

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ
ВАДИМА ГЕТЬМАНА**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ «ІНСТИТУТ ІНФОРМАЦІЙНИХ
ТЕХНОЛОГІЙ В ЕКОНОМІЦІ»**

Кафедра системного аналізу та кібербезпеки

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «КІБЕРБЕЗПЕКА»

Галузь знань 12 «Інформаційні технології»

Спеціальність 125 «Кібербезпека»

Форма навчання: очна (денна)

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

**на тему «Дослідження та удосконалення системи управління
інформаційною безпекою банківської установи»**

здобувача Семендя Богдана Андрійовича _____

Науковий керівник: к.е.н., проф. Бегун Анатолій Володимирович

**Робота допущена до захисту перед екзаменаційною комісією
з атестації здобувачів вищої освіти (ЕК)**

Завідувач кафедри: д.ф.-м.н., професор Джалладова І.А.

Київ 2026

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ
ВАДИМА ГЕТЬМАНА

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ «ІНСТИТУТ ІНФОРМАЦІЙНИХ
ТЕХНОЛОГІЙ В ЕКОНОМІЦІ»

Кафедра системного аналізу та кібербезпеки

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «КІБЕРБЕЗПЕКА»

Галузь знань 12 «Інформаційні технології»

Спеціальність 125 «Кібербезпека»

ПОГОДЖЕНО

Керівник проєктної групи (гарант)
Освітньо-професійної програми
«Кібербезпека»

_____ к.е.н., проф. А.В. Бегун
_____ 2026р.

ЗАТВЕРДЖУЮ

Завідувач кафедри системного аналізу
та кібербезпеки

_____ д.ф.-м.н., проф. І.А. Джалладова
_____ 2026р.

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

здобувача вищої освіти Семендя Богдана Андрійовича

очної (денної) форми навчання

на підготовку кваліфікаційної бакалаврської роботи
*на тему « Дослідження та удосконалення системи управління
інформаційною безпекою банківської установи »*

Тему затверджено наказом ректора Університету від _____

Кваліфікаційна бакалаврська робота виконується на матеріалах літературних, нормативно-правових та інформаційних джерел, міжнародних стандартів, а також із використанням відкритих електронних ресурсів для аналізу функціональних можливостей інструментів та обґрунтування пропонованих практичних заходів.

План кваліфікаційної бакалаврської роботи

Розділ 1	Концептуальні засади управління інформаційною безпекою банківської установи
Розділ 2	Аналіз поточного стану системи управління інформаційною безпекою АТ “Демо-Банк”
Розділ 3	Удосконалення системи управління інформаційною безпекою АТ “Демо-Банк”

Об’єкт дослідження:	Процес управління інформаційною безпекою банківської установи
Предмет дослідження:	Теоретичні, методичні та практичні підходи до аналізу, оцінювання та удосконалення системи управління інформаційною безпекою банку
Мета кваліфікаційної бакалаврської роботи:	Дослідження системи управління інформаційною безпекою банківської установи, виявлення її основних прогалин та розробка обґрунтованих рекомендацій щодо підвищення рівня інформаційної безпеки

Конкретні завдання, які здобувач повинен виконати для досягнення поставленої мети:

У розділі 1 «Концептуальні засади управління інформаційною безпекою банківської установи»: дослідити сутність системи управління інформаційною безпекою, розкрити її основні принципи побудови та визначити роль СУІБ у забезпеченні конфіденційності, цілісності й доступності інформації. Охарактеризувати особливості забезпечення інформаційної безпеки у банківських установах, визначити основні об’єкти захисту, типові загрози та узагальнити нормативно-методичні підходи до побудови, оцінювання й удосконалення СУІБ банку.

У розділі 2 «Аналіз поточного стану системи управління інформаційною безпекою АТ “Демо-Банк”»: охарактеризувати інформаційні активи, критичні об’єкти СУІБ та організаційні ролі, що беруть участь у забезпеченні інформаційної безпеки банківської установи. Проаналізувати наявні організаційні, програмні та технічні механізми захисту, визначити їхню роль у функціонуванні СУІБ, виявити основні прогалини контрольного середовища та оцінити пов’язані з ними ризики.

У розділі 3 «Удосконалення системи управління інформаційною безпекою АТ “Демо-Банк”»: сформувати цільову модель удосконалення СУІБ банку, розробити практичні контрольні заходи для зниження виявлених ризиків та визначити інструменти їх реалізації, відповідальних осіб, періодичність виконання і доказову базу. Обґрунтувати етапність впровадження запропонованих заходів та оцінити їх очікувану ефективність шляхом порівняння початкового і залишкового рівня ризиків.

Завдання підготував
науковий керівник

Бегун А. В.

«____» _____ 2026 р.

Завдання одержав
здобувач

Семендй Б. А.

«____» _____ 2026 р.

РЕФЕРАТ

Кваліфікаційна бакалаврська робота містить 87 сторінки, 30 таблиць, 1 формулу, 6 рисунків, список використаних джерел з 26 найменувань.

Об'єкт дослідження: процес управління інформаційною безпекою банківської установи.

Мета кваліфікаційної роботи: дослідження системи управління інформаційною безпекою банківської установи, виявлення її основних прогалин та розробка обґрунтованих рекомендацій щодо підвищення рівня інформаційної безпеки.

Методи дослідження: методи наукової абстракції, аналізу та синтезу, порівняння, класифікації, експертного оцінювання, моделювання та узагальнення.

У роботі проведено дослідження системи управління інформаційною безпекою банківської установи на прикладі умовної моделі АТ «Демо-Банк». Розкрито сутність СУІБ, принципи її побудови, особливості забезпечення інформаційної безпеки у банківському секторі та нормативно-методичні підходи до її оцінювання й удосконалення.

Проаналізовано критичні об'єкти СУІБ АТ «Демо-Банк», організаційні ролі та наявні механізми забезпечення інформаційної безпеки. Виявлено основні прогалини контрольного середовища, оцінено пов'язані з ними ризики та визначено напрями їх зниження.

Запропоновано цільову модель удосконалення СУІБ, що ґрунтується на ризик-орієнтованому підході. Розроблено комплекс практичних контрольних заходів, зокрема розширення MFA, періодичний перегляд доступів, контроль привілейованих акаунтів, впровадження SIEM-моніторингу, DLP-контролю, перегляд мережевої сегментації, тестування відновлення, формалізацію реагування на інциденти та навчання персоналу.

Практичне значення роботи полягає в тому, що запропоновані контрольні заходи, інструменти їх реалізації та нормативно-методичні орієнтири можуть бути

використані під час дослідження, оцінювання та подальшого удосконалення СУІБ реальної банківської установи.

Наукова новизна дослідження полягає в розробленні послідовного підходу до удосконалення СУІБ банківської установи, який поєднує аналіз критичних об'єктів захисту, оцінювання наявних механізмів інформаційної безпеки, визначення прогалин, оцінку ризиків і формування контрольних заходів із зазначенням інструментів їх реалізації та очікуваного ефекту.

Ключові слова: інформаційна безпека, СУІБ, банківська установа, ризик-орієнтований підхід, контрольні заходи, кіберризики.

ВІДГУК

на кваліфікаційну бакалаврську роботу

студента Семендя Богдана Андрійовича гр. ІК-401

на тему: «Дослідження та удосконалення системи управління інформаційною безпекою банківської установи»

Актуальність теми. Дослідження та удосконалення системи управління інформаційною безпекою банківської установи є актуальним завданням, оскільки дозволяє перейти від фрагментарного застосування окремих засобів захисту до комплексного, ризик-орієнтованого та керованого підходу..

Повнота розкриття теми в дипломній роботі відповідає поставленим меті, задачам, обсягу і змісту. Робота складається з трьох розділів, кожний з яких має свою специфіку і особливості.

Теоретичний рівень запропонованої роботи свідчить про вміння здобувача опрацьовувати та аналізувати наукові видання, нормативні документи, технічну документацію, проводити аналіз, використовувати методи максимального правдоподібності та синтезу.

Практична значущість дипломної роботи полягає у розробці конкретних рекомендацій та практичних рішень, які можуть бути використані як основа для удосконалення та оцінки СУІБ банківської установи, продемонстровано принципи виявлення ключових прогалин в управлінні інформаційною безпекою, оцінено пов'язані з ними ризики та розроблено практичні контрольні заходи із зазначенням інструментів їх реалізації, відповідальних осіб, періодичності виконання й доказової бази.

Самостійність виконання роботи визначається здатністю здобувача самостійно працювати з науково-технічною літературою, послідовно знаходити і обробляти статистичну, публічну і наукову інформацію, будувати вектор дослідження.

Якість оформлення, загальна та спеціальна грамотність відповідає вимогам кафедри до написання пояснювальної записки дипломної роботи бакалавра, написана якісно і в доступній для ознайомлення формі.

Наведена дипломна робота та її результати свідчать про важливість і актуальність процесів інформаційної безпеки, посилення контролю доступу, моніторингу подій, захисту конфіденційної інформації, готовність до відновлення та реагування на інциденти, які забезпечать конфіденційність, цілісність та доступність інформаційних активів Цей факт дозволяє зробити висновок про те, що дипломна робота Семендя Б. А. має теоретичне і практичне значення, відповідає вимогам кваліфікаційної роботи, виконана на відповідному рівні і заслуговує позитивної оцінки, а здобувачу може бути присвоєно освітній рівень бакалавра за спеціальністю «Кібербезпека та захист інформації».

Науковий керівник

професор кафедри системного аналізу та кібербезпеки

Інституту інформаційних технологій в економіці

к.е.н., професор

Бегун А. В.

РЕЦЕНЗІЯ

на кваліфікаційну бакалаврську роботу

студента Семендя Богдана Андрійовича гр. ІК-401

на тему: «Дослідження та удосконалення системи управління інформаційною безпекою банківської установи»

Актуальність теми. Тема дипломної роботи є актуальною, оскільки банківські установи функціонують в умовах високої залежності від інформаційних систем, цифрових каналів обслуговування та постійного зростання кіберризиків. Забезпечення належного рівня інформаційної безпеки банку має важливе значення для захисту клієнтських даних, платіжної інформації, безперервності банківських процесів і виконання регуляторних вимог.

Наукова новизна. Наукова новизна роботи полягає в систематизації підходу до удосконалення системи управління інформаційною безпекою банківської установи на основі послідовного зв'язку між критичними об'єктами захисту, наявними механізмами інформаційної безпеки, виявленими прогалинами, ризиками та контрольними заходами їх зниження. У роботі запропоновано ризик-орієнтовану модель удосконалення СУІБ, адаптовану до специфіки банківської діяльності.

Якість проведеного аналізу. Аналіз у роботі проведено послідовно та логічно. Автор розкрив теоретичні засади СУІБ, охарактеризував особливості інформаційної безпеки у банківських установах, визначив критичні об'єкти захисту та розглянув наявні організаційні, програмні й технічні механізми забезпечення інформаційної безпеки. Окрему увагу приділено виявленню прогалин контрольного середовища та оцінюванню пов'язаних із ними ризиків за критеріями ймовірності та впливу.

Уміння користуватися літературними джерелами. У роботі використано літературні, нормативно-правові та інформаційні джерела. Автором опрацьовано міжнародні стандарти ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, нормативні документи Національного банку України, законодавчі акти України, а також

сучасні електронні ресурси та наукові публікації з питань інформаційної безпеки, кіберризиків і банківської діяльності.

Практична цінність висновків і рекомендацій. Практична цінність роботи полягає в результатах дослідження, що можуть бути використані як основа для оцінювання та удосконалення СУІБ реальної банківської установи. У роботі розроблено комплекс контрольних заходів із визначенням інструментів їх реалізації, відповідальних осіб, періодичності виконання та доказової бази. Запропоновані заходи спрямовані на посилення контролю доступу, моніторингу подій, захисту конфіденційної інформації, готовності до відновлення та реагування на інциденти.

Переваги та недоліки. До переваг роботи слід віднести логічну структуру, чіткий зв'язок між теоретичною, аналітичною та практичною частинами, використання ризик-орієнтованого підходу, а також конкретизацію запропонованих контрольних заходів. Недоліком роботи є те, що дослідження виконано на основі умовної моделі банківської установи, тому окремі висновки потребують додаткової перевірки під час практичного застосування в реальному банківському середовищі.

Загальний висновок і оцінка роботи. Дипломна робота є завершеним самостійним дослідженням, відповідає поставленій меті та завданням, має теоретичне і практичне значення. Зміст роботи свідчить про належний рівень підготовки автора, уміння аналізувати стан системи управління інформаційною безпекою, оцінювати ризики та формувати практичні рекомендації щодо її удосконалення. Робота заслуговує на позитивну оцінку.

РЕЦЕНЗЕНТ

керівник переддипломної практики

ТОВ EY Ukraine Digital

м. Київ, вул. Хрещатик, 19А

Провідний аналітик з Digital-ризиків

Матвієнко В. С.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ	4
ВСТУП.....	5
РОЗДІЛ 1 КОНЦЕПТУАЛЬНІ ЗАСАДИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ БАНКІВСЬКОЇ УСТАНОВИ.....	8
1.1 Сутність та принципи побудови системи управління інформаційною безпекою	8
1.2 Особливості забезпечення інформаційної безпеки у банківських установах	11
1.3 Нормативно-методичні підходи до оцінювання та удосконалення СУІБ банку	19
РОЗДІЛ 2 АНАЛІЗ ПОТОЧНОГО СТАНУ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ АТ “ДЕМО-БАНК”.....	24
2.1 Характеристика інформаційних активів та організаційної структури АТ “Демо-Банк”	24
2.2 Аналіз наявних механізмів забезпечення інформаційної безпеки АТ “Демо-Банк”	30
2.3 Оцінювання достатності механізмів СУІБ та пов’язаних ризиків інформаційної безпеки АТ “Демо-Банк”.....	40
РОЗДІЛ 3 УДОСКОНАЛЕННЯ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ АТ “ДЕМО-БАНК”	48
3.1 Формування цільової моделі удосконалення СУІБ АТ “Демо-Банк”	48
3.2 Розроблення та практична реалізація контрольних заходів для зниження ризиків СУІБ АТ “Демо-Банк”	52
3.2.1 Визначення принципів розробки контрольних заходів	52
3.2.2. Посилення автентифікації, перегляду доступів і контролю привілейованих облікових записів.....	58

3.2.3 Впровадження централізованого моніторингу та правил виявлення подій.....	62
3.2.4 Запровадження DLP-контролю для захисту конфіденційної інформації	64
3.2.5 Перегляд мережевої сегментації та правил міжсегментного доступу	65
3.2.6 Організація тестового відновлення та захисту резервних копій	67
3.2.7 Розроблення сценаріїв реагування на інциденти та програми навчання персоналу	68
3.2.8 Визначення етапності впровадження контрольних заходів	71
3.3 Оцінювання ефективності запропонованих заходів удосконалення СУІБ АТ “Демо-Банк”	72
ВИСНОВКИ.....	81
ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ	85

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ІБ – інформаційна безпека

СУІБ – система управління інформаційною безпекою

ІЗ – інформаційне забезпечення

ІС – інформаційна система

ІТ – інформаційні технології

БД – база даних

НБУ – Національний банк України

ISO – Міжнародна організація зі стандартизації

PDCA – цикл вдосконалення: планування, виконання, перевірка, дія

КІЦД – конфіденційність, цілісність, доступність

MFA – багатофакторна автентифікація

RBAC – рольова модель управління доступом

SIEM – система управління інформацією та подіями безпеки

EDR – система виявлення та реагування на загрози на кінцевих пристроях

DLP – система запобігання витоку даних

SOC – центр моніторингу та реагування на кіберінциденти

VPN – віртуальна приватна мережа

RTO – допустимий час відновлення після збою

RPO – допустимий обсяг втрати даних у часі

ВСТУП

У сучасних умовах банк є не лише фінансовою організацією, а й складною інформаційною системою, у межах якої щоденно обробляються значні обсяги персональних, фінансових, платіжних, операційних та управлінських даних. Від належного рівня захисту таких даних залежить безперервність банківських процесів, довіра клієнтів, виконання регуляторних вимог і здатність установи протидіяти внутрішнім та зовнішнім загрозам.

Особливої актуальності проблема управління інформаційною безпекою набуває для України, оскільки банківський сектор є одним із ключових елементів фінансової стабільності держави та критично важливої інфраструктури. В умовах воєнного стану, активної цифровізації фінансових послуг і зростання кількості кібератак банки стають однією з пріоритетних цілей для зловмисників. Порушення роботи банківських інформаційних систем може призвести не лише до технічних збоїв, а й до фінансових, репутаційних та соціально-економічних наслідків.

Дослідження та удосконалення системи управління інформаційною безпекою банківської установи є актуальним завданням, оскільки дозволяє перейти від фрагментарного застосування окремих засобів захисту до комплексного, ризик-орієнтованого та керованого підходу. Практична доцільність теми полягає у можливості виявити прогалини у СУІБ банку, оцінити пов'язані з ними ризики та розробити обґрунтовані заходи для підвищення рівня інформаційної безпеки, стійкості банківських процесів і готовності установи до сучасних кіберзагроз.

Проблематика управління інформаційною безпекою розглядається у працях багатьох вітчизняних і зарубіжних науковців та практиків. Значну увагу питанням захисту інформаційних ресурсів, управління ризиками, організації СУІБ та побудови систем інформаційної безпеки приділяли такі дослідники, як В.

Домарєв, В. Хорошко, О. Корченко, С. Євсєєв, С. Гнатюк, В. Бурячок, Ю. Даник, а також зарубіжні автори Б. Шнайєр, Р. Андерсон, К. Мітнік, Ю. Спеффорд та інші.

Метою даної кваліфікаційної роботи є дослідження системи управління інформаційною безпекою банківської установи, виявлення її основних прогалин та розробка обґрунтованих рекомендацій щодо підвищення рівня інформаційної безпеки.

Для досягнення мети кваліфікаційної роботи поставлені окремі завдання:

1. Розкрити сутність системи управління інформаційною безпекою та принципи її побудови.
2. Визначити особливості забезпечення інформаційної безпеки у банківських установах.
3. Узагальнити нормативно-методичні підходи до побудови, оцінювання та удосконалення СУІБ банку.
4. Охарактеризувати інформаційні активи, процеси та організаційні аспекти функціонування СУІБ банківської установи.
5. Проаналізувати наявні механізми забезпечення інформаційної безпеки.
6. Виявити основні прогалини у системі управління інформаційною безпекою та оцінити пов'язані з ними ризики.
7. Сформувати цільову модель удосконалення СУІБ банку.
8. Розробити комплекс практичних заходів підвищення рівня інформаційної безпеки із зазначенням відповідних інструментів, контролів і пріоритетів впровадження.
9. Оцінити очікувану ефективність запропонованих заходів шляхом порівняння рівня ризиків до та після їх реалізації.

Об'єктом дослідження є процес управління інформаційною безпекою банківської установи.

Предметом дослідження є теоретичні, методичні та практичні підходи до аналізу, оцінювання та удосконалення системи управління інформаційною безпекою банку.

У процесі вирішення поставлених завдань, у кваліфікаційній роботі використано: загальнонаукові та спеціальні методи дослідження. Метод аналізу застосовано для вивчення складових СУІБ, інформаційних активів, загроз і наявних механізмів захисту. Метод синтезу використано для узагальнення підходів до побудови цільової моделі СУІБ. Метод порівняння застосовано для зіставлення поточного стану системи інформаційної безпеки з бажаним цільовим станом. Метод класифікації використано для групування інформаційних активів, загроз, ризиків і заходів захисту. Метод експертного оцінювання застосовано для визначення рівня ризиків за критеріями ймовірності та впливу. Метод моделювання застосовано для формування цільової моделі удосконалення СУІБ банку. Розрахунковий метод використано для оцінювання рівня ризиків до та після впровадження запропонованих заходів.

Практична цінність роботи полягає в тому, що її результати можуть бути використані як основа для дослідження, оцінювання та удосконалення СУІБ реальної банківської установи. У роботі визначено типові прогалини в управлінні інформаційною безпекою банку, оцінено пов'язані з ними ризики та запропоновано комплекс контрольних заходів із конкретними інструментами реалізації, відповідальними особами, періодичністю виконання й доказовою базою. Запропонована модель дозволяє посилити контроль доступу, моніторинг подій, захист конфіденційної інформації, готовність до відновлення та реагування на інциденти, а також забезпечує більш керований і ризик-орієнтований підхід до розвитку системи управління інформаційною безпекою банку.

РОЗДІЛ 1

КОНЦЕПТУАЛЬНІ ЗАСАДИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ БАНКІВСЬКОЇ УСТАНОВИ

1.1 Сутність та принципи побудови системи управління інформаційною безпекою

Система управління інформаційною безпекою є складовою загальної системи управління організацією та спрямована на забезпечення належного рівня захисту інформаційних активів. Її призначення полягає у формуванні впорядкованого підходу до управління ризиками інформаційної безпеки, визначенні правил захисту інформації, розподілі відповідальності між учасниками процесу та контролі ефективності впроваджених заходів.

Інформаційна безпека в межах СУІБ розглядається не як окремий технічний захід, а як безперервний управлінський процес. Вона охоплює встановлення політик, оцінку ризиків, впровадження контрольних заходів, моніторинг подій, реагування на інциденти, проведення аудитів і постійне вдосконалення. Саме тому СУІБ має поєднувати організаційні, технічні, процедурні та кадрові заходи.

Основною метою СУІБ є забезпечення трьох базових властивостей інформації: **конфіденційності, цілісності та доступності**. Ці властивості формують основу інформаційної безпеки та визначають головні напрями захисту інформаційних активів.

Конфіденційність означає, що інформація має бути доступною лише для уповноважених осіб, систем або процесів. Її забезпечення передбачає контроль доступу, автентифікацію користувачів, розмежування прав, захист каналів передачі даних та запобігання несанкціонованому розкриттю інформації.

Цілісність передбачає збереження точності, повноти та достовірності інформації. Для її забезпечення застосовуються контроль змін, журналювання дій,

резервне копіювання, механізми перевірки коректності даних та обмеження несанкціонованого внесення змін.

Доступність означає, що інформаційні ресурси та сервіси мають бути доступними уповноваженим користувачам у необхідний момент часу. Вона забезпечується шляхом резервування, моніторингу, відмовостійкості, планування безперервності діяльності та процедур відновлення після збоїв або інцидентів.

Побудова СУІБ ґрунтується на низці принципів, які визначають її ефективність і практичну придатність [1].

Першим ключовим принципом є **ризик-орієнтований підхід**. Він передбачає, що заходи захисту мають визначатися на основі оцінки реальних ризиків для інформаційних активів. Тобто організація спочатку визначає активи, загрози, вразливості, ймовірність реалізації ризиків та можливий вплив, а вже потім обирає відповідні механізми захисту. Такий підхід дозволяє спрямовувати ресурси насамперед на найбільш критичні напрями.

Другим принципом є **комплексність**. СУІБ не може складатися лише з одного технічного засобу або окремого регламенту. Ефективний захист формується через поєднання політик, процедур, технічних засобів, навчання персоналу, моніторингу, аудиту та реагування на інциденти. Комплексність означає, що організаційні й технічні заходи мають доповнювати один одного.

Третім принципом є **безперервність управління**. Інформаційна безпека не є одноразовим заходом, оскільки загрози, технології, бізнес-процеси та вимоги регуляторів постійно змінюються. Тому СУІБ має регулярно переглядатися, перевірятися та вдосконалюватися [2].

У цьому контексті доцільно застосовувати цикл **PDCA: Plan - Do - Check - Act**. Ця модель дозволяє розглядати СУІБ як процес постійного вдосконалення, у межах якого заходи інформаційної безпеки не лише впроваджуються, а й систематично оцінюються та коригуються (рис. 1.1).



Рисунок 1.1 – Цикл PDCA у системі управління інформаційною безпекою

Джерело: Розроблено автором на основі [3]

- На етапі **Plan** визначаються контекст організації, інформаційні активи, ризики, цілі безпеки, політики та необхідні контролі.
- На етапі **Do** здійснюється впровадження запланованих заходів: процедур, технічних засобів, правил доступу, механізмів моніторингу та навчання персоналу.
- На етапі **Check** проводиться перевірка ефективності СУІБ: аудит, аналіз подій, оцінка результатів моніторингу, перевірка виконання політик і аналіз інцидентів.
- На етапі **Act** реалізуються коригувальні та покращувальні дії: оновлення політик, усунення недоліків, перегляд ризиків, зміна контролів і вдосконалення процесів [4].

Четвертим принципом є **принцип мінімальних привілеїв**. Він передбачає, що користувачі, адміністратори, сервіси та процеси повинні мати лише ті права, які необхідні для виконання визначених функцій. Надлишкові права підвищують ризик несанкціонованих дій, помилок і зловживань.

П'ятим принципом є **розмежування обов'язків**. Його сутність полягає в тому, що критичні дії не повинні повністю залежати від однієї особи. Наприклад, ініціювання, погодження, виконання та контроль важливих змін мають бути

розділені між різними ролями. Це знижує ризик зловживань, помилок і неконтрольованих операцій [5].

Шостим принципом є **документованість**. Політики, процедури, інструкції та регламенти інформаційної безпеки мають бути формалізовані, затверджені та доведені до відповідальних осіб. Документованість забезпечує єдине розуміння вимог, можливість контролю та основу для проведення аудиту [6].

Сьомим принципом є **підзвітність і контрольованість**. Будь-які суттєві дії користувачів, адміністраторів і систем повинні фіксуватися в журналах подій. Це дозволяє виявляти порушення, проводити розслідування інцидентів, оцінювати ефективність контролів і підтверджувати виконання встановлених вимог.

Восьмим принципом є **адаптивність**. СУІБ має змінюватися разом із розвитком організації, появою нових інформаційних систем, зміною загроз і оновленням нормативних вимог. Без адаптивності система безпеки швидко втрачає актуальність і перестає відповідати реальним ризикам [7].

Можна зробити висновок, що СУІБ є не окремим технічним рішенням, а системою управління, що забезпечує організований захист інформаційних активів. Її побудова має ґрунтуватися на забезпеченні конфіденційності, цілісності та доступності інформації, оцінці ризиків, комплексному застосуванні контролів, документованості процесів, підзвітності дій і постійному вдосконаленні за циклом PDCA. Саме такі принципи створюють основу для подальшого аналізу стану інформаційної безпеки банківської установи та визначення напрямів її удосконалення .

1.2 Особливості забезпечення інформаційної безпеки у банківських установах

Банківські установи належать до організацій, для яких інформаційна безпека має стратегічне значення. Це зумовлено тим, що банк у своїй діяльності обробляє значні обсяги фінансової, персональної, платіжної, службової та управлінської інформації. Порушення безпеки такої інформації може призвести не

лише до технічних збоїв, а й до фінансових втрат, порушення прав клієнтів, претензій з боку регулятора, репутаційних наслідків і зниження довіри до банківської установи [8].

На відміну від багатьох інших суб'єктів господарювання, банк виконує низку критично важливих функцій: забезпечує зберігання коштів, проведення платежів, відкриття та супровід рахунків, кредитування, дистанційне обслуговування клієнтів, формування фінансової і регуляторної звітності, а також взаємодію з іншими учасниками фінансової системи. Тому інформаційна безпека банку повинна розглядатися не як захист окремих комп'ютерів або програмних засобів, а як комплексна система заходів, спрямована на захист інформаційних ресурсів, інфраструктури, процесів, користувачів, каналів обміну даними та управлінських процедур [9].

Особливість забезпечення інформаційної безпеки у банківській сфері полягає у широкому колі об'єктів захисту. У межах СУІБ банку доцільно розглядати не тільки окремі масиви даних, а всю сукупність об'єктів, які мають значення для стабільного функціонування установи. До них належать інформація з обмеженим доступом, персональні дані клієнтів і працівників, фінансова та платіжна інформація, електронні банківські документи, дані регуляторної та управлінської звітності, облікові записи й автентифікаційні дані, журнали подій, інформаційна інфраструктура, а також критично важлива відкрита інформація банку (таблиця 1.1). Такий підхід дозволяє врахувати не лише конфіденційність даних, а й їхню цілісність, доступність, підзвітність та значення для безперервності діяльності банківської установи.

Таблиця 1.1 – Основні об'єкти захисту в системі управління інформаційною безпекою банку

Об'єкт захисту	Приклади	Значення для банку
1. Інформація з обмеженим доступом	банківська таємниця, комерційна таємниця, службова інформація	захист інтересів банку, клієнтів і партнерів; запобігання витоку критичної інформації

Продовження таблиці 1.1

Об'єкт захисту	Приклади	Значення для банку
2. Персональні дані клієнтів і працівників	ідентифікаційні, контактні, фінансові, кадрові дані	виконання вимог захисту персональних даних і забезпечення довіри клієнтів
3. Фінансова та платіжна інформація	дані про рахунки, платежі, транзакції, залишки, реквізити	забезпечення коректності та безперервності банківських операцій
4. Електронні банківські документи	платіжні доручення, договори, заявки, внутрішні погодження	підтвердження здійснення операцій, юридична значущість і контроль процесів
5. Дані регуляторної та управлінської звітності	фінансова звітність, управлінські звіти, регуляторні форми	забезпечення достовірності звітності та виконання вимог регулятора
6. Облікові записи та автентифікаційні дані	акаунти працівників, адміністраторів, сервісні облікові записи, ключі доступу	контроль доступу до ІС, запобігання несанкціонованим діям
7. Журнали подій та аудиторські записи	записи входів, змін прав, адміністративних дій, операцій у системах	підзвітність, розслідування інцидентів, підтвердження виконання контролів
8. Інформаційна інфраструктура	ІС, сервери, робочі станції, мережі, канали зв'язку, засоби захисту	забезпечення обробки, зберігання та передавання інформації
9. Критично важлива відкрита інформація	публічна звітність, офіційні повідомлення, інформація на сайті банку	підтримка довіри, репутації та доступності публічної інформації

Джерело: Розроблено автором

Висока критичність зазначених об'єктів захисту визначає підвищені вимоги до конфіденційності, цілісності та доступності інформації. Порухення конфіденційності може спричинити розкриття банківської таємниці, персональних даних клієнтів або службової інформації. Для банку це створює не лише

технічний ризик, а й ризик втрати довіри, репутаційних втрат і претензій з боку клієнтів або регулятора [10].

Не менш важливою є цілісність інформації. Для банківської установи коректність даних має принципове значення, оскільки фінансові операції, залишки на рахунках, реквізити платежів, електронні документи, звітність і управлінські рішення залежать від точності та незмінності інформації. Несанкціонована або помилкова зміна даних може призвести до спотворення фінансової інформації, некоректного виконання операцій, помилок у звітності або неправомірних дій у банківських процесах.

Доступність також є критичною характеристикою інформаційної безпеки банку. Банківські послуги мають надаватися стабільно, а критичні процеси повинні залишатися доступними навіть у разі технічних збоїв, кібератак, помилок адміністрування або інших інцидентів. Тому інформаційна безпека банку безпосередньо пов'язана з резервним копіюванням, плануванням відновлення, відмовостійкістю, моніторингом критичних сервісів і визначенням допустимого часу простою [11].

Для банківських установ характерною є одночасна дія зовнішніх і внутрішніх загроз. Загрози можуть бути спрямовані не лише на викрадення інформації, а й на порушення її цілісності, блокування доступу до сервісів, компрометацію облікових записів, зміну платіжних реквізитів, несанкціоноване використання привілеїв або порушення нормальної роботи банківських процесів. До типових зовнішніх загроз належать фішинг, шкідливе програмне забезпечення, ransomware, DDoS-атаки, атаки на вебресурси, атаки на API, brute force та password spraying. До внутрішніх загроз належать надлишкові права доступу, помилки персоналу, зловживання повноваженнями, порушення процедур, формальне виконання політик безпеки та недостатній контроль адміністративних дій [12].

Окрему увагу слід приділяти загрозам, пов'язаним із третіми сторонами. Банківська установа взаємодіє з постачальниками, підрядниками, сервісними організаціями, хмарними платформами, платіжними провайдерами та іншими

зовнішніми учасниками. Якщо такі сторони мають доступ до інформаційних систем, даних або каналів інтеграції, це створює додаткові ризики для конфіденційності, цілісності та доступності інформації.

Наведені групи загроз демонструють, що інформаційна безпека банку не може забезпечуватися лише окремими технічними засобами. Наприклад, міжмережевий екран може обмежувати мережевий трафік, але не усуває ризик фішингу; антивірусний захист може виявляти частину шкідливого програмного забезпечення, але не гарантує захисту від зловживання легітимними обліковими записами; резервне копіювання допомагає відновити дані, але не запобігає їх витоку. Тому СУІБ банку повинна поєднувати превентивні, детективні та коригувальні заходи.

Суттєвим чинником ризику для банків є компрометація облікових записів. Обліковий запис працівника, адміністратора або сервісного користувача може бути використаний як точка входу до інформаційних систем. У зв'язку з цим особливого значення набувають автентифікація, багатофакторний захист доступу, принцип мінімальних привілеїв, регулярний перегляд прав, контроль привілейованих облікових записів і журналювання дій користувачів [13].

Водночас забезпечення інформаційної безпеки банку не може зводитися лише до управління доступом. Ефективна СУІБ повинна поєднувати управління ризиками, захист інформаційних ресурсів, захист інформаційної інфраструктури, технічні та організаційні контролю, моніторинг подій, реагування на інциденти, навчання персоналу, резервне копіювання, аудит і забезпечення безперервності діяльності. Саме взаємозв'язок цих напрямів дозволяє не лише запобігати інцидентам, а й своєчасно їх виявляти, локалізувати та зменшувати наслідки [14].

Особливу роль у банківській СУІБ відіграє моніторинг подій інформаційної безпеки. У процесі діяльності банку формується велика кількість подій, що можуть свідчити як про штатну роботу систем, так і про потенційні порушення безпеки. До таких подій належать успішні та невдалі входи, зміни прав доступу, адміністративні дії, мережеві підключення, операції з даними, спрацювання

засобів захисту, події резервного копіювання, а також повідомлення користувачів про підозрілу активність (таблиця 1.2).

Таблиця 1.2 – Основні джерела подій інформаційної безпеки банківської установи

Джерело подій	Приклади подій	Значення для СУІБ
Active Directory	успішні та невдалі входи, зміни груп, блокування акаунтів	контроль доступу та виявлення компрометації
MFA / VPN	підключення з нетипових локацій, відмови MFA, нові пристрої	контроль віддаленого доступу
Робочі станції	запуск підозрілих процесів, зараження malware, підключення USB	виявлення загроз на endpoint
Сервери	помилки служб, зміни конфігурації, підозрілі процеси	контроль стабільності та безпеки систем
Firewall / IDS / IPS	заблоковані з'єднання, сканування портів, підозрілий трафік	виявлення мережових атак
Банківські прикладні системи	помилки авторизації, нетипові операції, зміни параметрів	контроль бізнес-критичних дій
Бази даних	запити до критичних таблиць, зміни даних, помилки доступу	контроль цілісності та конфіденційності даних
Файлові ресурси	масове копіювання, видалення, зміна файлів	виявлення витоку або пошкодження інформації
DLP	спроби пересилання конфіденційних даних	запобігання витоку інформації
Backup-системи	успішні/невдалі копії, спроби видалення backup	контроль готовності до відновлення
Service Desk	повідомлення про фішинг, збої, підозрілі листи	джерело первинної інформації про інциденти
Зовнішні сервіси/API	помилки інтеграцій, аномальні запити, недоступність сервісу	контроль ризиків третіх сторін

Джерело: Розроблено автором

Якщо такі події не збираються, не аналізуються та не корелюються, банк може несвоєчасно виявити інцидент або не мати достатньої доказової бази для його розслідування.

Не менш важливою особливістю є необхідність формалізованого реагування на інциденти. Для банку недостатньо лише зафіксувати факт підозрілої події або порушення. Необхідно визначити порядок аналізу події, критерії класифікації інциденту, відповідальних осіб, порядок ескалації, дії з локалізації, усунення наслідків, відновлення роботи та документування результатів. Відсутність таких процедур може призвести до затримок у реагуванні, неузгодженості дій і збільшення наслідків інциденту [15].

Інформаційна безпека банківської установи також має враховувати людський фактор. Навіть за наявності сучасних технічних засобів захисту працівники можуть залишатися джерелом ризику через необережність, недостатню обізнаність, порушення процедур, використання слабких паролів, відкриття фішингових повідомлень або неправильну обробку конфіденційної інформації. Тому навчання персоналу, інформування про актуальні загрози та формування культури інформаційної безпеки є необхідними елементами СУІБ банку.

Важливою складовою інформаційної безпеки банку є підзвітність і доказовість. Банківська установа повинна мати можливість підтвердити, що встановлені вимоги безпеки фактично виконуються. Для цього необхідні журнали подій, записи аудиту, документи з оцінки ризиків, звіти про інциденти, результати перевірок, підтвердження виконання контрольних процедур і докази усунення виявлених недоліків. Підзвітність особливо важлива для процесів, пов'язаних із доступом до критичних ресурсів, адміністративними діями, обробкою конфіденційної інформації та реагуванням на інциденти.

Забезпечення інформаційної безпеки у банківських установах має чітко регламентований характер. Банки повинні враховувати вимоги законодавства, нормативні акти регулятора, міжнародні стандарти та внутрішні політики. Така регламентація зумовлена тим, що банківська діяльність має високий рівень суспільної значущості, а порушення безпеки може впливати не лише на окрему установу, а й на клієнтів, партнерів та фінансову систему загалом. Окрім цього,

банківська СУІБ повинна бути здатною підтверджувати не лише наявність захисних заходів, а й їх фактичне виконання та ефективність [16].

Отже, забезпечення інформаційної безпеки у банківських установах має комплексний, регламентований і ризик-орієнтований характер. Воно охоплює захист інформаційних ресурсів, інформаційної інфраструктури, процесів обробки даних, облікових записів, журналів подій, каналів взаємодії та зовнішніх залежностей. Особливість банківської сфери полягає у високій цінності інформаційних ресурсів, значній залежності від інформаційних технологій, необхідності безперервного функціонування, постійній дії зовнішніх і внутрішніх загроз, а також потребі підтверджувати виконання вимог безпеки.

З огляду на це СУІБ банку має функціонувати як цілісна система управління, яка поєднує організаційні, технічні та процедурні заходи. Її ефективність залежить не лише від наявності окремих засобів захисту, а й від здатності банку своєчасно виявляти події безпеки, оцінювати ризики, реагувати на інциденти, забезпечувати безперервність діяльності та постійно вдосконалювати контрольні механізми.

1.3 Нормативно-методичні підходи до оцінювання та удосконалення СУІБ банку

Побудова, оцінювання та удосконалення системи управління інформаційною безпекою банківської установи мають здійснюватися з урахуванням нормативно-методичної бази. Це пояснюється тим, що СУІБ не може формуватися довільно або лише на основі окремих технічних рішень. Вона повинна спиратися на міжнародні стандарти, вимоги регулятора, ризик-орієнтований підхід, внутрішні політики та реальні потреби банку щодо захисту інформаційних ресурсів, управління доступом, моніторингу подій, реагування на інциденти та забезпечення безперервності діяльності.

Нормативно-методичні підходи виконують декілька функцій (таблиця 1.3). По-перше, вони визначають загальну логіку побудови СУІБ. По-друге, дають

орієнтири для вибору контрольних заходів. По-третє, дозволяють оцінити поточний стан інформаційної безпеки та виявити прогалини. По-четверте, створюють основу для оцінювання ризиків і розроблення заходів удосконалення.

Таблиця 1.3 – Стандарти та регуляторні вимоги, що застосовуються в управлінні інформаційною безпекою банку

Документ / підхід	Характеристика	Основний фокус	Значення для СУІБ банку
ISO/IEC 27001	Міжнародний стандарт, що встановлює вимоги до створення, впровадження, підтримання та постійного вдосконалення СУІБ	Побудова системи управління інформаційною безпекою	Визначає загальну логіку функціонування СУІБ: політики, ризики, відповідальність, аудит, моніторинг і вдосконалення
ISO/IEC 27002	Практичний стандарт-рекомендація, що містить перелік контрольних заходів інформаційної безпеки	Контролі інформаційної безпеки	Допомагає визначити, які організаційні, технічні та процедурні заходи доцільно застосовувати для захисту інформаційних ресурсів банку
ISO/IEC 27005	Стандарт, що описує підхід до управління ризиками інформаційної безпеки	Ідентифікація, оцінювання та оброблення ризиків	Дає методичну основу для оцінки ризиків, пов'язаних із загрозами, вразливостями та прогалинами в СУІБ
Нормативні вимоги НБУ	Обов'язкові для банків України вимоги регулятора щодо інформаційної безпеки, кіберзахисту та управління ризиками	Банківська специфіка, кіберзахист, регуляторна відповідність	Забезпечують прив'язку СУІБ до вимог банківського сектору України, критичних процесів, відповідальності банку та очікувань регулятора

Джерело: Розроблено автором

Опираючись на характеристики надані вище, можна впевнитись, що документи виконують різні, але взаємопов'язані функції: ISO/IEC 27001 визначає загальну модель СУІБ, ISO/IEC 27002 деталізує контрольні заходи, ISO/IEC 27005

формує підхід до управління ризиками, а нормативні вимоги НБУ забезпечують урахування специфіки банківської діяльності в Україні. Саме поєднання цих підходів дозволяє розглядати СУІБ банку не як набір окремих технічних засобів, а як цілісну систему управління інформаційною безпекою.

Основним міжнародним стандартом у сфері побудови системи управління інформаційною безпекою є ISO/IEC 27001. Він визначає вимоги до створення, впровадження, підтримання та постійного вдосконалення СУІБ. Ключова ідея стандарту полягає в тому, що інформаційна безпека має бути інтегрована в загальну систему управління організацією, а не існувати у вигляді окремих технічних або адміністративних заходів [17].

Для банківської установи значення ISO/IEC 27001 полягає в тому, що він задає структуровану логіку управління інформаційною безпекою. Стандарт передбачає визначення контексту організації, сфери застосування СУІБ, політики інформаційної безпеки, ролей і відповідальності, підходу до оцінювання ризиків, вибору заходів оброблення ризиків, документування процесів, внутрішнього аудиту, перегляду з боку керівництва та постійного вдосконалення [18].

Доповненням до ISO/IEC 27001 є ISO/IEC 27002. Якщо ISO/IEC 27001 визначає вимоги до системи управління, то ISO/IEC 27002 містить рекомендації щодо конкретних контрольних заходів інформаційної безпеки. Його практична цінність полягає в тому, що він допомагає визначити, які саме організаційні, технічні та процедурні контролю можуть застосовуватися для зниження ризиків інформаційної безпеки.

Для банківської установи такі контролю можуть стосуватися управління доступом, захисту інформаційних ресурсів, безпеки персоналу, захисту кінцевих пристроїв, мережевого захисту, журналювання та моніторингу подій, резервного копіювання, реагування на інциденти, управління постачальниками та забезпечення безперервності діяльності. Тобто ISO/IEC 27002 є корисним не як формальний перелік вимог, а як практичний орієнтир для оцінювання того, які напрями СУІБ реалізовані достатньо, а які потребують посилення [19].

Окреме значення має ISO/IEC 27005, який стосується управління ризиками інформаційної безпеки. Для СУІБ банку ризик-орієнтований підхід є принциповим, оскільки не всі загрози та не всі об'єкти захисту мають однаковий рівень критичності. Одні прогалини можуть мати обмежений вплив, тоді як інші здатні призвести до витоку конфіденційної інформації, компрометації облікових записів, порушення цілісності даних або недоступності критичних банківських сервісів.

Для банківських установ України важливе значення мають також нормативні вимоги Національного банку України. Якщо міжнародні стандарти ISO формують загальну методичну основу управління інформаційною безпекою, то вимоги НБУ конкретизують цю логіку саме для банківського сектору України. Це важливо, оскільки банк є не просто суб'єктом господарювання, а фінансовою установою, діяльність якої має підвищену суспільну значущість і регуляторний контроль [20].

Нормативні вимоги НБУ доцільно розглядати як основу для врахування банківської специфіки під час аналізу СУІБ. Вони акцентують увагу на необхідності управління кіберризиками, захисту банківської інформації, забезпечення безперервності діяльності, контролю доступу, моніторингу подій, реагування на інциденти, оцінювання стану кіберзахисту та відповідальності банку за належну організацію процесів інформаційної безпеки.

Кожен із розглянутих нормативно-методичних підходів виконує конкретну роль у межах дослідження. ISO/IEC 27001 використовується як загальна основа побудови та оцінювання СУІБ. ISO/IEC 27002 дає орієнтир для аналізу контрольних заходів і формування рекомендацій. ISO/IEC 27005 забезпечує методичну основу для оцінювання ризиків. Нормативні вимоги НБУ дозволяють врахувати специфіку банківської діяльності, регуляторні очікування та підвищену критичність інформаційної безпеки у фінансовому секторі.

Отже, нормативно-методична база є необхідною основою для системного дослідження СУІБ банківської установи. Її використання дозволяє проводити аналіз не хаотично, а послідовно: від визначення вимог і контрольних напрямів до

виявлення прогалин, оцінювання ризиків і розроблення практичних заходів підвищення рівня інформаційної безпеки. Саме такий підхід забезпечує зв'язок між теоретичними засадами, аналітичною частиною та практичними рекомендаціями щодо удосконалення СУІБ банку.

РОЗДІЛ 2

АНАЛІЗ ПОТОЧНОГО СТАНУ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ АТ “ДЕМО-БАНК”

2.1 Характеристика інформаційних активів та організаційної структури АТ “Демо-Банк”

Для проведення аналізу стану системи управління інформаційною безпекою необхідно визначити загальний контекст досліджуваної банківської установи, основні категорії інформації, критичні інформаційні активи та організаційні ролі, що беруть участь у функціонуванні СУІБ. У межах цієї роботи використовується узагальнена модель банківської установи — АТ “Демо-Банк”. Назва є умовною та застосовується виключно для опису типових інформаційних активів, процесів, організаційної структури та механізмів інформаційної безпеки, характерних для банківського сектору.

Робота не містить конфіденційної інформації реальної банківської установи. Кількісні фінансово-економічні показники АТ “Демо-Банк” у роботі не деталізуються, оскільки предметом дослідження є не господарська діяльність банку, а система управління інформаційною безпекою, її поточний стан, прогалини та напрями удосконалення.

АТ “Демо-Банк” розглядається як банківська установа середнього масштабу, що здійснює обслуговування фізичних та юридичних осіб, забезпечує проведення платежів, відкриття та супровід рахунків, кредитування, дистанційне банківське обслуговування, формування звітності та виконання внутрішніх управлінських процесів. У процесі такої діяльності банк обробляє значні обсяги інформації різного рівня критичності, зокрема персональні дані, фінансову інформацію, платіжні дані, службову інформацію, управлінську та регуляторну звітність (таблиця 2.1).

Таблиця 2.1 – Загальна характеристика діяльності АТ “Демо-Банк”

Характеристика	Опис
Тип установи	банківська установа, що здійснює обслуговування фізичних та юридичних осіб
Масштаб моделі	банківська установа середнього масштабу з типовими процесами банківського сектору
Формат діяльності	поєднання роботи центрального офісу, відділень і дистанційних каналів обслуговування
Основні напрями діяльності	відкриття та супровід рахунків, проведення платежів, кредитування, обслуговування клієнтів, формування звітності
Основні категорії клієнтів	фізичні особи, малі та середні підприємства, корпоративні клієнти
Основні категорії користувачів	працівники фронт-офісу, бек-офісу, керівники, ІТ-персонал, працівники підрозділу ІБ, внутрішній аудит, зовнішні підрядники з обмеженим доступом
Основні категорії інформації	персональні дані, платіжна інформація, фінансова інформація, службова інформація, регуляторна та управлінська звітність

Джерело: Розроблено автором

У процесі діяльності АТ “Демо-Банк” інформація створюється, обробляється, передається, зберігається та використовується в різних банківських процесах. Однак не всі інформаційні ресурси мають однаковий рівень критичності. Для аналізу СУІБ доцільно виділити саме ті активи, порушення конфіденційності, цілісності або доступності яких може безпосередньо вплинути на виконання банківських операцій, обслуговування клієнтів, формування звітності або безперервність діяльності банку.

До критичних об’єктів СУІБ АТ “Демо-Банк” доцільно віднести ті інформаційні ресурси, системи, облікові сутності та допоміжні компоненти, порушення безпеки яких може безпосередньо вплинути на виконання банківських операцій, обслуговування клієнтів, формування звітності або безперервність діяльності. До таких об’єктів належать клієнтські дані, платіжна та транзакційна інформація, основна банківська система, система дистанційного банківського

обслуговування, фінансова, управлінська та регуляторна звітність, привілейовані облікові записи й автентифікаційні дані, журнали подій, резервні копії критичних систем і даних, а також канали інтеграції та обміну даними (таблиця 2.2).

Таблиця 2.2 – Критичні об’єкти СУІБ АТ “Демо-Банк”

Критичний об’єкт СУІБ	Що включає	Критична властивість	Можливий наслідок порушення
Клієнтські дані	персональні, контактні, ідентифікаційні та фінансові дані	конфіденційність, цілісність	витік даних, претензії клієнтів, репутаційні втрати
Платіжна та транзакційна інформація	реквізити, платежі, транзакції, залишки	цілісність, доступність	некоректні платежі, фінансові втрати
Основна банківська система	операції, рахунки, клієнтські профілі	доступність, цілісність	зупинка ключових банківських процесів
Система дистанційного банківського обслуговування	інтернет-банкінг, мобільний банкінг, клієнтські сесії	доступність, конфіденційність, цілісність	недоступність сервісів, шахрайські операції
Фінансова, управлінська та регуляторна звітність	звіти, регуляторні форми, управлінські показники	цілісність, доступність	недостовірна звітність, претензії регулятора
Привілейовані облікові записи та автентифікаційні дані	адміністративні акаунти, сервісні акаунти, ключі доступу	конфіденційність, підзвітність	несанкціонований доступ, зміна налаштувань
Журнали подій та аудиторські записи	входи, зміни прав, адміністративні дії, операції	цілісність, доступність	неможливість розслідувати інцидент
Резервні копії критичних систем і даних	копії БД, конфігурацій, системних станів	доступність, цілісність	неможливість відновлення після збою або атаки

Продовження таблиці 2.2

Критичний об'єкт СУІБ	Що включає	Критична властивість	Можливий наслідок порушення
Канали інтеграції та обміну даними	API, обмін із зовнішніми сервісами, платіжними й регуляторними системами	конфіденційність, цілісність, доступність	порушення обміну даними, витік або спотворення інформації

Джерело: Розроблено автором

Зазначені вище активи (об'єкти) використовуються у ключових процесах АТ “Демо-Банк”, зокрема під час обслуговування клієнтів, відкриття та супроводу рахунків, проведення платежів, кредитування, дистанційного банківського обслуговування, формування звітності, управління доступом, моніторингу подій, резервного копіювання та реагування на інциденти. Це означає, що захист критичних активів не може розглядатися ізолювано від процесів, у межах яких вони використовуються.

Суттєве значення для СУІБ має також організаційна структура управління інформаційною безпекою (рис 2.1).

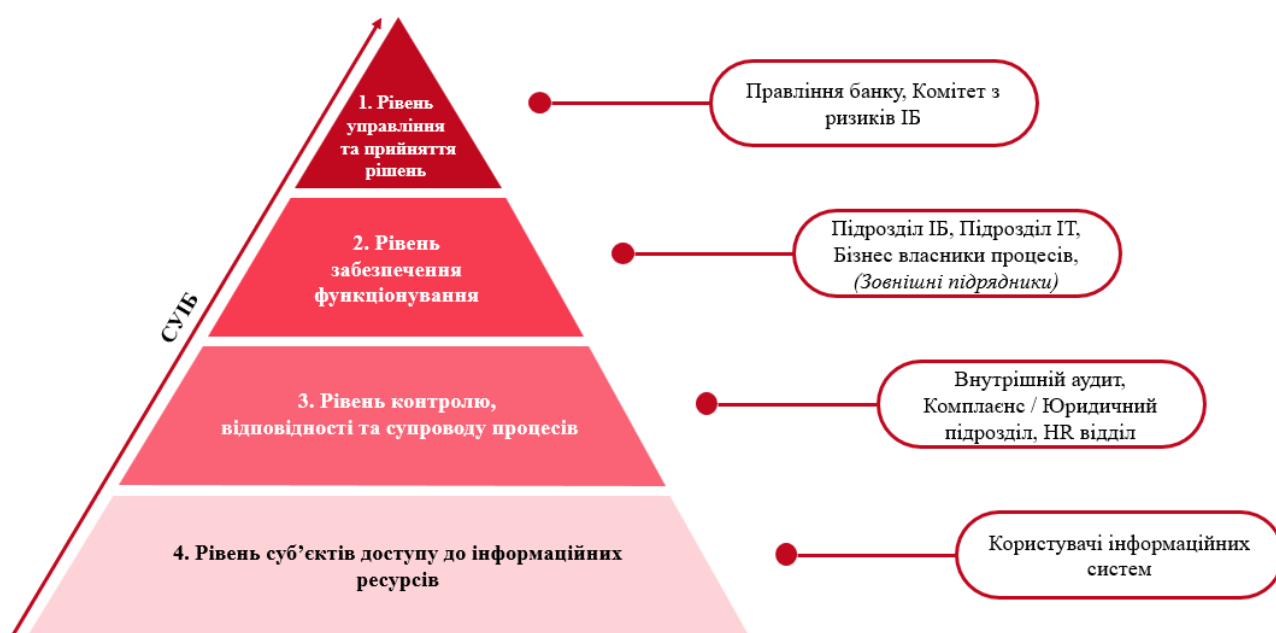


Рисунок 2.1 – Організаційна структура функціонування СУІБ банку

Джерело: Розроблено автором

Захист інформації в банку не може забезпечуватися виключно технічними засобами, оскільки СУІБ передбачає розподіл відповідальності, затвердження політик, контроль виконання вимог, оцінювання ризиків, реагування на інциденти та проведення внутрішніх перевірок. Тому в забезпеченні інформаційної безпеки беруть участь не лише ІТ- та ІБ-підрозділи, а й керівництво, власники бізнес-процесів, комплаєнс, внутрішній аудит, HR, користувачі інформаційних систем і зовнішні підрядники з обмеженим доступом [21].

Керівництво банку визначає загальні пріоритети інформаційної безпеки, затверджує політики та забезпечує ресурси для функціонування СУІБ. Підрозділ інформаційної безпеки відповідає за методологію, оцінювання ризиків, контроль виконання вимог, моніторинг подій та координацію реагування на інциденти. ІТ-підрозділ забезпечує технічну реалізацію заходів захисту, підтримку інфраструктури та адміністрування інформаційних систем. Внутрішній аудит перевіряє ефективність контролів, а комплаєнс і юридичний підрозділ контролюють відповідність вимогам законодавства, регулятора та внутрішніх документів (таблиця 2.3).

Таблиця 2.3 – Ролі підрозділів АТ “Демо-Банк” у забезпеченні функціонування СУІБ

Підрозділ / роль	Функції в межах СУІБ
Правління банку	затвердження політик інформаційної безпеки, визначення стратегічних пріоритетів, забезпечення ресурсів для функціонування СУІБ
Комітет з ризиків ІБ	розгляд питань ризиків ІБ, погодження пріоритетів захисту, контроль виконання ключових заходів
Підрозділ ІБ	розробка вимог і політик ІБ, оцінювання ризиків, контроль виконання заходів, координація реагування на інциденти
Підрозділ ІТ	адміністрування систем, підтримка інфраструктури, впровадження технічних засобів захисту, резервне копіювання
Власники бізнес-процесів	визначення критичності процесів та інформації, погодження доступів, участь в оцінці ризиків

Продовження таблиці 2.3

Підрозділ / роль	Функції в межах СУІБ
Внутрішній аудит	перевірка ефективності контролів, оцінка відповідності політикам і процедурам, формування рекомендацій
Комплаєнс / Юридичний підрозділ	контроль відповідності вимогам законодавства, регулятора, договорів і внутрішніх нормативних документів
HR відділ	участь у процесах прийняття, переведення та звільнення працівників, організація навчання з питань інформаційної безпеки
Користувачі інформаційних систем	дотримання політик ІБ, коректне використання доступів, повідомлення про підозрілі події
Зовнішні підрядники з обмеженим доступом	виконання робіт у межах погоджених повноважень, дотримання вимог банку щодо захисту інформації

Джерело: Розроблено автором

Розподіл ролей у межах СУІБ має важливе значення, оскільки інформаційна безпека залежить не лише від наявності технічних рішень, а й від чіткості управлінських процедур. Якщо відповідальність між підрозділами не визначена або визначена формально, це може призвести до несвоєчасного реагування на інциденти, затримок у відкликанні доступу, недостатнього контролю виконання політик або неузгодженості дій між ІТ, ІБ та бізнес-підрозділами.

Резюмуючи, було визначено профіль АТ “Демо-Банк”, критичні інформаційні активи та основні організаційні ролі, що беруть участь у функціонуванні СУІБ. Що створює основу для подальшого аналізу програмних, технічних та організаційних механізмів забезпечення інформаційної безпеки. У наступному підрозділі буде розглянуто, які засоби використовуються для захисту визначених активів, підтримання контрольованості процесів і зниження ризиків інформаційної безпеки.

2.2 Аналіз наявних механізмів забезпечення інформаційної безпеки АТ “Демо-Банк”

Після визначення контексту діяльності АТ “Демо-Банк”, критичних активів та об’єктів захисту СУІБ доцільно перейти до аналізу наявних механізмів забезпечення інформаційної безпеки. Оскільки АТ “Демо-Банк” є модельною банківською установою, у межах дослідження фіксується умовний поточний стан його СУІБ, який відображає типовий набір організаційних, програмних і технічних засобів захисту для банківської установи середнього масштабу.

Подальший аналіз зазначених механізмів здійснюється за такими напрямками: управління доступом, захист кінцевих пристроїв та інфраструктури, захист інформаційних ресурсів, журналювання і моніторинг подій, резервне копіювання та відновлення, реагування на інциденти, а також організаційне забезпечення СУІБ.

Управління доступом. В АТ “Демо-Банк” централізоване управління користувачами здійснюється за допомогою Microsoft Active Directory. Ця служба каталогів використовується для створення доменних облікових записів працівників, об’єднання користувачів у групи безпеки, надання доступу до файлових ресурсів, внутрішніх систем і окремих адміністративних функцій.

Для налаштування базових параметрів безпеки використовуються Group Policy Objects. Через групові політики встановлюються вимоги до складності паролів, строку їх дії, блокування облікового запису після невдалих спроб входу, обмеження запуску окремого програмного забезпечення, налаштування параметрів робочих станцій і базові правила використання зовнішніх носіїв.

Доступ до ресурсів надається через групи безпеки Active Directory. Окремі групи застосовуються для працівників фронт-офісу, бек-офісу, ІТ-персоналу, працівників підрозділу інформаційної безпеки, керівників і зовнішніх підрядників з обмеженим доступом. Такий підхід дозволяє реалізувати розмежування прав відповідно до функціональних обов’язків користувачів.

Для віддаленого доступу до внутрішніх ресурсів використовується VPN із частковим застосуванням MFA. Багатофакторна автентифікація використовується переважно для VPN-доступу, однак не охоплює всі критичні внутрішні системи та адміністративні дії. Це створює потенційне обмеження, оскільки компрометація пароля користувача може залишатися достатньою умовою для доступу до окремих ресурсів.

Окрему групу ризику становлять привілейовані облікові записи: адміністративні акаунти, сервісні облікові записи та облікові записи інтеграцій. Вони використовуються для адміністрування систем, виконання службових процесів і технічної взаємодії між системами [22]. Основним обмеженням є потреба в регулярному перегляді таких акаунтів, контролі їхніх дій і посиленій автентифікації (таблиця 2.4).

Таблиця 2.4 – Аналіз засобів управління доступом АТ “Демо-Банк”

Засіб / механізм	Як використовується	Потенційне обмеження
Microsoft Active Directory	централізоване управління доменними обліковими записами, групами користувачів і доступом до ресурсів	ризик накопичення неактуальних або надлишкових прав доступу
Group Policy Objects	налаштування паролівних політик, блокування акаунтів, параметрів безпеки робочих станцій	потреба в регулярному перегляді та актуалізації політик
Групи безпеки AD	надання доступу до файлових ресурсів і внутрішніх систем відповідно до ролей	можливе збереження зайвих доступів після зміни функцій працівника
Парольні політики	встановлення вимог до складності, строку дії та блокування після невдалих входів	недостатній рівень захисту без MFA для критичних систем
MFA для VPN	додаткове підтвердження особи під час віддаленого доступу	MFA не охоплює всі критичні внутрішні системи
Привілейовані облікові записи	адміністрування систем, сервісів та критичних ресурсів	потреба в посиленому контролі, журналюванні та регулярному перегляді

Джерело: Розроблено автором

Захист кінцевих пристроїв та інфраструктури. Для захисту робочих станцій і серверів в АТ “Демо-Банк” використовується Microsoft Defender for Endpoint. Він забезпечує базове виявлення шкідливого програмного забезпечення, контроль підозрілої активності на кінцевих пристроях і централізоване отримання подій безпеки. Водночас ефективність цього засобу залежить від повноти налаштування політик, регулярного аналізу спрацювань і інтеграції з процесом реагування на інциденти.

Для управління оновленнями використовується Windows Server Update Services. Через WSUS здійснюється централізоване розповсюдження оновлень операційних систем і програмного забезпечення Microsoft. Основним обмеженням є ризик затримки встановлення критичних оновлень, якщо процес погодження, тестування або розгортання патчів займає надто багато часу.

Мережевий захист в АТ “Демо-Банк” забезпечується міжмережевим екраном FortiGate. Він використовується для фільтрації трафіку, контролю доступу між мережевими зонами, VPN-підключень і журналювання мережевих подій. Також у банку застосовується VLAN-сегментація та ACL для розмежування користувацьких, серверних і адміністративних сегментів мережі.

Водночас мережеві правила та винятки потребують регулярного перегляду. Якщо правила firewall або ACL не актуалізуються, у мережі можуть залишатися надлишкові дозволи між сегментами. Це підвищує ризик lateral movement у разі компрометації окремого облікового запису або робочої станції (таблиця 2.5).

Таблиця 2.5 – Аналіз технічних засобів захисту інфраструктури АТ “Демо-Банк”

Засіб / механізм	Як використовується	Потенційне обмеження
Microsoft Defender for Endpoint	захист робочих станцій і серверів, виявлення malware та підозрілої активності	потреба в належному налаштуванні політик і регулярному аналізі спрацювань
WSUS	централізоване встановлення оновлень ОС і програмного забезпечення	ризик затримки встановлення критичних оновлень

Продовження таблиці 2.5

Засіб / механізм	Як використовується	Потенційне обмеження
Контроль USB через GPO	обмеження використання зовнішніх носіїв на робочих станціях	контроль може бути застосований не до всіх категорій користувачів
FortiGate Firewall	фільтрація мережевого трафіку, контроль периметра, VPN, журналювання	потреба в регулярному перегляді правил і винятків
VPN	захищений віддалений доступ до внутрішніх ресурсів банку	ризик несанкціонованого доступу без повного MFA та контролю сесій
VLAN / ACL	сегментація мережі та обмеження взаємодії між сегментами	можлива надмірна відкритість між окремими мережевими зонами
IDS/IPS-функції FortiGate	виявлення та блокування частини підозрілого мережевого трафіку	потреба в налаштуванні сигнатур і регулярному аналізі спрацювань

Джерело: Розроблено автором

Захист інформаційних ресурсів, журналювання та резервне копіювання. Для контролю доступу до файлових ресурсів в АТ “Демо-Банк” використовуються NTFS permissions у поєднанні з групами безпеки Active Directory. Це дозволяє надавати доступ до папок і файлів відповідно до ролей, підрозділів і службових потреб користувачів.

Для захисту даних на ноутбуках і робочих станціях використовується BitLocker. Шифрування дисків знижує ризик розкриття інформації у разі втрати або викрадення пристрою. Водночас BitLocker не контролює подальше передавання даних після того, як користувач отримав авторизований доступ до системи.

Для баз даних застосовуються вбудовані механізми контролю доступу, журналювання змін і обмеження дій користувачів відповідно до їхніх повноважень. Передавання даних між окремими системами здійснюється через захищені з'єднання. Водночас повноцінне DLP-рішення в АТ “Демо-Банк” не впроваджене, що обмежує можливості контролю копіювання, пересилання або вивантаження конфіденційної інформації.

Журналювання подій здійснюється за допомогою Windows Event Log, журналів Active Directory, журналів FortiGate, VPN-журналів, подій Microsoft Defender та журналів окремих прикладних систем. Ці джерела дозволяють фіксувати успішні й невдалі входи, зміни прав доступу, адміністративні дії, мережеві підключення та спрацювання засобів захисту.

Разом з тим у поточній моделі АТ “Демо-Банк” відсутнє повноцінне централізоване SIEM-рішення. Окремі журнали зберігаються та аналізуються локально або періодично відповідальними працівниками. Це ускладнює кореляцію подій між різними системами та може призводити до пізнього виявлення інцидентів.

Для резервного копіювання критичних серверів, баз даних і конфігурацій використовується Veeam Backup & Replication. Резервні копії створюються для основних систем і даних, необхідних для відновлення після технічних збоїв, помилок користувачів або кібератак. Водночас тестування відновлення проводиться нерегулярно, а захист резервних копій від несанкціонованого видалення або шифрування потребує посилення (таблиця 2.6).

Таблиця 2.6 – Аналіз засобів захисту даних, журналювання та резервного копіювання АТ “Демо-Банк”

Засіб / механізм	Як використовується	Потенційне обмеження
NTFS permissions / AD groups	розмежування доступу до файлових ресурсів	ризик застарілих або надлишкових прав доступу
BitLocker	шифрування дисків робочих станцій і ноутбуків	не контролює передавання даних після авторизованого доступу
Database access control	обмеження доступу до баз даних і критичних таблиць	потреба в аудиті привілейованих дій і змін
Шифрування з'єднань	захист даних під час передавання між системами	потреба в контролі конфігурацій і сертифікатів
DLP	у поточній моделі повноцінно не впроваджене	обмежений контроль витоку конфіденційної інформації

Продовження таблиці 2.6

Засіб / механізм	Як використовується	Потенційне обмеження
Windows Event Log / AD logs	фіксація подій ОС, доменних входів і змін прав	складність аналізу без централізації
FortiGate / VPN logs	фіксація мережевих підключень і віддаленого доступу	обмежений контекст без кореляції з іншими джерелами
SIEM	повноцінне централізоване рішення не впроваджене	пізнє виявлення складних або пов'язаних подій
Veeam Backup & Replication	резервне копіювання критичних систем, даних і конфігурацій	потреба в регулярному тестуванні відновлення
Immutable backup	у поточній моделі не застосовується повною мірою	ризик видалення або шифрування резервних копій

Джерело: Розроблено автором

Реагування на інциденти та організаційне забезпечення СУІБ. Для реєстрації звернень, технічних проблем і частини інцидентів в АТ “Демо-Банк” використовується GLPI Service Desk. Система дозволяє фіксувати звернення, призначати відповідальних осіб, контролювати статус виконання та зберігати історію опрацювання.

Водночас GLPI Service Desk використовується переважно як система реєстрації та супроводу заявок. Повноцінний процес реагування на інциденти інформаційної безпеки потребує додаткової формалізації: класифікації інцидентів, критеріїв критичності, порядку ескалації, відповідальних осіб і типових сценаріїв реагування.

У поточній моделі АТ “Демо-Банк” incident response playbooks розроблені неповною мірою. Для окремих типових ситуацій, таких як фішинговий лист, підозріле VPN-підключення, зараження робочої станції або несанкціонована зміна прав доступу, порядок дій не деталізований достатньо. Це може збільшувати час реагування і робити процес залежним від досвіду конкретних працівників.

Організаційні документи з інформаційної безпеки зберігаються на корпоративному порталі SharePoint. До них належать політика інформаційної

безпеки, політика управління доступом, правила роботи з інформацією обмеженого доступу, інструкції для користувачів, порядок резервного копіювання та порядок повідомлення про інциденти (таблиця 2.7).

Разом з тим ефективність організаційних механізмів залежить не лише від наявності документів. Важливо, щоб політики регулярно переглядалися, працівники проходили навчання, результати ознайомлення фіксувалися, а виявлені під час внутрішнього аудиту недоліки перетворювалися на конкретні коригувальні дії.

Таблиця 2.7 – Аналіз механізмів реагування на інциденти та організаційного забезпечення СУІБ АТ “Демо-Банк”

Засіб / механізм	Як використовується	Потенційне обмеження
GLPI Service Desk	реєстрація звернень, технічних проблем і частини інцидентів	не замінює повноцінного процесу реагування на інциденти ІБ
Email / корпоративні сповіщення	інформування відповідальних осіб про події або інциденти	ризик хаотичної комунікації без формалізованого порядку
Incident response playbooks	у поточній моделі розроблені неповно	відсутність деталізованих сценаріїв для типових інцидентів
Політика інформаційної безпеки	визначає загальні вимоги до захисту інформації	потребує регулярного перегляду та контролю виконання
Політика управління доступом	регламентує надання, зміну та відкликання доступу	може виконуватися формально без регулярного access review
Навчання персоналу	проводиться для ознайомлення з базовими вимогами ІБ	потребує регулярності та перевірки засвоєння матеріалу
Внутрішній аудит	перевіряє виконання політик і ефективність контролів	може охоплювати не всі напрями СУІБ
SharePoint	зберігання політик, процедур, інструкцій і підтверджень ознайомлення	ризик формального ведення документів без фактичного впливу на процеси

Джерело: Розроблено автором

Аналіз наявних механізмів інформаційної безпеки показує, що в АТ “Демо-Банк” сформовано базовий контур захисту, який охоплює управління доступом, технічний захист інфраструктури, захист інформаційних ресурсів, журналювання, резервне копіювання та організаційне забезпечення СУІБ. Проте ефективність цих механізмів залежить не лише від факту їх наявності, а й від повноти

впровадження, регулярності контролю, інтеграції між засобами та здатності своєчасно виявляти й обробляти події інформаційної безпеки.

З метою подальшого виявлення прогалин СУІБ розглянуті механізми доцільно узагальнити за напрямками, поточною роллю та ключовими обмеженнями (таблиця 2.8). Це дозволить перейти від характеристики AS-IS стану до оцінювання ризиків, що виникають унаслідок неповного охоплення MFA, недостатньої централізації журналювання, обмеженого DLP-контролю, нерегулярного тестування відновлення та неповної формалізації реагування на інциденти.

Таблиця 2.8 – Узагальнення поточного стану механізмів інформаційної безпеки АТ “Демо-Банк”

Напрямок	Приклади засобів	Поточна роль	Ключове обмеження
Управління доступом	Active Directory, GPO, AD groups, паролі політики, MFA для VPN	централізоване управління користувачами, доступами та базовими політиками	ризик надлишкових прав, MFA не охоплює всі критичні системи
Endpoint-захист	Microsoft Defender for Endpoint, WSUS, контроль USB	захист робочих станцій і серверів, оновлення, базове виявлення загроз	потреба в кращій інтеграції з моніторингом і реагуванням
Мережевий захист	FortiGate, VPN, VLAN, ACL, IDS/IPS	контроль периметра, віддаленого доступу та взаємодії між сегментами	потреба в посиленні сегментації та контролю VPN-доступу
Захист інформаційних ресурсів	NTFS permissions, AD groups, BitLocker, DB access control	обмеження доступу, шифрування та контроль операцій із даними	відсутність повноцінного DLP і ризик неактуальних прав
Журналювання та моніторинг	Windows Event Log, AD logs, FortiGate logs, VPN logs, Defender logs	фіксація подій безпеки в окремих системах	відсутність повноцінної SIEM-централізації та кореляції
Резервне копіювання	Veeam Backup & Replication	відновлення даних і систем після збоїв або атак	нерегулярне тестування відновлення, недостатній immutable backup
Реагування на інциденти	GLPI Service Desk, email-сповіщення, журнал інцидентів	реєстрація та супровід подій і звернень	недостатня формалізація incident response playbooks
Організаційні механізми	політики ІБ, інструкції, навчання, внутрішній аудит, SharePoint	формалізація вимог і контроль виконання процедур	ризик формального виконання та нерегулярного перегляду

Джерело: Розроблено автором

За результатами аналізу наявних механізмів забезпечення інформаційної безпеки АТ “Демо-Банк” можна резюмувати, що в установі наявний базовий набір організаційних, програмних і технічних засобів захисту. Водночас ефективність цих засобів обмежується неповним охопленням MFA, ризиком надлишкових доступів, відсутністю повноцінного DLP, недостатньою централізацією журналювання, нерегулярним тестуванням резервного відновлення та неповною формалізацією реагування на інциденти. У наступному підрозділі зазначені обмеження будуть розглянуті як прогалини СУІБ, що формують ризики для конфіденційності, цілісності та доступності критичних активів і об’єктів захисту банку.

2.3 Оцінювання достатності механізмів СУІБ та пов’язаних ризиків інформаційної безпеки АТ “Демо-Банк”

Результати аналізу наявних механізмів забезпечення інформаційної безпеки АТ “Демо-Банк” свідчать, що в установі сформовано базовий контур СУІБ, який охоплює управління доступом, технічний захист інфраструктури, захист інформаційних ресурсів, журналювання подій, резервне копіювання, організаційні політики та реєстрацію інцидентів. Водночас наявність окремих програмних, технічних і організаційних засобів не є достатньою умовою ефективності СУІБ.

Оцінювання достатності механізмів СУІБ передбачає не лише встановлення факту наявності або відсутності окремих засобів захисту, а й аналіз того, наскільки ці засоби відповідають критичності інформаційних активів, характеру загроз і потребам банківських процесів. У цьому контексті недостатність контрольного середовища може проявлятися у неповному охопленні критичних систем, нерегулярному виконанні контрольних процедур, слабкій інтеграції між окремими засобами захисту або відсутності належного підтвердження їх ефективності. Такі обмеження створюють підґрунтя для виникнення ризиків інформаційної безпеки, тому їх подальший розгляд здійснюється через визначення пов’язаних ризикових сценаріїв і пріоритетів їх оброблення (таблиця 2.9).

Таблиця 2.9 - Виявлені прогалини у СУІБ АТ “Демо-Банк”

Напрямок	Виявлена прогалина	Потенційний наслідок
Управління доступом	MFA застосовується переважно для VPN-доступу та не охоплює всі критичні системи	підвищення ймовірності використання скомпрометованих облікових даних
Управління доступом	Регулярний перегляд прав доступу не формалізований достатньо	накопичення надлишкових або неактуальних прав
Привілейовані облікові записи	Контроль адміністративних, сервісних та інтеграційних акаунтів є недостатньо посиленням	несанкціоновані зміни, зловживання повноваженнями
Endpoint-захист	Події з кінцевих пристроїв недостатньо інтегровані з централізованим моніторингом	несвоєчасне виявлення складної атаки на робочій станції або сервері
Мережевий захист	Правила firewall, ACL та сегментація потребують регулярного перегляду	поширення атаки між мережевими сегментами
Захист інформаційних ресурсів	Повноцінне DLP-рішення не впроваджене	неконтрольоване копіювання або пересилання конфіденційної інформації
Журналювання та моніторинг	Відсутня повноцінна SIEM-централізація та кореляція подій	пізнє виявлення інцидентів і складність розслідування
Резервне копіювання	Тестування відновлення виконується нерегулярно	відсутність підтвердженої готовності до відновлення після збою або атаки
Резервне копіювання	Immutable backup застосовується неповною мірою	ризик видалення або шифрування резервних копій
Реагування на інциденти	Incident response playbooks розроблені неповно	неузгоджені дії відповідальних осіб під час інциденту
Організаційні заходи	Політики, навчання та внутрішні процедури можуть виконуватися формально	збереження людського фактора як джерела інцидентів

Джерело: Розроблено автором

Узагальнення наведених прогалин показує, що основні проблемні зони СУІБ АТ “Демо-Банк” пов’язані не з повною відсутністю базових засобів захисту, а з недостатнім рівнем їх зрілості. Найбільш суттєвими є обмеження у сфері управління доступом, моніторингу подій, контролю витоку інформації, резервного відновлення та реагування на інциденти. Зокрема, наявність централізованого

управління обліковими записами не усуває ризик надлишкових прав без регулярного access review; наявність журналів подій не забезпечує своєчасне виявлення інцидентів без централізованої кореляції; наявність резервного копіювання не гарантує готовності до відновлення без регулярного тестування recovery-процедур.

Оскільки виявлені прогалини мають різний рівень впливу на діяльність банку, їх доцільно оцінювати з позиції ризик-орієнтованого підходу. У межах роботи ризик інформаційної безпеки розглядається як поєднання ймовірності реалізації небажаної події та її потенційного впливу на діяльність банківської установи. Такий підхід відповідає логіці ISO/IEC 27005, відповідно до якої оцінювання ризиків має бути пов'язане з активами, загрозами, вразливостями, наявними контролями та можливими наслідками для організації [23].

Для практичного оцінювання ризиків у роботі застосовується спрощена якісна модель оцінки. Ймовірність реалізації ризику і потенційні збитки (вплив) оцінюються за шкалою від 1 до 5, де 1 означає мінімальний рівень, а 5 – максимальний (таблиця 2.10). Рівень ризику визначається за формулою:

$$\text{Ризик } (R) = \frac{\text{Ймовірність } (P)}{\text{Вплив } (I)}, \quad (2.1)$$

де R (*Risk*) – рівень ризику;

P (*Probability*) – ймовірність реалізації ризику;

I (*Impact*) – збитки або шкода, які настануть у разі реалізації ризику.

Застосування такої моделі дозволяє порівняти між собою ризики різної природи: ризики доступу, моніторингу, витоку даних, резервного відновлення та реагування на інциденти. Це важливо для подальшого визначення пріоритетів удосконалення, оскільки не всі прогалини потребують однакового рівня уваги та ресурсів.

Таблиця 2.10 – Класифікація ризиків інформаційної безпеки за рівнем критичності

Значення ризику	Рівень ризику	Характеристика
1–5	Низький	ризик є прийнятним, достатньо базового контролю
6–10	Середній	ризик потребує моніторингу та планових заходів
11–15	Високий	ризик потребує пріоритетного зниження
16–25	Критичний	ризик потребує першочергових заходів реагування

Джерело: Розроблено автором

На основі виявлених прогалин було сформовано перелік ключових ризиків інформаційної безпеки АТ “Демо-Банк” (таблиця 2.11). Кожен ризик пов’язано з конкретною прогалиною СУІБ, що дає змогу обґрунтувати його походження та визначити подальші напрями оброблення. Такий підхід дозволяє уникнути формального переліку ризиків і забезпечує зв’язок між фактичним станом контрольного середовища, проблемними зонами та необхідними заходами удосконалення.

Таблиця 2.11 – Оцінка ризиків інформаційної безпеки АТ “Демо-Банк”

№	Ризик	Пов’язана прогалина	Ймовірність виникнення	Потенційні збитки	Рівень ризику	Категорія
R1	Несанкціонований доступ унаслідок компрометації облікових даних	MFA не охоплює всі критичні системи	4	5	20	Критичний
R2	Накопичення надлишкових прав доступу до критичних інформаційних ресурсів	регулярний перегляд прав доступу не формалізований достатньо	4	5	20	Критичний
R3	Неконтрольоване використання привілейованих облікових записів	недостатній контроль адміністративних, сервісних та інтеграційних акаунтів	3	5	15	Високий

Продовження таблиці 2.11

№	Ризик	Пов'язана прогалина	Ймовірність виникнення	Потенційні збитки	Рівень ризику	Категорія
R4	Несвоєчасне виявлення інцидентів інформаційної безпеки	відсутня повноцінна SIEM-централізація, кореляція подій та інтеграція endpoint-подій	4	4	16	Критичний
R5	Неконтрольоване передавання або розголошення конфіденційної інформації	повноцінне DLP-рішення не впроваджене	3	5	15	Високий
R6	Поширення несанкціонованої активності між сегментами мережі	правила firewall, ACL та сегментація потребують регулярного перегляду	3	5	15	Високий
R7	Недостатня готовність до відновлення критичних систем і даних	тестування відновлення виконується нерегулярно, immutable backup застосовується неповною мірою	3	5	15	Високий
R8	Неузгоджене реагування на інциденти інформаційної безпеки	incident response playbooks розроблені неповно	3	4	12	Високий
R9	Виникнення інцидентів через недостатню обізнаність персоналу	політики, навчання та процедури можуть виконуватися формально	3	3	9	Середній

Джерело: Розроблено автором

Результати оцінювання свідчать, що найбільш критичними для АТ “Демо-Банк” є сценарії, пов’язані з несанкціонованим доступом унаслідок компрометації облікових даних, накопиченням надлишкових прав доступу до критичних інформаційних ресурсів та несвоєчасним виявленням інцидентів інформаційної безпеки. Їх критичність пояснюється поєднанням високої ймовірності реалізації та

значного впливу на діяльність банку. Такі ризики можуть одночасно впливати на декілька складових СУІБ: контроль доступу, захист клієнтських і платіжних даних, підзвітність адміністративних дій, збереження доказової бази та здатність банку оперативно реагувати на порушення (рис. 2.2).

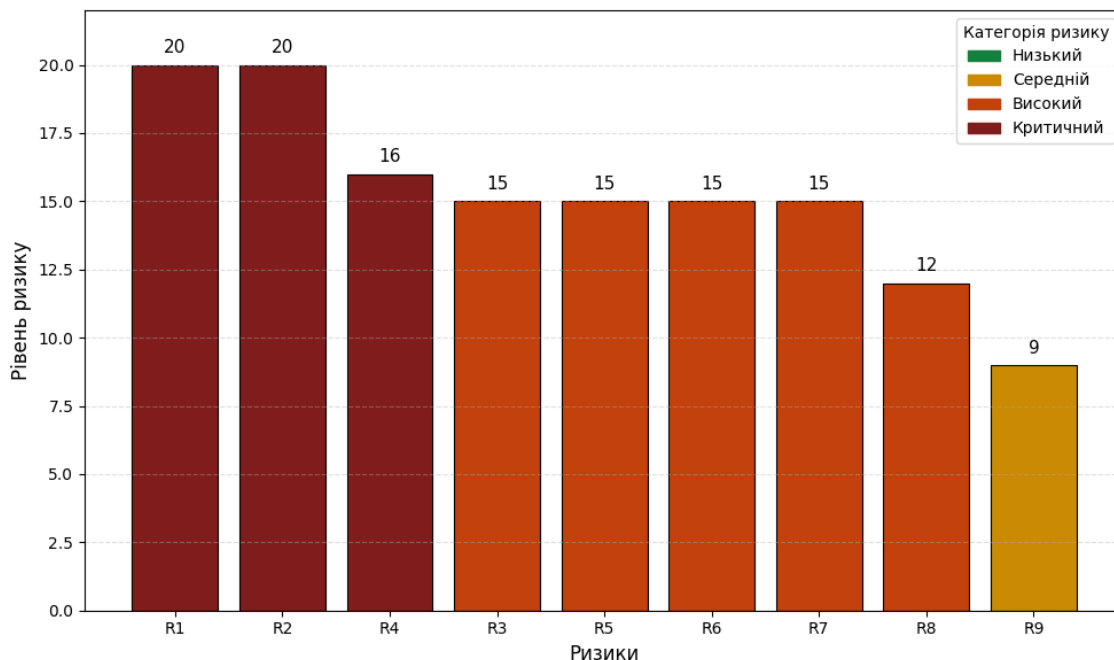


Рисунок 2.2 – Поточний рівень ризиків АТ “Демо-Банк”

Джерело: Розроблено автором

Ризики високого рівня пов’язані із привілейованими обліковими записами, витоком конфіденційної інформації, поширенням несанкціонованої активності між сегментами мережі, недостатньою готовністю до відновлення та неузгодженим реагуванням на інциденти. Вони не мають однакової природи, однак у сукупності демонструють потребу в посиленні контрольованого середовища, кращій інтеграції технічних засобів і формалізації процедур СУІБ.

Окремо слід зазначити, що ризик, пов’язаний із виникненням інцидентів через недостатню обізнаність персоналу, має середній рівень за кількісною оцінкою, однак його значення не можна ігнорувати. Людський фактор впливає на більшість напрямів інформаційної безпеки: фішинг, помилки в роботі з даними, порушення процедур доступу, несвоєчасне повідомлення про підозрілі події та

недостатнє дотримання вимог внутрішніх політик. Тому навіть ризики середнього рівня можуть мати системний вплив на загальну зрілість СУІБ.

Для формування подальших заходів удосконалення необхідно визначити пріоритетність оброблення ризиків (таблиця 2.12). Пріоритет визначається не лише числовим значенням ризику, а й характером його впливу на критичні активи, можливістю реалізації швидких коригувальних дій та зв'язком із ключовими процесами банку. Такий підхід дозволяє спрямувати ресурси насамперед на ті напрями, де очікуваний ефект від удосконалення буде найбільш суттєвим.

Таблиця 2.12 - Пріоритетність оброблення ризиків АТ “Демо-Банк”

Пріоритет	Ризик	Обґрунтування
1	Несанкціонований доступ унаслідок компрометації облікових даних	може надати доступ до внутрішніх і критичних систем банку
2	Накопичення надлишкових прав доступу до критичних інформаційних ресурсів	створює умови для несанкціонованого доступу або зловживань
3	Несвоєчасне виявлення інцидентів інформаційної безпеки	збільшує масштаб наслідків атаки або порушення
4	Неконтрольоване передавання або розголошення конфіденційної інформації	має правові, фінансові та репутаційні наслідки
5	Недостатня готовність до відновлення критичних систем і даних	впливає на безперервність діяльності банку
6	Поширення несанкціонованої активності між сегментами мережі	може вплинути на декілька систем і мережевих зон
7	Неконтрольоване використання привілейованих облікових записів	може призвести до зміни налаштувань, доступів або даних
8	Неузгоджене реагування на інциденти інформаційної безпеки	збільшує час локалізації та усунення наслідків
9	Виникнення інцидентів через недостатню обізнаність персоналу	підвищує ймовірність фішингу, помилок і порушення процедур

Джерело: Розроблено автором

Пріоритетність, наведена вище, показує, що першочергового опрацювання потребують ризики, пов'язані з доступом, моніторингом і захистом

конфіденційної інформації. Саме ці напрями формують базові умови ефективності СУІБ: контроль того, хто має доступ до критичних систем; можливість своєчасного виявлення підозрілої активності; здатність запобігати витоку даних; готовність до відновлення після інциденту; наявність узгодженого порядку реагування. Без посилення цих напрямів інші заходи можуть мати обмежений ефект, оскільки не будуть інтегровані в цілісну систему управління ризиками інформаційної безпеки.

Отже, виявлені прогалини свідчать про необхідність подальшого підвищення зрілості СУІБ АТ “Демо-Банк”. Основні ризики пов’язані з недостатнім контролем доступу, фрагментарним моніторингом, неповним захистом від витоку даних, недостатньою формалізацією реагування та обмеженою перевіркою готовності до відновлення. Вони не свідчать про повну відсутність захисту, однак демонструють, що наявні механізми потребують посилення, інтеграції та регулярного контролю.

РОЗДІЛ 3

УДОСКОНАЛЕННЯ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ АТ “ДЕМО-БАНК”

3.1 Формування цільової моделі удосконалення СУІБ АТ “Демо-Банк”

Результати аналізу, проведеного у другому розділі, показали, що в АТ “Демо-Банк” уже сформовано базовий контур СУІБ, який охоплює управління доступом, технічний захист інфраструктури, журналювання подій, резервне копіювання, організаційні політики та реєстрацію інцидентів. Водночас виявлені прогалини свідчать про недостатній рівень інтегрованості та регулярного контролю окремих механізмів. Основні ризики пов’язані з несанкціонованим доступом, накопиченням надлишкових прав, несвоєчасним виявленням інцидентів, витоком конфіденційної інформації, недостатньою готовністю до відновлення та неповною формалізацією реагування.

З огляду на це удосконалення СУІБ АТ “Демо-Банк” має здійснюватися не шляхом окремого впровадження нових інструментів, а через формування цільової моделі контрольного середовища. Така модель повинна забезпечити зв’язок між виявленими ризиками, контрольними заходами та очікуваним результатом (рис. 3.1).



Рисунок 3.1 – Цільова модель удосконалення СУІБ АТ “Демо-Банк”

Джерело: Розроблено автором

Першим напрямом цільової моделі є посилення управління доступом. У межах цього напрямку необхідно розширити MFA на критичні системи, VPN-доступ, корпоративну пошту та привілейовані облікові записи; формалізувати регулярний перегляд доступів; розділити звичайні та адміністративні акаунти; забезпечити журналювання змін у привілейованих групах. Це дозволить зменшити ризики несанкціонованого доступу, накопичення надлишкових прав і неконтрольованого використання адміністративних повноважень.

Другим напрямом є централізація журналювання та моніторингу. Поточна модель передбачає наявність окремих джерел подій, зокрема Windows Event Log, журналів Active Directory, FortiGate, VPN та Microsoft Defender for Endpoint. Проте без централізованої кореляції такі події не завжди дають повну картину інциденту. Тому цільова модель має передбачати впровадження централізованого SIEM-моніторингу, підключення ключових джерел подій, налаштування правил виявлення та передачу інцидентів у процес реагування.

Третім напрямом є посилення захисту конфіденційної інформації. Наявні механізми, зокрема NTFS permissions, BitLocker і контроль доступу до баз даних, забезпечують базовий рівень захисту, однак не контролюють рух даних після авторизованого доступу. Тому в цільовій моделі необхідно передбачити впровадження DLP-контролю для персональних, платіжних, службових і регуляторних даних. Це має зменшити ризик неконтрольованого передавання, копіювання або розголошення конфіденційної інформації.

Четвертим напрямом є підвищення стійкості інфраструктури та готовності до відновлення. Для цього необхідно не лише виконувати резервне копіювання, а й регулярно перевіряти можливість відновлення критичних систем і даних. У цільовій моделі мають бути визначені RTO/RPO для критичних систем, запроваджене тестове відновлення, документування результатів перевірок і застосування immutable backup для захисту резервних копій від видалення або шифрування.

П'ятим напрямом є формалізація реагування на інциденти. У цільовій моделі процес реагування має бути не ситуативним, а регламентованим. Для цього

необхідно розробити incident response playbooks для типових сценаріїв: фішинговий лист, компрометація облікового запису, підозрілий VPN-вхід, malware на кінцевому пристрої, спрацювання DLP, недоступність критичної системи та несанкціонована зміна прав доступу. Кожен сценарій має визначати порядок виявлення, ескалації, локалізації, відновлення та документування інциденту.

Шостим напрямом напрямом є підвищення обізнаності персоналу. Навчання з інформаційної безпеки має бути регулярним і перевірюваним, а не формальним ознайомленням із політиками. Доцільно передбачити короткі навчальні модулі, тестування знань, фішингові симуляції та окремі інструктажі для адміністраторів, власників бізнес-процесів і працівників, які працюють із клієнтськими або платіжними даними.

Характеристика виокремлених напрямів наочно демонструє, що цільова модель удосконалення СУІБ АТ “Демо-Банк” має комплексний характер. Вона охоплює технічні заходи, зокрема MFA, SIEM, DLP, мережеву сегментацію та захист резервних копій, а також організаційні заходи: регулярний перегляд доступів, формалізацію реагування, навчання персоналу та документування результатів контролю (таблиця 3.1).

Таблиця 3.1 – Відповідність ризиків напрямам удосконалення СУІБ АТ “Демо-Банк”

Ризик	Напрямок удосконалення	Очікуваний результат
Несанкціонований доступ унаслідок компрометації облікових даних	розширення MFA на критичні системи, VPN-доступ і привілейовані акаунти	зниження ймовірності доступу лише за скомпрометованим паролем
Накопичення надлишкових прав доступу до критичних інформаційних ресурсів	регулярний перегляд прав доступу	своєчасне виявлення та відкликання неактуальних або надлишкових прав
Неконтрольоване використання привілейованих облікових записів	регламентоване використання адміністративних і сервісних акаунтів	підвищення підзвітності привілейованих дій
Несвоєчасне виявлення інцидентів інформаційної безпеки	централізація журналювання та SIEM-кореляція подій	скорочення часу виявлення підозрілої активності
Неконтрольоване передавання або розголошення конфіденційної інформації	впровадження DLP-контролю	зменшення ризику витоку персональних, платіжних і службових даних

Продовження таблиці 3.1

Ризик	Напрямок удосконалення	Очікуваний результат
Поширення несанкціонованої активності між сегментами мережі	перегляд сегментації, firewall-правил та ACL	обмеження переміщення атаки між мережевими зонами
Недостатня готовність до відновлення критичних систем і даних	тестове відновлення та посилення захисту резервних копій	підвищення готовності до відновлення після збою або атаки
Неузгоджене реагування на інциденти інформаційної безпеки	розроблення incident response playbooks	стандартизація дій відповідальних осіб під час інциденту
Виникнення інцидентів через недостатню обізнаність персоналу	регулярне навчання, тестування знань і фішингові симуляції	зменшення кількості помилок і успішних фішингових атак

Джерело: Розроблено автором

Важливо, що запропонована модель не передбачає ізолюваного впровадження окремих засобів. Її ефективність залежить від взаємозв'язку між заходами. Наприклад, MFA знижує ризик компрометації облікових даних, але не замінює регулярний перегляд доступів. SIEM підвищує швидкість виявлення інцидентів, але потребує формалізованого процесу реагування. DLP зменшує ризик витоку даних, однак має бути пов'язаний із журналюванням, розслідуванням і дисциплінарними процедурами [24].

Отже, цільова модель удосконалення СУІБ АТ “Демо-Банк” спрямована на підвищення керованості контрольного середовища. Її основними елементами є посилення контролю доступу, централізація моніторингу, захист конфіденційної інформації, підвищення готовності до відновлення, формалізація реагування на інциденти та розвиток обізнаності персоналу. У наступному підрозділі ці напрями деталізуються через конкретні контрольні заходи, інструменти, відповідальних осіб, періодичність виконання та доказову базу.

3.2 Розроблення та практична реалізація контрольних заходів для зниження ризиків СУІБ АТ “Демо-Банк”

3.2.1 Визначення принципів розробки контрольних заходів

Практична реалізація удосконалення СУІБ АТ “Демо-Банк” буде ґрунтуватися на ризик-орієнтованому підході. Це означає, що запропоновані заходи визначатимуться не як окремий перелік технічних рішень, а як система контрольних дій, спрямованих на зниження ризиків, встановлених у підрозділі 2.3. Такий підхід дозволяє забезпечити послідовний зв'язок між виявленою прогалиною, ризиковою подією, контрольним заходом, інструментом реалізації, відповідальними особами, періодичністю виконання та доказами фактичного функціонування контролю.

У межах цієї роботи контрольний захід розглядається як організаційна, технічна або процедурна дія, спрямована на зменшення ймовірності реалізації ризику або зниження рівня його можливих наслідків для банківської установи. При цьому інструмент не ототожнюється із самим контролем. Наприклад, Microsoft Entra MFA, FortiToken, Wazuh, Microsoft Purview DLP, FortiGate або Veeam Backup & Replication є засобами реалізації відповідних контрольних заходів, однак ефективність залежить від того, як саме вони налаштовані, які процеси підтримують, хто відповідає за їх виконання та які підтвердження залишаються після виконання контролю.

Формування контрольних заходів буде здійснюватися з урахуванням методичних підходів ISO/IEC 27002, ризик-орієнтованої логіки ISO/IEC 27005 та банківського регуляторного контексту. ISO/IEC 27002 використовуватиметься як основа для визначення відповідних сфер контролів, зокрема управління доступом, захисту інформації, журналювання, моніторингу, мережевої безпеки, резервного копіювання, управління інцидентами та підвищення обізнаності персоналу. ISO/IEC 27005 застосовуватиметься як методична основа для переходу від виявлених прогалин до оцінювання ризиків і вибору заходів їх оброблення.

Також ми врахуємо регуляторна логіка НБУ, як банківський контекст, у межах якого особливого значення набувають захист критичних інформаційних активів, контроль доступу, безперервність діяльності, реагування на інциденти та належне управління ризиками.

Перед деталізацією окремих контрольних заходів доцільно показати їх методичне узгодження із загальними сферами контролів ISO/IEC 27002 та банківським контекстом (таблиця 3.2). Це надасть нам змогу обґрунтувати, що запропоновані заходи не є довільним набором рекомендацій, а впливають із поєднання результатів аналізу ризиків, міжнародних підходів до побудови СУІБ та особливостей функціонування банківської установи.

Таблиця 3.2 – Узгодження контрольних заходів із методичною основою СУІБ

Контрольний захід	Сфера застосування за ISO/IEC 27002	Зв'язок із банківським регуляторним контекстом
Обов'язкове застосування MFA для критичних систем, VPN-доступу та привілейованих облікових записів	управління ідентичністю, автентифікація, контроль доступу	посилення контролю доступу до критичних систем і зниження ризику несанкціонованого доступу
Періодичний перегляд прав доступу до критичних інформаційних ресурсів	управління правами доступу, перегляд доступів користувачів	забезпечення актуальності повноважень працівників і зниження операційних ризиків
Регламентоване використання привілейованих і сервісних облікових записів	управління привілейованими правами доступу	підвищення підзвітності адміністративних дій і контроль критичних повноважень
Централізований збір, кореляція та аналіз подій інформаційної безпеки	журналювання, моніторинг, виявлення подій інформаційної безпеки	своєчасне виявлення інцидентів і забезпечення можливості їх розслідування
Обмеження передавання та вивантаження конфіденційної інформації	захист інформації, запобігання витоку даних, класифікація інформації	захист банківської таємниці, персональних, платіжних і службових даних

Продовження таблиці 3.2

Контрольний захід	Сфера застосування за ISO/IEC 27002	Зв'язок із банківським регуляторним контекстом
Управління мережевою сегментацією та правилами міжсегментної взаємодії	мережева безпека, контроль трафіку, розмежування мережевих зон	обмеження поширення інцидентів і захист критичних банківських систем
Резервне копіювання та тестове відновлення критичних систем і даних	резервне копіювання, готовність до відновлення, безперервність діяльності	підтримання безперервності банківських процесів і готовності до відновлення після інцидентів
Формалізовані сценарії реагування на інциденти інформаційної безпеки	управління інцидентами інформаційної безпеки	формалізація виявлення, ескалації, локалізації, документування та післяінцидентного аналізу
Підвищення обізнаності персоналу з питань інформаційної безпеки	обізнаність, навчання та підготовка персоналу	зниження ризиків людського фактора та підвищення культури інформаційної безпеки

Джерело: Розроблено автором

Наведене узгодження показує, що контрольні заходи охоплюють ключові сфери СУІБ, які є критичними для банківської установи: управління доступом, захист даних, моніторинг подій, мережева безпека, резервне копіювання, реагування на інциденти та обізнаність персоналу. Водночас сама відповідність певній сфері контролів не є достатньою. Для практичного застосування кожен захід має бути деталізований через конкретний дизайн, інструментальну підтримку, відповідальних осіб, періодичність виконання та доказову базу.

З цією метою подальший опис контрольних заходів подається у вигляді узагальненого дизайну. Такий формат дозволяє одразу встановити, який ризик знижується кожним контролем, яким способом контроль буде виконуватися, за допомогою яких інструментів реалізовуватиметься, хто відповідатиме за його функціонування та які документи, журнали або заявки підтверджуватимуть його виконання (таблиця 3.3).

Таблиця 3.3 – Дизайн контрольних заходів для зниження ризиків СУІБ АТ
“Демо-Банк”

№	Ризик	Контрольний захід	Дизайн контролю	Інструмент	Періодичність	Доказ виконання
C1	Несанкціонований доступ унаслідок компрометації облікових даних	Обов’язкове застосування MFA для критичних систем, VPN-доступу та привілейованих облікових записів	MFA застосовується для VPN, корпоративної пошти, адміністративних акаунтів і критичних систем; винятки погоджуються підрозділом ІБ та мають обмежений строк дії	Microsoft Entra MFA, FortiToken	постійно; перегляд винятків щомісячно	перелік користувачів з MFA, журнали входів, реєстр винятків
C2	Накопичення надлишкових прав доступу до критичних інформаційних ресурсів	Періодичний перегляд прав доступу до критичних інформаційних ресурсів	ІТ щоквартально формує звіт щодо складу критичних AD-груп; власники процесів підтверджують актуальність доступів; зайві права відкликаються через GLPI	Active Directory, PowerShell, GLPI, SharePoint	щоквартально	звіт AD-груп, погодження власників, GLPI-заявки
C3	Неконтрольоване використання привілейованих облікових записів	Регламентоване використання привілейованих і сервісних облікових записів	адміністративні акаунти відокремлюються від звичайних; сервісні акаунти мають власника, призначення та строк перегляду; зміни у привілейованих групах журналюються	Active Directory, GPO, Wazuh	постійно; перегляд щоквартально	перелік privileged accounts, журнали змін, звіт перегляду

Продовження таблиці 3.3

№	Ризик	Контрольний захід	Дизайн контролю	Інструмент	Періодичність	Доказ виконання
C4	Несвоєчасне виявлення інцидентів інформаційної безпеки	Централізований збір, кореляція та аналіз подій інформаційної безпеки	події з AD, Windows Server, FortiGate, VPN, Defender та критичних серверів передаються до SIEM; для ключових сценаріїв налаштовуються правила виявлення	Wazuh	постійно	SIEM-алерти, дашборди, інциденти в GLPI
C5	Неконтрольоване передавання або розголошення конфіденційної інформації	Обмеження передавання та вивантаження конфіденційної інформації	DLP-політики блокують або фіксують пересилання персональних, платіжних і службових даних на зовнішню пошту, USB або зовнішні ресурси	Microsoft Purview DLP	постійно	DLP-інциденти, журнали спрацювань, звіти ІБ
C6	Поширення несанкціонованої активності між сегментами мережі	Управління мережевою сегментацією та правилами міжсегментної взаємодії	мережа поділяється на користувацький, серверний, адміністративний, VPN, DMZ, contractor і critical systems сегменти; доступ дозволяється лише за службовою необхідністю	FortiGate, VLAN, ACL	перегляд раз на пів року	реєстр firewall-правил, схема сегментації, протокол перегляду

Продовження таблиці 3.3

№	Ризик	Контрольний захід	Дизайн контролю	Інструмент	Періодичність	Доказ виконання
C7	Недостатня готовність до відновлення критичних систем і даних	Резервне копіювання та тестове відновлення критичних систем і даних	для критичних систем визначаються RTO/RPO; резервні копії створюються через Veeam; відновлення тестується за графіком; застосовується immutable repository	Veeam Backup & Replication	щомісячно / щоквартально залежно від критичності	звіт тестового відновлення, логи Veeam, реєстр backup
C8	Неузгоджене реагування на інциденти інформаційної безпеки	Формалізовані сценарії реагування на інциденти інформаційної безпеки	для типових інцидентів визначаються етапи виявлення, ескалації, локалізації, відновлення, документування та post-incident review	GLPI, SharePoint	перегляд раз на пів року	playbooks, GLPI-заявки, звіти інцидентів
C9	Виникнення інцидентів через недостатню обізнаність персоналу	Підвищення обізнаності персоналу з питань інформаційної безпеки	працівники проходять регулярне навчання, тестування знань і фішингові симуляції; результати фіксуються, а працівники з низьким результатом проходять повторне навчання	SharePoint, Forms / LMS	щоквартально	результати тестів, звіти симуляцій, реєстр проходження

Джерело: Розроблено автором

Узагальнення дизайну запропонованих контрольних заходів показує, що удосконалення СУІБ АТ “Демо-Банк” передбачає не лише вибір окремих інструментів, а й формування керованого контрольного середовища. Кожен захід має визначену мету, пов’язаний ризик, спосіб реалізації, періодичність виконання та доказову базу. Це створює основу для подальшого деталізованого розгляду

практичної реалізації контролів у наступних підпунктах, а також для оцінювання їх очікуваної ефективності у підрозділі 3.3.

3.2.2. Посилення автентифікації, перегляду доступів і контролю привілейованих облікових записів

Початковим напрямом практичного удосконалення є посилення контролів управління доступом. Саме доступи є одним із ключових елементів СУІБ банку, оскільки через них визначається, хто має право працювати з критичними інформаційними ресурсами, виконувати адміністративні дії, підключатися до внутрішньої мережі та обробляти конфіденційні дані [25]. У поточній моделі АТ “Демо-Банк” базою управління доступом є Active Directory, групи безпеки, групові політики та часткове застосування MFA для VPN-доступу. Водночас цього недостатньо для зниження ризиків, пов’язаних із компрометацією облікових даних, надлишковими правами та неконтрольованим використанням привілейованих акаунтів.

Першим контрольним заходом у цьому напрямі є обов’язкове застосування MFA для критичних систем, VPN-доступу та привілейованих облікових записів. У поточному стані АТ “Демо-Банк” багатофакторна автентифікація застосовується переважно для VPN-доступу, однак ризик компрометації облікових даних залишається актуальним і для корпоративної пошти, адміністративних акаунтів та внутрішніх систем, у яких обробляються клієнтські або платіжні дані.

Вибір інструментів має бути пов’язаний із наявною інфраструктурою банку. Для VPN-доступу доцільно використовувати FortiToken, оскільки в AS-IS моделі АТ “Демо-Банк” VPN і мережевий периметр реалізовані через FortiGate. Для корпоративної пошти, облікових записів Microsoft і адміністративних входів доцільно застосувати Microsoft Entra MFA. Це дозволяє не створювати окремий ізольований механізм автентифікації, а посилити вже наявні канали доступу (таблиця 3.4).

Таблиця 3.4 – Параметри застосування MFA в АТ “Демо-Банк”

Область застосування	Інструмент	Категорія користувачів	Обґрунтування	Очікуваний результат
VPN-доступ	FortiToken	віддалені працівники, ІТ, підрядники	FortiToken інтегрується з FortiGate, який використовується для VPN-доступу	зниження ризику зовнішнього несанкціонованого доступу
Корпоративна пошта	Microsoft Entra MFA	працівники банку	поштові акаунти часто є точкою входу для фішингу та подальшої компрометації	зниження ризику захоплення поштових облікових записів
Адміністративні акаунти	Microsoft Entra MFA / FortiToken	ІТ, ІБ, адміністратори систем	привілейовані акаунти мають підвищений вплив на критичні системи	посилення захисту адміністративних дій
Критичні системи	Microsoft Entra MFA	користувачі з доступом до критичних ресурсів	доступ до критичних систем не має залежати лише від пароля	зменшення ймовірності несанкціонованого доступу

Джерело: Розроблено автором

Дизайн цього контролю має включати управління винятками. Винятки з MFA не повинні надаватися безстроково або за усним погодженням. Для кожного винятку необхідно визначити підставу, строк дії, відповідального власника та погодження підрозділу ІБ. Щомісячний перегляд винятків дозволяє запобігти ситуації, коли тимчасове послаблення контролю стає постійною вразливістю.

Другим контрольним заходом є періодичний перегляд прав доступу до критичних інформаційних ресурсів. Його мета – зменшити ризик накопичення надлишкових або неактуальних прав. Для АТ “Демо-Банк” цей контроль має особливе значення, оскільки доступи надаються через групи безпеки Active Directory, а зміна посади, переведення працівника або завершення роботи

підрядника можуть призводити до збереження доступів, які вже не відповідають фактичним обов'язкам.

Процедура має виконуватися щоквартально. До скоупу перегляду обов'язково потрібно включити групи доступу до критичних файлових ресурсів, VPN-групи, групи адміністраторів, групи доступу до критичних систем, групи зовнішніх підрядників і групи сервісних акаунтів. Використання PowerShell є доцільним, оскільки він дозволяє сформувати вивантаження складу AD-груп без закупівлі додаткового інструмента. GLPI використовується для фіксації дій із відкликання доступів, а SharePoint – для зберігання підтверджень виконання контролю (таблиця 3.5).

Таблиця 3.5 – Процедура періодичного перегляду прав доступу

Крок	Дія	Інструмент	Відповідальний	Результат
1	Визначення критичних груп доступу, що підлягають перегляду	Active Directory, SharePoint	ІБ, ІТ	перелік груп у межах review
2	Вивантаження складу груп	PowerShell	ІТ	звіт щодо членства в AD-групах
3	Передача звіту власникам процесів	SharePoint / корпоративна пошта	ІБ	звіт передано на погодження
4	Перевірка актуальності доступів	Excel / SharePoint	власники процесів	підтверджені або відхилені доступи
5	Відкликання неактуальних прав	Active Directory, GLPI	ІТ	видалені зайві доступи
6	Збереження доказів виконання	SharePoint	ІБ	пакет підтверджень виконання контролю

Продовження таблиці 3.5

Крок	Дія	Інструмент	Відповідальний	Результат
7	Перевірка повноти виконання	внутрішній аудит / ІБ	аудит, ІБ	підтвердження якості виконання review

Джерело: Розроблено автором

Ефективність цього контролю залежить від участі власників бізнес-процесів. ІТ-підрозділ може технічно сформувати звіт і відкликати права, однак саме власник процесу має підтвердити, чи є доступ обґрунтованим з погляду службових обов’язків. Підрозділ ІБ у цій процедурі виконує контрольну функцію: визначає score, слідкує за строками, перевіряє повноту підтверджень і зберігає доказову базу.

Третім контрольним заходом є регламентоване використання привілейованих і сервісних облікових записів. Привілейовані акаунти є критичними, оскільки дозволяють змінювати налаштування систем, керувати доступами, адмініструвати сервери, резервне копіювання та мережеву інфраструктуру. Для АТ “Демо-Банк” необхідно розділити звичайні користувацькі акаунти та адміністративні акаунти. Адміністративний акаунт не повинен використовуватися для щоденної роботи, корпоративної пошти або вебсерфінгу.

Сервісні акаунти також мають бути окремим об’єктом контролю. Для кожного сервісного акаунта потрібно визначити власника, призначення, систему використання, рівень доступу, дату створення та строк наступного перегляду. Це дозволяє уникнути ситуації, коли сервісні акаунти існують без відповідального власника, мають надлишкові права або продовжують використовуватися після завершення потреби (таблиця 3.6).

Таблиця 3.6 – Правила управління привілейованими та сервісними обліковими записами

Елемент контролю	Реалізація	Інструмент	Доказ виконання
Розділення user/admin-акаунтів	для щоденної роботи використовується звичайний акаунт, для адміністрування – окремий admin-акаунт	Active Directory, GPO	перелік адміністративних акаунтів, налаштування GPO
MFA для привілейованих входів	адміністративні акаунти підлягають обов’язковій MFA	Microsoft Entra MFA / FortiToken	журнали входів, політики MFA
Моніторинг privileged groups	зміни в Domain Admins, Server Admins, Backup Admins передаються до SIEM	Wazuh, AD logs	SIEM-алерти, журнали AD
Облік сервісних акаунтів	кожен сервісний акаунт має власника, опис призначення та дату перегляду	AD, SharePoint	реєстр сервісних акаунтів
Заборона спільних admin-акаунтів	адміністративні дії виконуються персоніфікованими акаунтами	AD, GPO	журнали адміністративних дій

Джерело: Розроблено автором

У сукупності ці три контролі формують більш зрілу модель управління доступом: MFA зменшує ймовірність використання скомпрометованих паролів, access review знижує накопичення зайвих прав, а контроль привілейованих акаунтів підвищує підзвітність адміністративних дій.

3.2.3 Впровадження централізованого моніторингу та правил виявлення подій

Наступним напрямом практичного удосконалення є впровадження централізованого моніторингу подій інформаційної безпеки. У поточній моделі АТ “Демо-Банк” події фіксуються в різних джерелах: Windows Event Log, журналах

Active Directory, FortiGate, VPN, Microsoft Defender for Endpoint та окремих прикладних системах. Проте без централізованої кореляції такі події залишаються фрагментарними, що ускладнює своєчасне виявлення інцидентів.

Для реалізації цього контролю доцільно використати Wazuh як SIEM-рішення. Його вибір є обґрунтованим для моделі АТ “Демо-Банк” з кількох причин. По-перше, Wazuh дозволяє централізовано збирати події з Windows-, Linux-систем, мережевих пристроїв і засобів захисту. По-друге, рішення підтримує правила виявлення, пріоритизацію подій та формування алертів. По-третє, воно є практично придатним для демонстраційної або середньої банківської моделі, оскільки не потребує значних ліцензійних витрат на початковому етапі впровадження.

Ведення журналів подій інформаційної безпеки є одним із ключових практичних засобів у забезпеченні інформаційної безпеки підприємства [26]. Але практична цінність SIEM полягає не лише у зборі журналів, а і в кореляції подій. Наприклад, масові невдалі спроби входу, подальший успішний VPN-вхід, зміна членства в адміністративній групі та підозрілий процес на робочій станції можуть окремо виглядати як різні події. У централізованому моніторингу вони можуть бути розглянуті як єдиний сценарій інциденту (таблиця 3.7).

Таблиця 3.7 – Практичний концепт правил виявлення для SIEM Wazuh

Сценарій	Умова спрацювання	Рівень критичності	Дія
Password spraying	багато невдалих входів на різні акаунти за короткий період	високий	сповіщення ІБ, перевірка джерела, блокування за потреби
Brute force	багато невдалих входів на один акаунт	високий	перевірка акаунта, блокування або скидання пароля
Зміна privileged group	додавання користувача до адміністративної групи	критичний	high alert, створення GLPI-інциденту

Продовження таблиці 3.7

Підозрілий VPN-вхід	вхід у неробочий час або з нетипового джерела	середній / високий	перевірка користувача, аналіз сесії
Malware detection	спрацювання Microsoft Defender	високий	ізоляція endpoint, створення інциденту
Підозрілий PowerShell	запуск нетипових команд або скриптів	високий	аналіз пристрою, перевірка активності користувача
Зміна firewall-правил	зміна правил FortiGate без погодженого запиту	високий	перевірка зміни, ескалація до ІБ

Джерело: Розроблено автором

SIEM-алерти мають бути пов'язані з процесом реагування. Для подій високої критичності має створюватися інцидент у GLPI, після чого відповідальні особи виконують перевірку, локалізацію та документування. Це дозволяє перетворити журналювання з пасивного збирання подій на активний процес виявлення і реагування.

3.2.4 Запровадження DLP-контролю для захисту конфіденційної інформації

Для банківської установи захист конфіденційної інформації має особливе значення, оскільки банк обробляє персональні дані клієнтів, платіжну інформацію, фінансову звітність, службові документи та іншу інформацію обмеженого доступу. У поточній моделі АТ “Демо-Банк” застосовуються NTFS permissions, BitLocker і контроль доступу до баз даних, однак ці механізми не забезпечують повного контролю руху даних після авторизованого доступу.

Саме тому доцільним є впровадження DLP-контролю. Для АТ “Демо-Банк” як цільове рішення можна використати Microsoft Purview DLP. Його вибір є обґрунтованим у разі використання корпоративної пошти, SharePoint, OneDrive або інших сервісів Microsoft. Це рішення дозволяє створювати політики виявлення конфіденційної інформації, блокувати або фіксувати небажані дії користувачів, формувати сповіщення та звіти для підрозділу ІБ (таблиця 3.8).

Таблиця 3.8 – DLP-політики для АТ “Демо-Банк”

Тип інформації	Канал контролю	Політика	Реакція
Персональні дані клієнтів	корпоративна пошта	заборона надсилання на зовнішні адреси без погодження	блокування, сповіщення ІБ
Платіжна інформація	пошта, файли, SharePoint	виявлення реквізитів і платіжних документів	попередження користувача або блокування
Службові документи	SharePoint, OneDrive, файлові ресурси	контроль документів із маркуванням “конфіденційно”	журналювання, approval за потреби
Масове копіювання файлів	файлові ресурси, endpoint	виявлення значного обсягу копіювання	alert ІБ, перевірка користувача
USB-носії	endpoint	обмеження копіювання конфіденційних файлів	блокування або виняток за погодженням

Джерело: Розроблено автором

DLP-контроль не повинен обмежуватися автоматичним блокуванням усіх операцій. Для окремих сценаріїв доцільно застосовувати попередження користувача, для критичних – блокування та автоматичне створення інциденту. Наприклад, спроба надіслати файл із клієнтськими даними на зовнішню адресу має блокуватися і передаватися на розгляд ІБ. Менш критичні події можуть лише журналюватися, щоб сформувати аналітику ризикової поведінки користувачів.

3.2.5 Перегляд мережевої сегментації та правил міжсегментного доступу

Посилення мережевої сегментації спрямоване на зниження ризику поширення несанкціонованої активності між сегментами мережі. У поточній моделі АТ “Демо-Банк” використовуються FortiGate, VLAN та ACL, однак

ефективність цих механізмів залежить від регулярного перегляду правил, актуальності дозволених потоків і правильного розмежування мережевих зон.

Для цільової моделі доцільно виділити користувацький сегмент, серверний сегмент, адміністративний сегмент, сегмент критичних банківських систем, DMZ, VPN-сегмент і сегмент підрядників. Основним принципом міжсегментної взаємодії має бути службова необхідність: доступ дозволяється лише до тих сервісів, які потрібні для виконання конкретної функції (таблиця 3.9).

Таблиця 3.9 – Цільова сегментація мережі АТ “Демо-Банк”

Сегмент	Призначення	Основні обмеження доступу
User VLAN	робочі станції працівників	доступ лише до дозволених сервісів
Server VLAN	прикладні сервери та внутрішні сервіси	доступ за конкретними портами і джерелами
Admin VLAN	адміністрування систем	доступ лише для адміністраторів з окремих робочих станцій
Critical Systems VLAN	core banking, критичні банківські системи	мінімально необхідні з'єднання, посилений моніторинг
DMZ	зовнішні вебсервіси та публічні компоненти	ізоляція від внутрішньої мережі
VPN VLAN	віддалений доступ працівників	доступ залежно від ролі та групи користувача
Contractor VLAN	доступ зовнішніх підрядників	тимчасовий, обмежений і журналюваний доступ

Джерело: Розроблено автором

Користувацькі робочі станції не повинні мати прямого доступу до адміністративних інтерфейсів серверів або критичних систем. Доступ адміністраторів має здійснюватися з адміністративного сегмента. VPN-користувачі мають отримувати доступ лише до ресурсів, визначених їх роллю. Сегмент підрядників повинен бути ізольованим, строковим і повністю журналюваним.

Перегляд правил FortiGate, VLAN та ACL доцільно проводити раз на пів року або після суттєвих змін в інфраструктурі. Результати перегляду мають

містити перелік актуальних правил, обґрунтування їх необхідності, власника доступу та рішення щодо видалення неактуальних винятків.

3.2.6 Організація тестового відновлення та захисту резервних копій

Наявність резервного копіювання не гарантує готовності до відновлення. Для АТ “Демо-Банк” використання Veeam Backup & Replication створює технічну основу для backup-процесу, однак ефективність цього контролю залежить від регулярного тестування відновлення, визначення RTO/RPO, перевірки цілісності копій і захисту backup-репозиторіїв від видалення або шифрування.

Для критичних систем банку необхідно визначити допустимий час відновлення та допустиму точку втрати даних. До таких систем належать основна банківська система, системи дистанційного банківського обслуговування, контролери домену, критичні бази даних, файлові ресурси та конфігурації мережевого обладнання (таблиця 3.10).

Таблиця 3.10 – Процедура тестування резервного відновлення

Крок	Дія	Інструмент	Результат
1	Визначення критичних систем для тестового відновлення	перелік активів, BIA / DRP	перелік систем у scope
2	Встановлення RTO/RPO	політика BCP/DRP	визначені цільові параметри відновлення
3	Виконання тестового відновлення	Veeam Backup & Replication	підтвердження можливості відновлення
4	Перевірка цілісності відновлених даних	Veeam SureBackup / ручна перевірка	підтвердження придатності копії
5	Документування результатів	SharePoint / GLPI	доказ виконання тесту
6	Усунення виявлених проблем	GLPI	виконані коригувальні дії

Джерело: Розроблено автором

Для критичних систем тестове відновлення доцільно проводити щомісячно або щоквартально залежно від їх критичності. Окремо необхідно захистити

backup-середовище: обмежити доступ до backup-консолі, запровадити MFA для адміністраторів резервного копіювання, використовувати окремі адміністративні акаунти та immutable repository для критичних копій. Це зменшує ризик втрати резервних копій під час ransomware-сценарію або компрометації доменної інфраструктури.

3.2.7 Розроблення сценаріїв реагування на інциденти та програми навчання персоналу

Формалізація реагування на інциденти потрібна для зниження ризику неузгоджених дій під час порушень інформаційної безпеки. У поточній моделі АТ “Демо-Банк” GLPI Service Desk використовується для реєстрації звернень та інцидентів, однак playbooks розроблені неповно. Для підвищення ефективності реагування необхідно визначити типові сценарії, порядок ескалації, відповідальних осіб, дії з локалізації, відновлення та документування (таблиця 3.11).

Таблиця 3.11 – Типові сценарії реагування на інциденти інформаційної безпеки

Сценарій	Джерело виявлення	Первинні дії	Ескалація
Фішинговий лист	користувач, поштовий захист, SIEM	ізоляція листа, перевірка посилань, попередження користувачів	ІБ
Компрометація акаунта	Wazuh, AD, VPN	блокування акаунта, скидання пароля, перевірка входів	ІБ + ІТ
Malware на endpoint	Defender, Wazuh	ізоляція пристрою, збір артефактів, перевірка поширення	ІТ + ІБ
Підозрілий VPN-вхід	FortiGate, Wazuh	перевірка сесії, контакт із користувачем, блокування за потреби	ІБ
Витік даних	DLP	блокування передачі, аналіз документа, визначення джерела	ІБ + власник процесу

Продовження таблиці 3.11

Сценарій	Джерело виявлення	Первинні дії	Ескалація
Недоступність критичної системи	моніторинг, Service Desk	перевірка сервісу, ескалація, запуск recovery-процедури	ІТ + власник системи
Несанкціонована зміна прав	AD logs, Wazuh	перевірка зміни, відкликання прав, аналіз ініціатора	ІБ + ІТ

Джерело: Розроблено автором

Кожен інцидент має реєструватися в GLPI із зазначенням часу виявлення, джерела повідомлення, категорії, критичності, відповідальних осіб, виконаних дій, часу локалізації та результатів відновлення. Playbooks і шаблони звітів доцільно зберігати у SharePoint, щоб відповідальні працівники мали доступ до актуальних процедур.

Окремо необхідно посилити навчання персоналу. Навіть якісно налаштовані технічні засоби не усувають людський фактор. Працівники можуть відкривати фішингові листи, неправильно обробляти конфіденційні дані, ігнорувати процедури повідомлення про інциденти або формально ставитися до політик ІБ. Тому навчання має бути регулярним і перевірюваним (таблиця 3.12).

Таблиця 3.12 – Програма підвищення обізнаності персоналу АТ “Демо-Банк”

Категорія працівників	Формат навчання	Періодичність	Контроль результату
Усі працівники	базовий курс з інформаційної безпеки	щоквартально	тестування знань
Фронт-офіс	фішинг, робота з клієнтськими даними	щоквартально	тест + фішингова симуляція
ІТ-адміністратори	privileged access, logging, incident response	раз на пів року	практичний сценарій
Власники процесів	access review, погодження прав доступу	раз на пів року	підтвердження участі
Нові працівники	вступний інструктаж з ІБ	під час прийняття на роботу	підтвердження ознайомлення

Джерело: Розроблено автором

Результати навчання мають фіксуватися у SharePoint або LMS. Працівники, які не пройшли тестування або показали негативний результат під час фішингової симуляції, повинні проходити повторне навчання. Для власників процесів окремий акцент має робитися на відповідальності за погодження доступів, оскільки саме вони беруть участь у процедурі access review.

3.2.8 Визначення етапності впровадження контрольних заходів

Після визначення дизайну контрольних заходів необхідно встановити послідовність їх впровадження. Не всі заходи мають однакову складність, вартість і залежність від інших процесів. Тому їх доцільно впроваджувати поетапно: спочатку контролі, що знижують критичні ризики доступу, далі – моніторинг і DLP, після цього – сегментація, резервне відновлення, реагування та навчання (таблиця 3.13).

Таблиця 3.13 – План впровадження контрольних заходів удосконалення СУІБ АТ “Демо-Банк”

Етап	Контрольні заходи	Відповідальні	Очікуваний результат
Етап 1. Посилення контролю доступу	MFA, access review, privileged accounts	ІТ, ІБ, власники процесів	зниження ризиків несанкціонованого доступу та надлишкових прав
Етап 2. Централізація моніторингу	Wazuh, підключення AD, Windows, FortiGate, VPN, Defender	ІБ, ІТ	скорочення часу виявлення інцидентів
Етап 3. Захист конфіденційної інформації	Microsoft Purview DLP, DLP-політики, обробка DLP-інцидентів	ІБ, ІТ, власники процесів	зниження ризику витоку даних
Етап 4. Сегментація та стійкість	FortiGate, VLAN, ACL, Veeam, immutable backup	ІТ, ІБ	обмеження поширення атак і підвищення готовності до відновлення
Етап 5. Реагування та обізнаність	GLPI, SharePoint, playbooks, навчання, фішингові симуляції	ІБ, ІТ, HR	стандартизація реагування та зниження впливу людського фактора

Джерело: Розроблено автором

Запропонована етапність дозволяє насамперед знизити ризики з найвищим рівнем критичності, а потім поступово підвищувати зрілість інших елементів СУІБ. Основна перевага такого підходу полягає в тому, що кожен контрольний захід має чітко визначену мету, пов'язаний ризик, інструментальну підтримку, відповідальних виконавців, періодичність виконання та доказову базу.

Консолідуючи, практична реалізація контрольних заходів у межах СУІБ АТ “Демо-Банк” забезпечує перехід від фрагментарного набору засобів захисту до більш керованої та доказової моделі управління інформаційною безпекою. Запропоновані контролю спрямовані на зниження ключових ризиків, визначених у другому розділі, та створюють основу для подальшої оцінки їх ефективності у підрозділі 3.3.

3.3 Оцінювання ефективності запропонованих заходів удосконалення СУІБ АТ “Демо-Банк”

Оцінювання ефективності запропонованих контрольних заходів є завершальним етапом покращення, оскільки дозволяє визначити, наскільки розроблені заходи здатні знизити ризики інформаційної безпеки, а також оцінити очікуваний результат їх впровадження.

Ефективність контрольних заходів у межах СУІБ не слід розглядати як повне усунення ризиків. Для банківської установи повна ліквідація ризиків інформаційної безпеки є практично неможливою, оскільки діяльність банку пов'язана з постійною обробкою критичних даних, використанням інформаційних систем, віддаленим доступом, взаємодією з клієнтами, підрядниками та регулятором. Тому основною метою удосконалення є зниження ризиків до більш контрольованого рівня, за якого вони можуть бути прийняті керівництвом банку або перебувати під постійним моніторингом.

У межах дослідження ефективність запропонованих заходів оцінюється через зміну рівня ризику до та після впровадження контрольних заходів. Початкові рівні ризиків були визначені у підрозділі 2.3. Після впровадження

контрольних заходів відбулося очікуване зниження ймовірності реалізації окремих ризикових подій, зменшення рівня можливих наслідків або одночасний вплив на обидва параметри (таблиця 3.14).

Таблиця 3.14 – Очікуваний рівень ризиків АТ “Демо-Банк” після впровадження контрольних заходів

№	Ризик	Запропонований контрольний захід	Очікувана ймовірність виникнення	Очікуваний рівень потенційних наслідків	Очікуваний залишковий рівень ризику	Категорія
R1	Несанкціонований доступ унаслідок компрометації облікових даних	Обов’язкове застосування MFA для критичних систем, VPN-доступу та привілейованих облікових записів	2	5	10	Середній
R2	Накопичення надлишкових прав доступу до критичних інформаційних ресурсів	Періодичний перегляд прав доступу до критичних інформаційних ресурсів	2	5	10	Середній
R3	Неконтрольоване використання привілейованих облікових записів	Регламентоване використання привілейованих і сервісних облікових записів	2	5	10	Середній
R4	Несвоєчасне виявлення інцидентів інформаційної безпеки	Централізований збір, кореляція та аналіз подій інформаційної безпеки	2	4	8	Середній
R5	Неконтрольоване передавання або розголошення конфіденційної інформації	Обмеження передавання та вивантаження конфіденційної інформації	2	4	8	Середній

Продовження таблиці 3.14

№	Ризик	Запропонований контрольний захід	Очікувана ймовірність виникнення	Очікуваний рівень потенційних наслідків	Очікуваний залишковий рівень ризику	Категорія
R6	Поширення несанкціонованої активності між сегментами мережі	Управління мережевою сегментацією та правилами міжсегментної взаємодії	2	4	8	Середній
R7	Недостатня готовність до відновлення критичних систем і даних	Резервне копіювання та тестове відновлення критичних систем і даних	2	4	8	Середній
R8	Неузгоджене реагування на інциденти інформаційної безпеки	Формалізовані сценарії реагування на інциденти інформаційної безпеки	2	3	6	Середній
R9	Виникнення інцидентів через недостатню обізнаність персоналу	Підвищення обізнаності персоналу з питань інформаційної безпеки	2	3	6	Середній

Джерело: Розроблено автором

Аналіз очікуваних значень показує, що запропоновані контрольні заходи впливають на рівень ризику по-різному: одні зменшують ймовірність реалізації ризикової події, інші – знижують можливі наслідки її настання. У більшості випадків основний ефект досягається саме через зменшення ймовірності.

Наприклад, впровадження MFA знижує ймовірність несанкціонованого доступу у разі компрометації пароля, оскільки одного пароля вже недостатньо для успішної автентифікації. Водночас MFA не усуває повністю можливі наслідки інциденту, якщо злоумисник усе ж отримає доступ до критичних ресурсів.

Подібну логіку мають контроль привілейованих облікових записів, регулярний перегляд прав доступу, SIEM-моніторинг, DLP-контроль і перегляд правил мережевої сегментації. Вони насамперед знижують імовірність виникнення інциденту або підвищують здатність банку своєчасно його виявити та локалізувати. Натомість заходи, пов'язані з резервним копіюванням, тестовим відновленням і використанням immutable backup, більшою мірою впливають на рівень можливих наслідків, оскільки підвищують здатність банку відновити критичні системи та дані після збою, атаки або пошкодження інформації.

Отже, зниження хоча б одного з параметрів – імовірності або можливих наслідків – позитивно впливає на загальний рівень ризику, оскільки у роботі він визначається як їх добуток. Саме тому очікуване зменшення рівнів ризику після впровадження контрольних заходів є логічним результатом посилення контрольного середовища СУІБ АТ “Демо-Банк” (рис. 3.2).

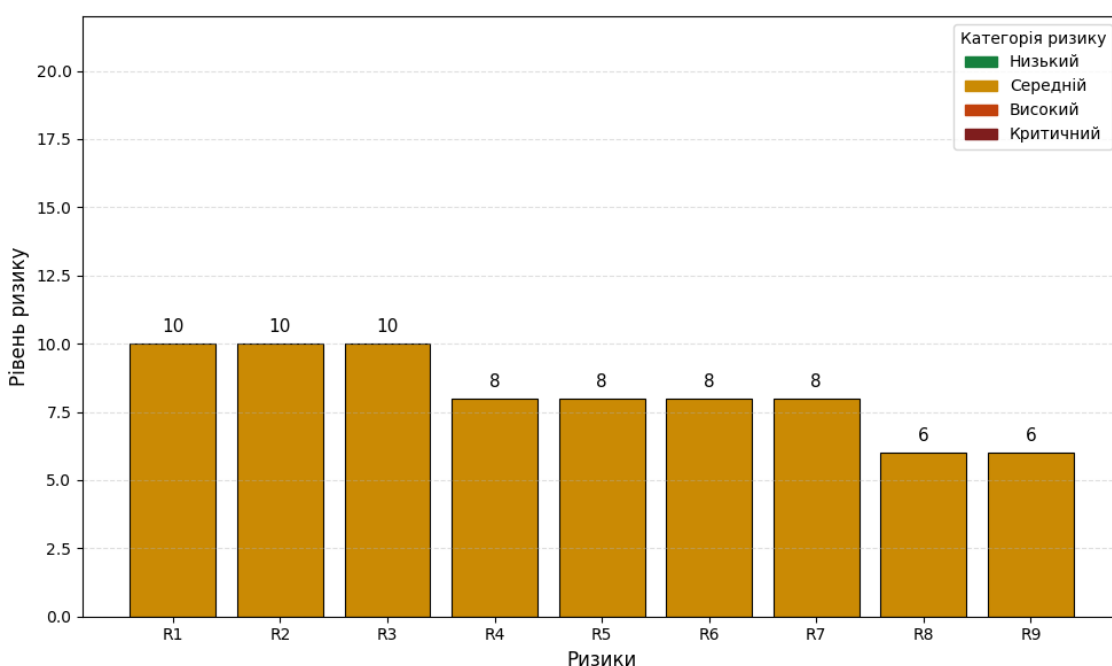


Рисунок 3.2 – Рівень ризиків АТ “Демо-Банк” після впровадження контрольних заходів

Джерело: Розроблено автором

Для наочного відображення результатів впровадження контрольних заходів доцільно подати порівняльну діаграму, яка продемонструє зміну рівнів ризику до

та після реалізації запропонованих заходів. Такий формат додатково дозволить оцінити очікуваний ефект удосконалення СУІБ АТ “Демо-Банк” та підтвердити зниження ризиків за ключовими напрямками контрольного середовища (рис 3.3).

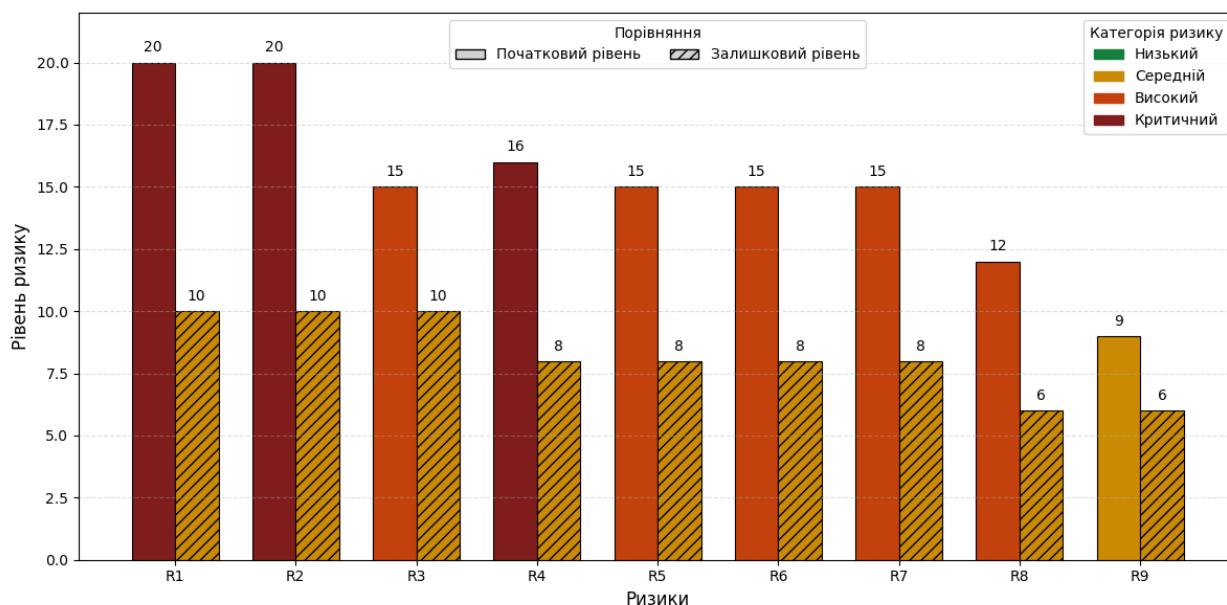


Рисунок 3.3 – Порівняння початкових та очікуваних залишкових рівнів ризиків інформаційної безпеки АТ “Демо-Банк”

Джерело: Розроблено автором

Як видно з результатів, продемонстрованих вище, запропоновані контрольні заходи дозволяють знизити більшість критичних і високих ризиків до середнього рівня. Найбільш суттєве зниження очікується за ризиками, пов’язаними з несанкціонованим доступом, накопиченням надлишкових прав, несвоєчасним виявленням інцидентів, витоком конфіденційної інформації та недостатньою готовністю до відновлення. Це пояснюється тим, що запропоновані заходи безпосередньо впливають на першопричини виявлених прогалин: неповне застосування MFA, нерегулярний перегляд доступів, відсутність централізованої кореляції подій, відсутність DLP-контролю та нерегулярне тестування відновлення.

Зниження ризику несанкціонованого доступу очікується завдяки тому, що MFA ускладнює використання скомпрометованих облікових даних як єдиної умови доступу до критичних систем. Навіть якщо пароль користувача буде

розкритий, додатковий фактор автентифікації зменшує ймовірність успішного входу. Аналогічно, періодичний перегляд доступів зменшує ризик накопичення надлишкових повноважень, оскільки неактуальні права мають виявлятися та відкликатися на регулярній основі.

Впровадження централізованого моніторингу через Wazuh знижує ризик несвоєчасного виявлення інцидентів за рахунок збору подій із різних джерел, їх кореляції та налаштування правил виявлення підозрілої активності. У поточній моделі банку події фіксуються окремо, що ускладнює аналіз інцидентів. Після впровадження SIEM-контролю підрозділ інформаційної безпеки отримує можливість бачити не лише окремі події, а й їх взаємозв'язок, наприклад між невдалими входами, VPN-підключенням, зміною груп доступу та активністю на кінцевому пристрої.

Зниження ризику витоку конфіденційної інформації забезпечується через впровадження Microsoft Purview DLP. Цей контроль не замінює права доступу або шифрування, але доповнює їх контролем руху даних після авторизованого доступу. Тобто користувач може мати право працювати з інформацією, однак спроби пересилання такої інформації на зовнішню пошту, копіювання на USB або масового вивантаження мають фіксуватися, блокуватися або передаватися на розгляд підрозділу ІБ.

Окремий ефект мають заходи, пов'язані з резервним копіюванням і відновленням. Регулярне тестування recovery-процедур та використання immutable backup не усувають імовірність технічного збою або кібератаки, але зменшують можливі наслідки таких подій. Якщо банк має підтверджену можливість відновити критичні системи та дані в межах визначених RTO/RPO, ризик тривалої недоступності сервісів або втрати даних суттєво знижується.

Для узагальнення очікуваних результатів доцільно розглянути зміни не лише за окремими ризиками, а й за основними напрямками функціонування СУІБ (таблиця 3.15).

Таблиця 3.15 – Очікувані результати удосконалення СУІБ АТ “Демо-Банк”
за основними напрямками”

Напрямок	Поточний стан	Запропонований стан	Очікуваний ефект
Управління доступом	MFA застосовується переважно для VPN, перегляд доступів недостатньо формалізований	MFA поширено на критичні системи, адміністративні акаунти та корпоративну пошту; запроваджено квартальний access review	зниження ризику несанкціонованого доступу та накопичення надлишкових прав
Привілейовані облікові записи	контроль адміністративних і сервісних акаунтів потребує посилення	розмежовано звичайні та адміністративні акаунти, визначено власників сервісних акаунтів, журналюються зміни в privileged groups	підвищення підзвітності адміністративних дій
Моніторинг подій	події фіксуються в окремих джерелах без повної кореляції	впроваджено централізований збір і кореляцію подій через Wazuh	скорочення часу виявлення інцидентів та покращення розслідування
Захист конфіденційної інформації	повноцінне DLP-рішення не впроваджене	налаштовано DLP-політики для персональних, платіжних і службових даних	зменшення ризику неконтрольованого передавання або розголошення даних
Мережева безпека	правила міжсегментної взаємодії потребують регулярного перегляду	визначено цільову сегментацію, правила FortiGate, VLAN та ACL переглядаються за графіком	обмеження поширення несанкціонованої активності між сегментами
Резервне копіювання та відновлення	резервні копії створюються, але recovery тестується нерегулярно	запроваджено тестове відновлення, immutable backup і документування результатів перевірок	підвищення готовності до відновлення критичних систем і даних

Продовження таблиці 3.15

Напрямок	Поточний стан	Запропонований стан	Очікуваний ефект
Реагування на інциденти	incident response playbooks розроблені неповно	формалізовано сценарії реагування, фіксацію дій у GLPI та зберігання процедур у SharePoint	узгоджене реагування та формування доказової бази
Обізнаність персоналу	навчання може виконуватися формально	впроваджено регулярне навчання, тестування знань і фішингові симуляції	зниження впливу людського фактора на виникнення інцидентів

Джерело: Розроблено автором

Виходячи з очікуваних результатів, наведених вище, можна стверджувати, що запропоновані контрольні заходи мають комплексний ефект. Вони не лише знижують окремі ризики, а й підвищують загальну зрілість СУІБ. Зокрема, управління доступом стає більш контрольованим завдяки MFA, access review і контролю привілейованих облікових записів. Моніторинг переходить від фрагментарного аналізу журналів до централізованої кореляції подій. Захист даних доповнюється DLP-контролем, а резервне копіювання перетворюється з технічної процедури на контрольовану готовність до відновлення.

Важливим результатом є також поява доказової бази виконання контрольних заходів. У запропонованій моделі кожен контроль залишає підтвердження виконання: журнали MFA-входів, звіти щодо складу AD-груп, GLPI-заявки, SIEM-алерти, DLP-інциденти, протоколи перегляду firewall-правил, звіти тестового відновлення, результати навчання персоналу. Це має значення не лише для поточного управління інформаційною безпекою, а й для внутрішнього аудиту, перевірки ефективності контролів і подальшого вдосконалення СУІБ.

Оцінюючи результати впровадження, необхідно враховувати поняття залишкового ризику. Залишковий ризик – це ризик, який залишається після впровадження контрольних заходів. У межах СУІБ він не повинен автоматично розглядатися як недолік, оскільки повне усунення ризиків є недосяжним або

економічно недоцільним. Важливо, щоб залишковий ризик був відомий, оцінений, документований і перебував під контролем відповідальних осіб.

Після впровадження запропонованих заходів більшість ризиків переходить до середнього рівня. Це означає, що вони не зникають повністю, але стають більш керованими. Такі ризики потребують подальшого моніторингу, регулярного перегляду ефективності контролів і періодичного оновлення процедур. Якщо в майбутньому зміниться інфраструктура банку, з'являться нові системи, зміняться регуляторні вимоги або зросте рівень загроз, оцінку залишкових ризиків необхідно буде переглянути.

Запропоновані контрольні заходи дозволяють досягти декількох практичних результатів. По-перше, знижується ймовірність несанкціонованого доступу за рахунок розширення MFA, регулярного перегляду доступів і посилення контролю привілейованих акаунтів. По-друге, скорочується час виявлення інцидентів завдяки централізованому моніторингу та кореляції подій. По-третє, зменшується ризик витоку конфіденційної інформації через впровадження DLP-контролю. По-четверте, підвищується готовність до відновлення завдяки регулярному тестуванню backup і застосуванню immutable backup. По-п'яте, реагування на інциденти стає більш формалізованим, а дії відповідальних осіб – більш узгодженими.

Отже, ефективність запропонованих заходів полягає не лише у зниженні числового рівня ризиків, а й у підвищенні керованості СУІБ АТ “Демо-Банк”. Запропонована модель створює більш чіткий зв'язок між ризиками, контрольними заходами, відповідальними особами, інструментами та доказами виконання. Це дозволяє перейти від фрагментарного набору засобів захисту до більш зрілої, контрольованої та доказової системи управління інформаційною безпекою банківської установи.

ВИСНОВКИ

У кваліфікаційній роботі було досліджено теоретичні, нормативно-методичні та практичні аспекти функціонування системи управління інформаційною безпекою банківської установи, а також розроблено комплекс заходів щодо її удосконалення на прикладі умовної моделі АТ “Демо-Банк”. Проведене дослідження дало змогу сформувати цілісне уявлення про СУІБ банку як про систему організаційних, технічних, процедурних і управлінських заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації.

У першому розділі було розкрито сутність системи управління інформаційною безпекою та принципи її побудови. Встановлено, що СУІБ не може розглядатися лише як сукупність технічних засобів захисту, оскільки її ефективність залежить від наявності політик, розподілу відповідальності, оцінювання ризиків, моніторингу, внутрішнього контролю та постійного вдосконалення. Було обґрунтовано, що побудова СУІБ має здійснюватися на основі ризик-орієнтованого підходу, циклу постійного вдосконалення та узгодження заходів захисту з цілями діяльності банківської установи.

Також у роботі визначено особливості забезпечення інформаційної безпеки у банківських установах. Встановлено, що банківський сектор характеризується підвищеною критичністю інформаційних активів, значними обсягами персональних, фінансових і платіжних даних, високою залежністю від інформаційних систем, наявністю регуляторних вимог та підвищеним рівнем кіберризиків. Особливе значення для банку мають захист клієнтських даних, платіжної інформації, основних банківських систем, каналів дистанційного обслуговування, облікових записів, журналів подій і резервних копій.

У межах теоретичної частини було узагальнено нормативно-методичні підходи до побудови, оцінювання та удосконалення СУІБ банку. Обґрунтовано використання ISO/IEC 27001 як загальної рамки побудови СУІБ, ISO/IEC 27002 як

джерела контрольних заходів, ISO/IEC 27005 як методичної основи для оцінювання ризиків, а також нормативних вимог НБУ як основи врахування банківської специфіки в Україні. Поєднання цих підходів дозволило сформувавши логіку дослідження: від визначення активів і контролів до оцінювання ризиків та розроблення практичних заходів удосконалення.

У другому розділі було охарактеризовано АТ “Демо-Банк” як умовну банківську установу, що використовується для моделювання типового середовища функціонування СУІБ. Було визначено основні категорії інформації, критичні активи та об’єкти захисту, а також організаційні ролі, які беруть участь у забезпеченні інформаційної безпеки. До таких ролей віднесено правління банку, підрозділ інформаційної безпеки, ІТ-підрозділ, власників бізнес-процесів, внутрішній аудит, комплаєнс, HR, користувачів інформаційних систем і зовнішніх підрядників з обмеженим доступом.

Під час аналізу наявних механізмів забезпечення інформаційної безпеки було встановлено, що в AS-IS моделі АТ “Демо-Банк” функціонує базовий набір організаційних, програмних і технічних засобів захисту. До них належать Microsoft Active Directory, Group Policy Objects, групи безпеки AD, парольні політики, часткове використання MFA для VPN-доступу, Microsoft Defender for Endpoint, WSUS, FortiGate, VLAN, ACL, NTFS permissions, BitLocker, Windows Event Log, журнали Active Directory, журнали FortiGate та VPN, Veeam Backup & Replication, GLPI Service Desk, SharePoint, політики інформаційної безпеки та внутрішні інструкції. Водночас встановлено, що наявність цих засобів не гарантує достатнього рівня зрілості СУІБ без регулярного контролю, інтеграції, документування та оцінки ефективності.

У результаті аналізу було виявлено основні прогалини СУІБ АТ “Демо-Банк”. Найбільш суттєвими серед них є неповне охоплення критичних систем багатофакторною автентифікацією, недостатня формалізація перегляду прав доступу, потреба в посиленому контролі привілейованих і сервісних облікових записів, відсутність повноцінної SIEM-централізації, відсутність повноцінного DLP-рішення, потреба в перегляді мережевої сегментації, нерегулярне тестування

резервного відновлення, неповне застосування immutable backup, недостатня деталізація incident response playbooks та формальний характер окремих організаційних процедур.

На основі виявлених прогалин було оцінено ризики інформаційної безпеки. Найвищий рівень отримали ризики несанкціонованого доступу внаслідок компрометації облікових даних, накопичення надлишкових прав доступу до критичних інформаційних ресурсів та несвочасного виявлення інцидентів інформаційної безпеки. Високий рівень також мають ризики неконтрольованого використання привілейованих облікових записів, неконтрольованого передавання конфіденційної інформації, поширення несанкціонованої активності між сегментами мережі, недостатньої готовності до відновлення та неузгодженого реагування на інциденти. Це підтвердило необхідність комплексного удосконалення СУІБ, а не лише точкового впровадження окремих інструментів.

У третьому розділі було сформовано цільову модель удосконалення СУІБ АТ “Демо-Банк”. Її основою став принцип “ризик – контрольний захід – очікуваний результат”. Запропонована модель передбачає посилення управління доступом, централізацію моніторингу, впровадження контролю передавання конфіденційної інформації, удосконалення мережевої сегментації, підвищення готовності до відновлення, формалізацію реагування на інциденти та розвиток обізнаності персоналу. Такий підхід дозволяє забезпечити зв’язок між результатами аналізу ризиків і практичними рішеннями щодо їх зниження.

У межах практичної частини було розроблено комплекс контрольних заходів із зазначенням інструментів, відповідальних осіб, періодичності виконання та доказової бази. Зокрема, запропоновано обов’язкове застосування MFA для критичних систем, VPN-доступу та привілейованих облікових записів із використанням Microsoft Entra MFA та FortiToken; періодичний перегляд прав доступу на основі Active Directory, PowerShell, GLPI та SharePoint; регламентоване використання привілейованих і сервісних акаунтів; централізований збір і кореляцію подій через Wazuh; впровадження Microsoft Purview DLP; перегляд правил FortiGate, VLAN та ACL; регулярне тестування резервного відновлення

через Veeam Backup & Replication; розроблення incident response playbooks із фіксацією інцидентів у GLPI; а також регулярне навчання персоналу з використанням SharePoint, Forms або LMS.

Оцінка очікуваної ефективності показала, що запропоновані заходи дозволяють знизити більшість критичних і високих ризиків до середнього рівня. Зокрема, ризик несанкціонованого доступу внаслідок компрометації облікових даних може бути знижений за рахунок розширення MFA, ризик накопичення надлишкових прав – завдяки регулярному access review, ризик несвоєчасного виявлення інцидентів – через централізований SIEM-моніторинг, ризик витоку конфіденційної інформації – через DLP-контроль, а ризик недостатньої готовності до відновлення – через регулярне тестування recovery-процедур та застосування immutable backup.

Узагальнюючи, в роботі було розкрито теоретичні засади СУІБ, визначено банківську специфіку інформаційної безпеки, узагальнено нормативно-методичну базу, охарактеризовано активи та організаційні аспекти функціонування СУІБ, проаналізовано наявні механізми захисту, виявлено прогалини та оцінено ризики, сформовано цільову модель удосконалення, розроблено практичні контрольні заходи та оцінено їх очікувану ефективність. Основний практичний результат роботи полягає у формуванні цілісного підходу до удосконалення СУІБ банку, за якого технічні інструменти поєднуються з організаційними процедурами, відповідальністю, доказовою базою та оцінкою залишкового ризику.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection – Information security controls. Geneva: International Organization for Standardization, 2022.
2. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection – Guidance on managing information security risks. Geneva: International Organization for Standardization, 2022.
3. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva: International Organization for Standardization, 2022.
4. ISO/IEC 27035-1:2023. Information technology – Information security incident management – Part 1: Principles and process. Geneva: International Organization for Standardization, 2023.
5. Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України: Постанова Правління Національного банку України від 28.09.2017 № 95 [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/go/v0095500-17>.
6. Про затвердження Положення про організацію кіберзахисту в банківській системі України та внесення змін до Положення про визначення об'єктів критичної інфраструктури в банківській системі України: Постанова Правління Національного банку України від 12.08.2022 № 178 [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/go/v0178500-22>.
7. Про банки і банківську діяльність: Закон України від 07.12.2000 № 2121-III [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/go/2121-14>.
8. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/go/2297-17>.

9. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/go/80/94-%D0%B2%D1%80>.
10. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/go/2163-19>.
11. Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/go/1882-20>.
12. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. 2024 [Електронний ресурс]. – Режим доступу: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>.
13. European Union Agency for Cybersecurity. ENISA Threat Landscape 2024 [Електронний ресурс]. – Режим доступу: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>.
14. Verizon. 2025 Data Breach Investigations Report [Електронний ресурс]. – Режим доступу: <https://www.verizon.com/business/resources/reports/dbir/>.
15. IBM. Cost of a Data Breach Report 2025 [Електронний ресурс]. – Режим доступу: <https://www.ibm.com/reports/data-breach>.
16. Microsoft. Microsoft Entra multifactor authentication overview. Microsoft Learn [Електронний ресурс]. – Режим доступу: <https://learn.microsoft.com/en-us/entra/identity/authentication/concept-mfa-howitworks>.
17. Microsoft. Learn about data loss prevention. Microsoft Purview. Microsoft Learn [Електронний ресурс]. – Режим доступу: <https://learn.microsoft.com/en-us/purview/dlp-learn-about-dlp>.
18. Wazuh. Security Information and Event Management (SIEM) [Електронний ресурс]. – Режим доступу: <https://wazuh.com/platform/siem/>.
19. Veeam. Immutability for Backup Files. Veeam Backup & Replication User Guide [Електронний ресурс]. – Режим доступу: <https://helpcenter.veeam.com/docs/vbr/userguide/immutability.html>.

20. Курій Є., Опірський І. ISO 27001: аналіз змін та особливості відповідності новій версії стандарту. Кібербезпека: освіта, наука, техніка. 2023. № 1(19). [Електронний ресурс]. – Режим доступу: <https://doi.org/10.28925/2663-4023.2023.19.4655>.
21. Теслюк С. А., Матвійчук Н. М., Левчук А. О. Фінансова безпека банківських установ в умовах цифровізації. Економіка та суспільство. 2024. № 60 [Електронний ресурс]. – Режим доступу: <https://doi.org/10.32782/2524-0072/2024-60-117>.
22. Коробчук Т., Чиж Н. Безпека банківської діяльності в умовах військових ризиків. Економіка та суспільство. 2025. № 72 [Електронний ресурс]. – Режим доступу: <https://doi.org/10.32782/2524-0072/2025-72-12>.
23. Засадна Х. О. Стандарти управління інформаційною безпекою банку. Фінансовий простір. 2011. № 3(3) [Електронний ресурс]. – Режим доступу: <https://fp.lnu.edu.ua/index.php/fp/article/download/57/52/>.
24. Литвин Н. А., Субіна Т. В. Деякі аспекти інформаційної безпеки банків. Європейські перспективи. 2021. № 4 [Електронний ресурс]. – Режим доступу: https://ep.unesco-socio.in.ua/wp-content/uploads/2021/11/51-Lytvyn_Subina.pdf.
25. Заячківська О., Швець В., Іллін В. Сутність та значення інформаційної безпеки в банківській діяльності. Herald of Khmelnytskyi National University. Economic Sciences. 2026. Т. 350, № 1 [Електронний ресурс]. – Режим доступу: <https://doi.org/10.31891/2307-5740-2026-350-48>.
26. Бегун А. В., Осипова О. І., Урденко О. Г. Ситуаційний лог-менеджмент інформаційної безпеки підприємства. Моделювання та інформаційні системи в економіці. 2018. Вип. 95 [Електронний ресурс]. – Режим доступу: <https://ir.kneu.edu.ua/items/f348cf8c-905e-4caf-9ff0-c9dfe7505b88>.

Короткий звіт подібності

Метадані

 ДОКУМЕНТ

Заголовок

КБР_Семендяй_Б_А

АВТОР

Семендяй Б А

Науковий керівник / Експерт

Бєгун А.В.

ID документу

334246428

ОРГАНІЗАЦІЯ

Назва організації

Kyiv National Economic University named after Vadym Hetman

KNEU

підрозділ

кафедра системного аналізу та кібербезпеки

 3BIT

Дата звіту

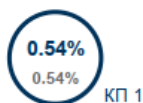
6/10/2026

Дата редагування

—

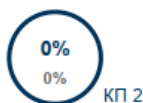
Обсяг знайдених подібностей

Коефіцієнт подібності визначає, який відсоток тексту по відношенню до загального обсягу тексту було знайдено в різних джерелах. Зверніть увагу, що високі значення коефіцієнта не автоматично означають плагіат. Звіт має аналізувати компетентна / уповноважена особа.



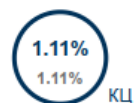
25

Довжина фрази для коефіцієнта подібності 2



15484

Кількість слів



128261

Кількість символів