеки.

У технічному аспекті в межах Zero Trust рекомендується впроваджувати сегментацію доступу до банківських інформаційних ресурсів. Логічна ізоляція сервісів і даних дозволяє обмежити масштаб можливих інцидентів і зменшити наслідки компрометації окремих компонентів системи. Такий підхід є особливо актуальним для банківських інформаційних систем із розподіленою або гібридною архітектурою.

Важливою рекомендацією є також регулярне оцінювання ефективності впровадженої технології Zero Trust. Доцільно використовувати кількісні показники, зокрема рівень зменшення кількості інцидентів інформаційної безпеки, скорочення часу реагування на події та зниження кількості ризикованих доступів.

Аналіз таких показників дозволяє обґрунтовувати подальші управлінські рішення та визначати напрями вдосконалення системи кібербезпеки.

Слід зазначити, що впровадження принципів Zero Trust повинно здійснюватися з урахуванням вимог регуляторних органів та внутрішніх політик безпеки банківської установи. Одним із ключових аспектів дотримання нормативних вимог у сфері захисту інформації є забезпечення можливості контролю доступу та аудиту дій користувачів, що реалізується в межах запропонованої технології.

В межі впровадження технології забезпечення кібербезпеки на основі принципів Zero Trust доцільно також передбачити механізми її подальшого розвитку та адаптації. Банківські інформаційні системи є динамічними за своєю природою, оскільки постійно змінюються як внутрішні бізнес-процеси, так і зовнішнє середовище загроз. Тому впроваджена технологія Zero Trust повинна розглядатися не як завершене рішення, а як основа для безперервного вдосконалення системи кібербезпеки.

Одним із напрямів подальшого розвитку технології є розширення набору параметрів, що використовуються для оцінювання ризику доступу. У практичній діяльності банківських установ з часом можуть з'являтися нові фактори ризику, пов'язані з поведінкою користувачів, використанням нових типів пристроїв або змінами у способах взаємодії з інформаційними ресурсами. Адаптація моделі ризику дозволяє підвищити точність прийняття рішень і зменшити ймовірність помилкових дозволів або необґрунтованих обмежень доступу.

Рекомендується також забезпечити інтеграцію технології Zero Trust із процесами управління інформаційною безпекою на організаційному рівні. Зокрема, результати оцінювання ризиків доступу можуть використовуватися для формування звітів для керівництва банку, планування заходів з підвищення рівня захисту та визначення пріоритетних напрямів інвестування у сфері кібербезпеки. Такий підхід дозволяє поєднати технічні механізми захисту з управлінськими рішеннями.

Окрему увагу доцільно приділяти питанням управління змінами в системі

кібербезпеки. У процесі експлуатації банківських інформаційних систем регулярно відбуваються оновлення програмного забезпечення, зміни у структурі підрозділів або впровадження нових сервісів. Усі такі зміни повинні супроводжуватися аналізом впливу на модель Zero Trust та коригуванням відповідних політик доступу. Це дозволяє уникнути ситуацій, коли нові компоненти системи залишаються поза межами дії механізмів захисту.

Ще одним важливим напрямом удосконалення технології є підвищення рівня автоматизації процесів реагування на інциденти інформаційної безпеки. У межах Zero Trust автоматизовані механізми можуть використовуватися для оперативного обмеження доступу, ізоляції скомпрометованих облікових записів або пристроїв, а також для ініціювання додаткових перевірок. Це особливо актуально для банківських установ, де швидкість реагування на інциденти безпосередньо впливає на масштаби можливих збитків.

На практиці рекомендується також періодично переглядати ефективність впровадженої технології Zero Trust із використанням кількісних і якісних показників. Аналіз статистики інцидентів, результатів аудитів безпеки та показників доступності сервісів дозволяє виявляти слабкі місця в системі та своєчасно вживати коригувальних заходів. Такий підхід сприяє підвищенню зрілості системи кібербезпеки банківської установи.

З урахуванням специфіки банківської діяльності важливо також забезпечити відповідність технології Zero Trust вимогам внутрішніх і зовнішніх нормативних документів. Запропонована в роботі технологія створює умови для детального аудиту дій користувачів і контролю доступу до інформаційних ресурсів, що є важливим елементом забезпечення відповідності регуляторним вимогам у сфері захисту інформації та персональних даних.

Окремо слід підкреслити, що впровадження технології Zero Trust у банківських інформаційних системах доцільно розглядати як довгостроковий процес, який потребує постійного вдосконалення та адаптації. Зміни у бізнес-процесах банку, поява нових цифрових сервісів і розширення каналів взаємодії з клієнтами неминуче впливають на вимоги до системи кібербезпеки, що вимагає

регулярного перегляду застосовуваних підходів і рішень.

Рекомендується також забезпечити тісну взаємодію між технічними підрозділами, службами інформаційної безпеки та керівництвом банківської установи. Така взаємодія дозволяє узгоджувати технічні рішення з бізнес-цілями організації та своєчасно враховувати ризики, які можуть впливати на стратегічну діяльність банку. У межах Zero Trust це особливо важливо, оскільки рішення щодо доступу та контролю безпосередньо пов'язані з виконанням бізнес-функцій.

Крім того, доцільно передбачити можливість масштабування впровадженої технології з урахуванням майбутнього розвитку інформаційної інфраструктури банку. Запропонована технологія повинна підтримувати розширення кількості користувачів, інтеграцію нових інформаційних ресурсів і зміну архітектури систем без необхідності суттєвого перегляду базових принципів безпеки. Це дозволяє зберегти інвестиції в кібербезпеку та забезпечити стабільність захисних механізмів у довгостроковій перспективі.

Таким чином, реалізація наведених рекомендацій не лише підвищує поточний рівень кібербезпеки банківських інформаційних систем, а й формує основу для їх подальшого розвитку відповідно до принципів Zero Trust. Запропонований підхід створює умови для побудови гнучкої, адаптивної та стійкої системи захисту, здатної ефективно протидіяти сучасним і перспективним кіберзагрозам.

Висновки щодо третього розділу кваліфікаційної роботи присвячено: розробці технології забезпечення кібербезпеки банківських інформаційних систем, що ґрунтується на сучасних принципах контролю доступу та управління ризиками. У межах розділу було сформовано архітектуру технології, розглянуто варіанти її реалізації та запропоновано практичні рекомендації щодо впровадження.

Розроблена архітектура технології орієнтована на захист інформаційних ресурсів незалежно від місця їх розташування та способу доступу. Запропонований підхід дозволяє відмовитися від апріорної довіри до користувачів і систем та реалізувати адаптивний механізм керування доступом на основі контексту та оцінки ризиків. Практичне опрацювання технології підтвердило доцільність

використання кількісних методів оцінки ризику доступу та ефективності впровадження заходів кібербезпеки. Запропоновані формалізовані показники дозволяють обґрунтовано приймати рішення щодо надання або обмеження доступу та оцінювати результати впровадження технології з точки зору зниження кількості інцидентів. Сформульовані рекомендації щодо впровадження технології враховують організаційні, технічні та регуляторні аспекти діяльності банківських установ і можуть бути використані на практиці без необхідності повної перебудови існуючої інфраструктури. У цілому результати третього розділу підтверджують можливість побудови ефективної, гнучкої та масштабованої системи кібербезпеки банківських інформаційних систем, здатної протистояти сучасним кіберзагрозам.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи було досліджено актуальну науково-практичну проблему забезпечення кібербезпеки банківських інформаційних систем в умовах цифрової трансформації фінансового сектору. Сучасні банківські установи функціонують у складному та динамічному інформаційному середовищі, яке характеризується активним використанням хмарних технологій, віддаленого доступу, інтеграції з зовнішніми сервісами та зростанням обсягів оброблюваних конфіденційних даних. За таких умов традиційні підходи до забезпечення інформаційної безпеки, що ґрунтуються на концепції довіреного мережевого периметра, виявляються недостатньо ефективними.

У першому розділі роботи було проаналізовано проблему кібербезпеки банківських інформаційних систем, визначено основні загрози та вразливості, характерні для сучасних фінансових установ. Особливу увагу приділено впливу цифровізації, зростанню складності інформаційної інфраструктури та ролі людського фактора у формуванні ризиків безпеки. Проведений аналіз показав, що кіберзагрози мають комплексний характер і можуть реалізовуватися як через технічні, так і через організаційні та поведінкові вразливості. Це зумовлює необхідність застосування системного підходу до побудови захисту банківських інформаційних ресурсів.

У другому розділі було здійснено аналіз методів та засобів забезпечення кібербезпеки банківських інформаційних систем. Розглянуто призначення та функції систем кібербезпеки, а також архітектурні підходи до їх побудови. Встановлено, що ефективна система захисту повинна мати багаторівневу архітектуру, поєднувати технічні, організаційні та управлінські механізми, а також забезпечувати постійний моніторинг подій безпеки. Аналіз існуючих рішень показав, що фрагментарне використання окремих засобів захисту не дозволяє досягти належного рівня безпеки в умовах розподілених і гібридних інформаційних систем.

У роботі розглянуто різні варіанти реалізації принципів Zero Trust у банківських інформаційних системах, зокрема централізовані, розподілені та гібридні архітектурні моделі. Обґрунтовано доцільність використання гібридного підходу, який забезпечує баланс між керованістю, масштабованістю та гнучкістю системи кібербезпеки. Такий підхід дозволяє поступово впроваджувати принципи Zero Trust без необхідності повної заміни існуючої інфраструктури, що є економічно доцільним для банківських установ. Важливим результатом роботи є практичне опрацювання технології впровадження Zero Trust із використанням формалізованого підходу до оцінки ризиків доступу. Запропоновано модель інтегрального показника ризику, яка враховує контекстні параметри доступу, зокрема характеристики користувача, стан пристрою, локацію та часові умови. Використання кількісної оцінки дозволяє автоматизувати процес прийняття рішень щодо доступу та зменшити вплив людського фактора. Наведені розрахунки демонструють практичну придатність запропонованої моделі та її ефективність у зниженні рівня кіберризиків. Загалом результати кваліфікаційної роботи підтверджують доцільність і ефективність застосування принципів Zero Trust для побудови сучасних систем кібербезпеки банківських інформаційних систем. Запропонована технологія створює основу для підвищення рівня захищеності інформаційних ресурсів, забезпечення безперервності банківських бізнес-процесів і адаптації системи кібербезпеки до сучасних і майбутніх загроз.

ПЕРЕЛІК ПОСИЛАНЬ

1. Zero Trust Architecture : NIST Special Publication 800-207. Gaithersburg : National Institute of Standards and Technology, 2020. 59 p.
2. Cybersecurity Framework Profile for the Financial Sector. Version 1.0. Gaithersburg : NIST, 2023. 78 p.
3. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Geneva : ISO, 2022. 32 p.
4. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — Information security controls. Geneva : ISO, 2022. 118 p.
5. ISO/IEC 27005:2022. Information security risk management. Geneva : ISO, 2022. 68 p.
6. European Central Bank. Cyber resilience oversight expectations for financial market infrastructures. Frankfurt am Main : ECB, 2023. 46 p.
7. Basel Committee on Banking Supervision. Principles for operational resilience. Basel : Bank for International Settlements, 2021. 36 p.
8. ENISA. Zero Trust Architecture — Current Trends. Heraklion : European Union Agency for Cybersecurity, 2022. 64 p.
9. Cloud Security Alliance. Zero Trust Advancement Center Overview. Seattle : CSA, 2023. 41 p.
10. Gartner. Zero Trust Network Access Market Guide. Stamford, CT : Gartner Research, 2023. 27 p.
11. Behl A., Behl K. Cyberwar and Information Warfare. 2nd ed. Oxford : Oxford University Press, 2022. 352 p.
12. Andress J. The Basics of Information Security: Understanding the Fundamentals of InfoSec. 3rd ed. Amsterdam : Elsevier, 2023. 416 p.
13. Stallings W. Effective Cybersecurity: A Guide to Using Best Practices and Standards. Boston : Pearson, 2022. 512 p.
14. Kahn Academy Cybersecurity Lab. Risk-Based Access Control Models. San Jose : Cisco Press, 2023. 214 p.
15. Microsoft. Zero Trust Deployment Guide. Redmond : Microsoft Security, 2023. 89 p.
16. Google Cloud. BeyondCorp Zero Trust Enterprise Security. Mountain View : Google LLC, 2022. 57 p.