КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Автоматизації і інформаційних технологій

(факультет)

Кібербезпеки та комп'ютерної інженерії

(назва випускової кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ БАКАЛАВР

на тему:

Оцінка ризиків інформаційної безпеки клієнтів телекомунікаційних підприємств

Зінченко Максим Романович

(прізвище, ім'я та по батькові здобувача повністю)

Київ 2026 р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
БУДІВНИЦТВА І АРХІТЕКТУРИ

Автоматизації і інформаційних технологій

(факультет)

Кібербезпеки та комп'ютерної інженерії

(назва кафедри)

ЗАТВЕРДЖУЮ

Завідувач кафедри

Делембовський М. М.

„__" _____20___року

КВАЛІФІКАЦІЙНА РОБОТА

ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ БАКАЛАВР

Оцінка ризиків інформаційної безпеки клієнтів телекомунікаційних підприємств

(назва)

Я як здобувач вищої освіти КНУБА розумію і підтримую політику закладу з академічної доброчесності. Я не надавав(-ла) і не одержував(-ла) недозволену допомогу під час підготовки цієї роботи. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

Здобувач Зінченко Максим Романович

(прізвище, ім'я та по батькові повністю)

125 "Кібербезпека"

(спеціальність)

Безпека інформаційних і комунікаційних систем

(освітня програма)

Група: БІКС–22

Керівник: Ізмайлова О. В.

(прізвище та ініціали)

Кандидат технічних наук, доцент

(вчене звання, науковий ступінь)

Рецензент Гончаренко Т. А.

(прізвище та ініціали)

Ідентичність підтверджую

Київ 2026 р.

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Факультет: Автоматизації і інформаційних технологій
Випускова кафедра: Кібербезпеки та комп'ютерної інженерії
Ступінь вищої освіти: Бакалавр
Спеціальність: 125 "Кібербезпека"
Освітня програма: Безпека інформаційних і комунікаційних систем

ЗАТВЕРДЖУЮ

Завідувач кафедри
Делембовський М. М.
„___"_____20___року

З А В Д А Н Н Я

ДО ВИКОНАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ ЗДОБУВАЧА СТУПЕНЯ ВИЩОЇ ОСВІТИ БАКАЛАВР

Зінченко Максим Романович

(прізвище, ім'я та по батькові здобувача)

1. Тема роботи

Оцінка ризиків інформаційної безпеки клієнтів телекомунікаційних підприємств

затверджена наказом ректора КНУБА № 576/52-15/13.2/26 від «14» травня 2026 року.

Керівник роботи

Ізмайлова Ольга Василівна доцент кафедри кібербезпеки та комп'ютерної інженерії, кандидат технічних наук, доцент

(прізвище, ім'я та по батькові, науковий ступінь, вчене звання)

3. Термін подання здобувачем роботи до захисту

4. Зміст пояснювальної записки за розділами:

Р. 1. Аналіз предметної області, клієнтських даних, загроз, вразливостей та підходів до оцінювання ризиків інформаційної безпеки.
Р. 2. Розроблення методики оцінювання ризиків: модель активів, ролей, критерії, шкали, формули розрахунку первинного і залишкового ризику.
Р. 3. Практична реалізація програмного модуля: архітектура, класова модель, алгоритм роботи, реалізація контролів, тестування та оцінка ефективності зниження ризиків.
7. Календарний план виконання роботи:

Види робіт та їх зміст	Дата виконання
Розділ 1	Квітень 2026 р.
Розділ 2	Травень 2026 р.
Розділ 3	Травень 2026 р.
Розділ 4	-
Розділ 5	-
Остаточне оформлення роботи	Червень 2026 р
Направлення роботи для перевірки на плагіат	Червень 2026 р
Попередній захист роботи	Червень 2026 р
Направлення роботи на рецензування	Червень 2026 р

8. Дата видачі завдання _____

Керівник _____ _____

Здобувач _____ _____

РЕЗЮМЕ (SUMMARY) *до кваліфікаційної випускової роботи здобувача*	ПІБ *здобувача українською та англійською мовами* *Зінченко Максим Романович* *Zinchenko Maksym Romanovych*		
ЗВО	Київський національний університет будівництва і архітектури		
Тема *(українською та англійською)*	Оцінка ризиків інформаційної безпеки клієнтів телекомунікаційних підприємств		
Освітній ступінь	Бакалавр		
Факультет	Автоматизації і інформаційних технологій		
Випускова кафедра	Кібербезпеки та комп'ютерної інженерії		
Спеціальність	125 "Кібербезпека"		
Освітня програма	Безпека інформаційних і комунікаційних систем		
Керівник	Ізмайлова Ольга Василівна, кандидат технічних наук, доцент		
Обсяг роботи:	*Пояснювальна записка, стор.*	*Розділів*	*Презентація, кількість слайдів*
	106	3	10
Розділ 1	Проаналізовано предметну область, клієнтські дані, загрози, вразливості та підходи до оцінювання ризиків.		
Розділ 2	Розроблено методику оцінювання первинного та залишкового ризику з урахуванням активів, ролей, шкал і контрзаходів.		
Розділ 3	Запропоновано програмний модуль, алгоритм роботи, класову модель, реалізацію контролів, тестування та перевірку ефективності.		
Розділ 4	-		
Розділ 5	-		
Висновки по роботі	2 стор.		
Ключові слова: Keywords:	Ключові слова: інформаційна безпека; оцінювання ризиків; телекомунікаційне підприємство; клієнтські дані; CRM; залишковий ризик information security; risk assessment; telecommunication enterprise; client data; CRM; residual risk.		

Здобувач _____/ _____

Керівник _____/ _____

АНОТАЦІЯ

У кваліфікаційній роботі розглянуто задачу оцінювання ризиків інформаційної безпеки клієнтських даних у телекомунікаційному підприємстві. Запропоновано методику визначення первинного та залишкового ризику, а також програмний модуль для перевірки типових ризикових сценаріїв: слабкої автентифікації, надлишкових прав доступу, масового експорту даних і резервного відновлення. Практичний результат роботи полягає у формуванні реєстру ризиків, підборі контрзаходів і контролі зниження залишкового ризику.

ANNOTATION

The qualification thesis addresses the assessment of information security risks for client data in a telecommunication enterprise. The work proposes a method for calculating primary and residual risk and presents a software module for checking typical risk scenarios, including weak authentication, excessive access rights, mass data export and backup recovery. The practical result is a risk register, a set of countermeasures and a repeatable procedure for monitoring residual risk reduction

Зміст

ВСТУП

Сучасні телекомунікаційні підприємства забезпечують безперервну взаємодію клієнтів із цифровими сервісами, обробляють великі обсяги персональних, фінансових і технічних даних та підтримують критичні для абонентів бізнес-процеси. У таких умовах інформаційна безпека клієнтів є не лише технічною вимогою, а й важливою умовою довіри до оператора зв'язку, стабільності сервісного обслуговування та виконання нормативних вимог щодо захисту персональних даних. Актуальність теми зумовлена тим, що клієнтські дані в телекомунікаційному підприємстві концентруються у CRM-системах, білінгових модулях, сервісах підтримки, журналах подій, резервних копіях і каналах експорту. Порушення конфіденційності, цілісності або доступності таких даних може призвести до шахрайських дій, помилок у фінансових нарахуваннях, втрати сервісної інформації, репутаційних наслідків і додаткових витрат на відновлення після інциденту. Особливу небезпеку становить поєднання технічних і організаційних недоліків: слабкої автентифікації, надлишкових прав доступу, відсутності контролю масового експорту, недостатнього журналювання та нерегулярної перевірки резервного відновлення. Саме тому оцінювання ризиків має спиратися не тільки на загальний перелік загроз, а й на конкретні активи, ролі користувачів, бізнес-процеси та фактичні сценарії обробки клієнтських даних. Метою кваліфікаційної роботи є підвищення обґрунтованості управління інформаційною безпекою клієнтів телекомунікаційного підприємства шляхом розроблення методики оцінювання ризиків і практичного прототипу програмного модуля для аналізу ризикових сценаріїв. Для досягнення поставленої мети необхідно вирішити такі завдання: проаналізувати предметну область обробки клієнтських даних у телекомунікаційному підприємстві; визначити ключові активи, загрози, вразливості та наслідки порушень; обґрунтувати методику оцінювання ризиків; сформувати шкали та формули для визначення первинного й залишкового ризику; реалізувати програмний прототип; перевірити ефективність запропонованих заходів на типових ризикових сценаріях.

Об’єктом дослідження є процеси обробки та захисту клієнтських даних у **телекомунікаційному підприємстві.**

Предметом дослідження є методи, моделі та критерії оцінювання ризиків інформаційної безпеки клієнтів у процесі функціонування CRM-системи та пов’язаних із нею бізнес-процесів. Методологічну основу роботи становлять підходи до управління ризиками інформаційної безпеки, принципи побудови системи управління інформаційною безпекою, аналіз активів, загроз і вразливостей, сценарний підхід, напівкількісне оцінювання, моделювання бізнес-процесів та програмна реалізація контрольних правил. Практичне значення роботи полягає у можливості використання запропонованої методики та програмного прототипу як основи для внутрішнього аудиту клієнтського контуру CRM-системи, формування реєстру ризиків, перевірки ефективності контрзаходів і контролю залишкового ризику після впровадження захисних заходів. Структура роботи відповідає логіці поставлених завдань. У першому розділі аналізується предметна область і формулюється задача дослідження. У другому розділі обґрунтовується та розробляється методика оцінювання ризиків. У третьому розділі подано практичну реалізацію програмного модуля, тестування та оцінювання ефективності запропонованих рішень.

РОЗДІЛ 1
АНАЛІЗ ЗАДАЧІ ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КЛІЄНТІВ У ТЕЛЕКОМУНІКАЦІЙНИХ ПІДПРИЄМСТВАХ

1.1. Актуальність оцінювання ризиків інформаційної безпеки клієнтів у телекомунікаційній сфері

Телекомунікаційні підприємства належать до критично важливих суб'єктів цифрової економіки, оскільки забезпечують передавання голосового трафіку, доступ до мережі Інтернет, обслуговування мобільних і фіксованих абонентів, підтримку сервісів самообслуговування, електронних платежів, технічної підтримки та взаємодії з партнерськими системами. У межах своєї повсякденної діяльності такі підприємства накопичують і постійно обробляють великі масиви відомостей про клієнтів: ідентифікаційні дані, контактну інформацію, договірні реквізити, історію фінансових розрахунків, технічні параметри підключення, журнали звернень до служби підтримки, записи про надані послуги та інші дані, які характеризують абонента, його поведінку і взаємодію з оператором. Саме через високу концентрацію чутливої інформації телекомунікаційне підприємство стає привабливою ціллю як для зовнішніх порушників, так і для внутрішніх осіб, що мають легітимний доступ до інформаційних ресурсів, але можуть використати його з порушенням встановлених правил. Для клієнта телекомунікаційної компанії інформаційна безпека не обмежується лише фактом технічного захисту серверів або мережевого периметра. У центрі уваги перебуває безпека персональних даних, фінансової інформації, історії користування послугами, даних про підключене обладнання, записів комунікації з оператором, а також захищеність сервісних операцій, які виконуються в CRM-системах, білінгових підсистемах, особистих кабінетах, мобільних застосунках та внутрішніх адміністративних консолях. Будь-яке порушення конфіденційності, цілісності або доступності таких даних здатне завдати клієнту матеріальної, репутаційної та правової шкоди, а для підприємства обертається втратою довіри, фінансовими збитками, конфліктами з абонентами, витратами на відновлення даних і перебудову захисної інфраструктури. Проблема

оцінювання ризиків інформаційної безпеки клієнтів є особливо важливою через те, що сучасна телекомунікаційна інфраструктура має складний розподілений характер. Дані проходять крізь декілька рівнів обробки: первинне введення оператором під час укладання договору, автоматизоване зберігання у базах даних, використання підсистемами білінгу, передавання до модулів підтримки, резервне копіювання, архівування, вибіркове вивантаження для формування звітності, використання у маркетингових та сервісних процесах. На кожному з цих етапів виникає окремий набір загроз, пов’язаний із помилками конфігурації, надлишковими правами доступу, недостатньою якістю автентифікації, людським фактором, недоліками журналювання, недостатнім контролем дій привілейованих користувачів та неякісно організованим резервуванням. Результати переддипломної практики підтверджують, що проблема має не абстрактний, а цілком прикладний характер. Під час аналізу тестового середовища CRM-системи телекомунікаційного підприємства було встановлено, що в ньому зберігалися повні ідентифікаційні дані клієнтів, контактна інформація, історія фінансових операцій, технічні параметри підключення та історія звернень у службу підтримки. Окремо слід підкреслити, що база персональних даних є найбільш вразливим і критично важливим елементом інфраструктури, а витік паспортних даних може призвести до шахрайських дій, тоді як порушення цілісності фінансових записів - до некоректних нарахувань і конфліктів з абонентами. Отже, питання оцінювання ризику повинно охоплювати не лише імовірність технічної атаки, а й тяжкість наслідків для конкретних категорій клієнтських даних і бізнес-процесів, у межах яких ці дані використовуються. Ще одна причина актуальності теми полягає в тому, що ризики в інформаційній сфері рідко проявляються ізольовано. Як правило, один недолік породжує ланцюг пов’язаних наслідків. Наприклад, слабка парольна політика сама по собі є вразливістю, але в поєднанні з відсутністю блокування облікового запису після кількох невдалих спроб входу вона перетворюється на канал підбору паролів. Якщо ж одночасно користувачеві надано надмірні права, а журналювання дій не забезпечує контроль масового експорту, то навіть компрометація одного облікового запису може призвести до масштабного витоку

клієнтської бази. Звідси випливає, що в телекомунікаційному підприємстві оцінювання ризиків має виконуватися системно і враховувати взаємозв’язок між активами, загрозами, вразливостями, бізнес-процесами та ролями персоналу. Таким чином, **актуальність** теми дипломної роботи визначається поєднанням трьох факторів: високої цінності клієнтських даних для підприємства та зловмисника, складності та багаторівневості процесів їх обробки в телекомунікаційних системах, а також наявності реальних організаційних і технічних недоліків, виявлених під час практики. Це зумовлює необхідність побудови такого підходу до оцінювання ризиків, який дозволить не лише перелічити потенційні загрози, а й виявити критичні точки в інфраструктурі, встановити взаємозалежність між джерелами небезпеки та можливими наслідками, а також сформувати основу для подальшого вибору заходів захисту.

1.2. Особливості предметної області: клієнтські дані та процеси їх обробки в телекомунікаційному підприємстві

Для коректного оцінювання ризиків необхідно насамперед визначити, які саме інформаційні активи підлягають захисту, де вони формуються, хто з ними працює та через які технічні засоби проходить їх життєвий цикл. У телекомунікаційному підприємстві ядром роботи з абонентами є CRM-система, пов’язана з внутрішньою мережею, базою даних, модулями укладання договорів, розрахунковими підсистемами, сервісом обробки звернень, інструментами технічної підтримки та резервного копіювання. Під час практики було встановлено, що така система функціонує через веб-інтерфейс і використовується співробітниками ІТ-відділу та операторами для виконання операцій з клієнтськими записами. Це означає, що предметна область дослідження має як технічний, так і організаційний вимір: безпека залежить не лише від наявності захищеного з’єднання чи налаштувань сервера, але й від того, як побудовано ролі, права доступу, контроль користувацьких дій, порядок створення резервних копій та регламенти обробки персональних даних.

На основі результатів, отриманих під час практики, виділено кілька категорій даних, які прямо впливають на рівень ризику. До першої категорії належать повні

ідентифікаційні дані клієнта. Вони дають змогу однозначно співвіднести запис у системі з конкретною фізичною особою і тому становлять підвищену цінність у випадку несанкціонованого доступу. До другої категорії відноситься контактна інформація, що використовується для обслуговування, ідентифікації та комунікації з абонентом. Третьою категорією є історія фінансових операцій, яка містить інформацію про нарахування, платежі, заборгованість, підключення додаткових послуг, перерахунки та інші дії, що прямо впливають на розрахунки з клієнтом. Четверта категорія охоплює технічні параметри підключення, котрі відображають характеристики сервісу, конфігурацію підключення, прив'язку до обладнання або точки доступу. П'ята категорія - історія звернень у службу підтримки, тобто операційна інформація про проблеми абонента, заявки, скарги та результати їх опрацювання. Кожна з названих категорій має різну чутливість, але в сукупності вони формують повний цифровий профіль клієнта. Особливість телекомунікаційного підприємства полягає в тому, що клієнтські дані проходять повний життєвий цикл: введення, уточнення, використання, передавання між модулями, резервування, відновлення, архівування та можливе вивантаження. На етапі введення особливу роль відіграє робота оператора, оскільки саме тут формується первинний запис, що надалі використовується іншими модулями системи. На етапі зберігання важливими є структура бази даних, сегментація доступу, механізми контролю цілісності, журналювання змін, політика резервного копіювання. Під час використання ключове значення мають правила авторизації та принцип мінімально необхідних прав. На етапі резервування та відновлення вирішальним стає не лише факт створення резервної копії, а й перевірка працездатності процедури відновлення. Під час архівування та експорту необхідно контролювати обсяг, легітимність і трасованість операцій, пов'язаних із масовим вивантаженням даних.

Життєвий цикл клієнтських даних у телекомунікаційному підприємстві подано на рисунку 1.1.

Рисунок 1.1 - Життєвий цикл клієнтських даних у телекомунікаційному підприємстві

Під час практики було встановлено, що доступ до CRM здійснювався через веб-інтерфейс із використанням захищеного з'єднання, а адміністратор підтвердив наявність SSL-сертифіката. Це свідчить, що на рівні транспортного захисту були реалізовані базові заходи безпеки. Однак для оцінювання ризику цього недостатньо, оскільки наявність захищеного каналу не усуває небезпеку компрометації облікових записів, неправильного розподілу прав або зловживання з боку співробітників. У телекомунікаційному підприємстві значна частина критичних інцидентів пов'язана саме з прикладним і організаційним рівнями захисту, де рішення щодо прав доступу, процедур адміністрування та правил роботи з даними визначають фактичний рівень ризику для клієнта. Підприємство телекомунікаційної сфери слід розглядати як систему з багатьма ролями користувачів. У ній присутні оператори абонентського відділу, працівники підтримки, системні адміністратори, аналітики, персонал розрахункових підрозділів, технічні спеціалісти з підключень, а інколи й зовнішні підрядники, які можуть отримувати обмежений доступ до окремих функцій. У межах такої ролезалежної системи будь-яка неточність у наданні доступів множить ризик, оскільки одна й та сама CRM може забезпечувати різним ролям перегляд, зміну, створення, експорт та видалення записів. Чим більша кількість ролей і чим глибше взаємопроникнення їхніх повноважень, тим вищими стають вимоги до системи

керування доступом. Важливо враховувати і те, що телекомунікаційні підприємства працюють у режимі безперервного надання послуг. На відміну від ізольованих корпоративних систем, тут порушення доступності або цілісності клієнтських даних швидко відображається на сервісному обслуговуванні. Якщо запис клієнта недоступний або спотворений, працівник не може коректно ідентифікувати абонента, перевірити стан договору, сформувати заявку, провести зміну тарифу чи усунути проблему з підключенням. Отже, в предметній області дослідження ризик слід розуміти як чинник, що здатний впливати не лише на захист даних у вузькому сенсі, а й на безперервність обслуговування клієнта та стабільність сервісного процесу в цілому. Таким чином, предметна область даної роботи охоплює сукупність клієнтських даних, інформаційних систем і організаційних процедур, за допомогою яких телекомунікаційне підприємство здійснює збирання, зберігання, обробку, використання та захист інформації про абонентів. Саме в межах цієї предметної області повинна будуватися модель оцінювання ризиків, що враховує ієрархію активів, ролі користувачів, життєвий цикл даних, технічні засоби захисту та практично виявлені слабкі місця.

Основні категорії клієнтських даних та їх значення для оцінювання ризиків наведено в таблиці 1.1.

Таблиця 1.1 – Основні категорії клієнтських даних та їх значення для оцінювання ризиків

Категорія даних	**Характеристика**	**Можливі наслідки порушення**	**Критичність**
Ідентифікаційні дані	ПІБ, паспортні та інші персональні реквізити, що однозначно ідентифікують клієнта	Шахрайські дії, несанкціоноване використання особистих даних, втрата довіри	Висока
Контактна інформація	Номер телефону, адреса, електронна пошта, канали зв’язку з абонентом	Несанкціонована комунікація, соціальна інженерія, порушення приватності	Середня/висока
Фінансові записи	Історія платежів, нарахувань,	Некоректні нарахування, спори з	Висока

	заборгованості, підключених сервісів	абонентами, фінансові збитки	
Технічні параметри підключення	Дані про конфігурацію послуги, обладнання, параметри доступу	Порушення сервісних налаштувань, ускладнення технічної підтримки	Середня
Історія звернень у підтримку	Заявки, скарги, результати опрацювання, сервісна історія	Репутаційні втрати, помилки в обслуговуванні, розкриття операційної інформації	Середня

1.3. Загрози, вразливості та можливі наслідки порушення безпеки клієнтських даних

Оцінювання ризиків інформаційної безпеки неможливе без системного аналізу загроз, вразливостей та наслідків. Загроза відображає потенційну можливість завдати шкоди інформаційному активу; вразливість – це слабке місце, через яке загроза може бути реалізована; наслідок характеризує ефект, що настає у випадку реалізації небажаної події. У телекомунікаційному підприємстві критичними наслідками є несанкціоноване розголошення персональних даних, спотворення фінансової інформації, втрата або недоступність клієнтських записів, неможливість відновлення після збою, а також порушення довіри абонентів до оператора. Саме поєднання цих компонентів утворює ризик як функцію ймовірності події та тяжкості її наслідків.

Взаємозв’язок активу, загрози, вразливості та наслідку показано на рисунку 1.2.

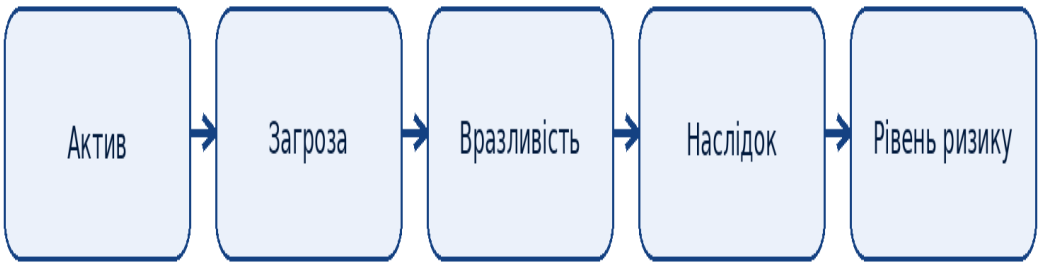

Рисунок 1.2 - Взаємозв’язок активу, загрози, вразливості та наслідку

Результати, отримані під час практики, дають змогу виділити низку конкретних вразливостей, властивих досліджуваному підприємству. Першою є недостатня жорсткість політики автентифікації. Було встановлено, що мінімальна довжина пароля становила вісім символів, але не було вимоги обов’язкового використання спеціальних символів. Окремо було з’ясовано, що система не блокувала обліковий запис після кількох невдалих спроб входу. Така комбінація недоліків створює передумови для підбору пароля, особливо якщо користувачі застосовують слабкі або шаблонні комбінації. Для телекомунікаційного підприємства це означає, що обліковий запис співробітника, який працює з CRM, може бути скомпрометований без подолання складних технічних бар’єрів, а отже, атака на рівні облікових даних стає більш імовірною. Другою суттєвою вразливістю є порушення принципу мінімально необхідних прав. У межах практики було з’ясовано, що окремі оператори мали доступ до розділів, не потрібних для виконання їхніх посадових обов’язків, зокрема до перегляду фінансової інформації всіх клієнтів. Подібна ситуація підвищує ризик як випадкових, так і умисних порушень. Навіть якщо співробітник не має наміру завдати шкоди, надлишковий доступ розширює площину можливих помилок: перегляд не того запису, внесення змін не у свій сегмент, некоректний експорт, використання конфіденційних відомостей без належної потреби. Якщо ж

відбудеться компрометація такого облікового запису, зловмисник одразу отримає ширший доступ до клієнтських даних, ніж це було б за умови суворого розмежування прав. Третя вразливість пов’язана з резервним копіюванням і відновленням. Під час практики було встановлено, що резервні копії бази даних створювалися автоматично, однак фактична перевірка процедури відновлення виконувалася нерегулярно. Ця обставина є дуже важливою для оцінювання ризиків, оскільки сам факт наявності резервних копій ще не гарантує відновлення працездатності після інциденту. Якщо резервна копія пошкоджена, створена з помилкою, несумісна з поточною версією системи або якщо персонал не має відпрацьованого сценарію відновлення, то в момент критичного збою підприємство може втратити значну частину даних або тривалий час залишатися без доступу до них. Для клієнтів це означатиме затримки в обслуговуванні, неможливість перевірки стану договорів, помилки в нарахуваннях та інші сервісні проблеми. Четверта вразливість стосується контролю масового експорту інформації. У межах практики було змодельовано сценарій несанкціонованого копіювання клієнтської бази співробітником із правами доступу. Результати показали, що експорт був можливим, а контроль за обсягом вивантажених даних був відсутній. Це одна з найбільш небезпечних ситуацій у контексті захисту клієнтів, оскільки загроза витоку в такому випадку реалізується не через складну зовнішню атаку, а через легітимний функціонал системи, який використовується без достатнього контролю. Якщо операція масового експорту не обмежується і не фіксується належним чином, то підприємство фактично не має механізму раннього виявлення масштабного виведення даних. П’ята група ризиків пов’язана з людським фактором і організаційними прогалинами. Серед запропонованих у роботі заходів окремо визначено регулярний перегляд прав доступу, проведення внутрішнього навчання з питань інформаційної безпеки та розробку внутрішнього документа, що регламентує порядок роботи з персональними даними клієнтів. Сам факт появи таких рекомендацій означає, що на підприємстві виявлено потребу не лише у вдосконаленні технічних засобів, але й в унормуванні поведінки персоналу. У телекомунікаційних системах навіть якісно налаштовані технічні засоби не

забезпечують потрібного рівня захисту, якщо співробітники не усвідомлюють критичність даних, не дотримуються процедур або не розуміють наслідків своїх дій.

Наслідки порушень безпеки доцільно розглядати крізь призму трьох класичних властивостей інформації: конфіденційності, цілісності та доступності. Порушення конфіденційності виникає у разі несанкціонованого ознайомлення з персональними або фінансовими даними клієнтів. У практичному кейсі це може бути перегляд надлишково доступної інформації оператором або експорт бази даних. Порушення цілісності полягає у внесенні несанкціонованих чи помилкових змін до фінансових записів, контактних реквізитів, технічних параметрів або історії звернень. За результатами практики саме цей вид порушення може призвести до неправильних нарахувань і конфліктів з абонентами. Порушення доступності виникає, коли через збій, атаку, пошкодження даних або неможливість відновлення система не може надати необхідну інформацію у потрібний час. Для підприємства, яке працює безперервно, це означає деградацію сервісу та втрату керованості клієнтським обслуговуванням. У контексті аналізу задачі важливо наголосити, що наслідки реалізації ризику мають подвійний характер. З одного боку, існує прямий вплив на клієнта: розголошення персональної інформації, помилки в розрахунках, недоступність обслуговування, потенційні шахрайські дії. З іншого боку, існує опосередкований вплив на підприємство: витрати на усунення інциденту, втрати довіри, погіршення репутації, зростання кількості звернень і скарг, необхідність проведення службових перевірок, перегляду політик доступу і технічної модернізації. Саме тому модель ризику має оцінювати не тільки технічну можливість інциденту, а й його бізнес-наслідки та вплив на взаємини з клієнтами. Отже, для досліджуваного телекомунікаційного підприємства критичними є загрози компрометації облікових записів, внутрішнього зловживання правами, неконтрольованого експорту даних, помилкової конфігурації доступів, а також неналежно організованого резервування й відновлення. Вразливості, виявлені під час практики, дають достатні підстави стверджувати, що без впорядкованого підходу до оцінювання ризиків підприємство не може об’єктивно визначити

пріоритети захисту. Саме це підводить до необхідності аналізу існуючих підходів до оцінювання ризиків і вибору такої схеми, яка найкраще відповідає специфіці обробки клієнтських даних у телекомунікаційній сфері.

1.4. Аналіз підходів до оцінювання ризиків інформаційної безпеки

У загальному вигляді оцінювання ризиків інформаційної безпеки передбачає послідовне виконання кількох взаємопов’язаних дій: ідентифікацію активів, визначення загроз, виявлення вразливостей, аналіз можливих сценаріїв реалізації небезпек, оцінювання ймовірності та наслідків, ранжування ризиків за рівнем критичності та підготовку пропозицій щодо їх мінімізації. У різних методичних школах акцент може зміщуватися в бік формалізованих кількісних оцінок або експертних якісних процедур, однак логічне ядро залишається незмінним: ризик має бути пов’язаний з конкретним активом, конкретним джерелом загрози та конкретними наслідками для організації і користувача. Для телекомунікаційного підприємства найпростішим і водночас достатньо ефективним на початковому етапі є якісний підхід, за якого ризики класифікуються за рівнями на кшталт низький, середній, високий або критичний. Перевагою такого підходу є відносна простота застосування в реальному середовищі, де не завжди можливо обчислити точну ймовірність кожного інциденту або вартісний еквівалент його наслідків. Якісний підхід дозволяє швидко пов’язати практичні спостереження з управлінськими рішеннями. Наприклад, відсутність блокування облікового запису після серії невдалих спроб входу, поєднана з надлишковими правами доступу, може бути віднесена до високого або критичного ризику навіть без складних математичних розрахунків, оскільки сценарій зловживання є зрозумілим, а наслідки – значними. Разом із тим лише якісна оцінка не завжди дає можливість порівняти альтернативні варіанти захисту, розставити інвестиційні пріоритети або обґрунтувати послідовність модернізації системи. З цієї причини доцільним є комбінований підхід, у якому якісне ранжування доповнюється елементами кількісної оцінки. Наприклад, можна оцінювати не абсолютну імовірність події, а частоту настання подібних ситуацій, кількість користувачів з надлишковими правами, обсяг записів, доступних для масового експорту, або критичність

категорій даних, що потрапляють у зону ризику. У такому разі підприємство отримує не лише описову характеристику проблеми, а й основу для зіставлення ризиків між собою. У класичній схемі аналізу ризику вихідною точкою є інформаційний актив. Для теми даної дипломної роботи найбільш цінними активами є персональні дані клієнтів, фінансові записи, технічна інформація про підключення, історія взаємодії із службою підтримки, облікові записи співробітників, база даних CRM, журнали подій та резервні копії. Наступним кроком є встановлення джерел загроз. Ними можуть бути зовнішні порушники, внутрішні користувачі, системні адміністратори, підрядники, зловмисне програмне забезпечення, технічні збої, помилки конфігурації або недоліки процедур. Після цього визначаються вразливості, через які загроза здатна реалізуватися: слабка парольна політика, відсутність багатофакторної автентифікації, надлишкові права, нерегулярне тестування відновлення, відсутність контролю вивантажень, неформалізовані регламенти роботи з персональними даними тощо. Лише коли ці елементи з’єднані між собою у сценарій, оцінка ризику набуває практичного сенсу. Значну роль відіграє вибір критеріїв оцінювання наслідків. У телекомунікаційній компанії недостатньо обмежитися загальною фразою про шкоду для безпеки. Доцільно оцінювати принаймні чотири виміри впливу: шкоду для клієнта, операційний вплив на підприємство, масштаб охоплення записів і складність відновлення після інциденту. Так, несанкціонований перегляд одного клієнтського запису матиме інший рівень критичності, ніж масовий експорт усієї бази. Аналогічно, короткочасна помилка в окремому полі відрізняється за наслідками від системного порушення цілісності фінансових даних або втрати резервних копій. Отже, модель оцінювання ризиків має бути багатокритеріальною, навіть якщо підсумкова оцінка подається у спрощеній шкалі. Для предметної області цієї роботи важливим є також процесний підхід. Ризик прив’язується не тільки до статичного активу, а й до конкретної операції: введення даних під час укладання договору, редагування клієнтського запису, перегляд фінансової історії, зміна параметрів підключення, створення резервної копії, відновлення бази, експорт інформації, обробка звернення в службі підтримки. Саме процесна деталізація

дозволяє виявити, на якому етапі виникає слабке місце і які ролі беруть участь у реалізації ризику. Перевага такого підходу особливо помітна у телекомунікаційній системі, де одна й та сама інформація може проходити через різні функціональні модулі й бути доступною різним категоріям персоналу. Ще одним важливим аспектом є розмежування зовнішніх і внутрішніх ризиків. У багатьох організаціях увага зосереджується переважно на мережевому периметрі, шифруванні каналів і захисті від зовнішніх атак. Проте практичні результати, отримані під час практики в межах переддипломної практики, показують, що суттєва частина небезпек концентрується всередині організації: надлишкові права користувачів, можливість перегляду чужої фінансової інформації, доступність масового експорту, недостатній контроль облікових записів. Це означає, що для оцінювання ризиків у телекомунікаційній компанії необхідно приділяти особливу увагу інсайдерським сценаріям, які реалізуються через легітимний функціонал системи. Суттєвим недоліком формального підходу до ризик-аналізу є те, що він інколи зводиться до заповнення переліку загроз без урахування конкретної інфраструктури. Для даної роботи більш доцільним є контекстний підхід, за якого кожний ризик аналізується в контексті реально існуючого середовища підприємства. Саме тому результати практики мають високу цінність: вони містять не абстрактні припущення, а фактичні спостереження за роботою CRM-системи, налаштуваннями автентифікації, структурою прав доступу, резервним копіюванням і сценаріями масового експорту. На цій підставі можна побудувати наближену до реальності модель ризику, де джерело загрози, уразливість і наслідок пов’язані з конкретною бізнес-функцією.

Підсумовуючи, до задачі оцінювання ризиків інформаційної безпеки клієнтів у телекомунікаційному підприємстві найбільш придатним є комбінований процесно-орієнтований підхід. Він поєднує якісне ранжування рівнів небезпеки, елементи кількісної деталізації, аналіз інформаційних активів, сценарний розгляд загроз і вразливостей, а також урахування ролей користувачів та етапів обробки даних. Саме такий підхід дозволяє перейти від загального опису проблеми до

формалізованої постановки задачі, що має бути вирішена у наступних розділах дипломної роботи.

1.5. Аналіз практичного кейсу підприємства як основи для постановки дослідницької задачі

Практична цінність дослідження суттєво зростає тоді, коли теоретичний аналіз підкріплюється реальними спостереженнями за функціонуванням інформаційної системи. Матеріали переддипломної практики, відображають саме такий приклад. Під час практики здійснювалася взаємодія із системним адміністратором і співробітниками IT-відділу, що забезпечують роботу CRM-системи та внутрішньої мережі. Основний фокус було зосереджено на аналізі ризиків інформаційної безпеки клієнтів, які виникають у процесі обробки персональних даних. Це дозволяє використовувати результати практики як фактичну основу для формулювання аналітичної та дослідницької частини першого розділу. Першим значущим результатом практики є ідентифікація критичних категорій інформації. Було встановлено, що система зберігає повні ідентифікаційні дані клієнтів, контактну інформацію, історію фінансових операцій, технічні параметри підключення та історію звернень у службу підтримки. З точки зору ризик-аналізу це свідчить про високу щільність чутливих відомостей в одному інформаційному середовищі. Поєднання цих даних в одній системі підвищує ризик кумулятивної шкоди, оскільки навіть один інцидент може призвести не до часткового, а до комплексного порушення безпеки клієнта. Наприклад, одночасне розголошення контактних і фінансових відомостей посилює можливості соціальної інженерії, шахрайства та несанкціонованого використання клієнтського профілю. Другим важливим результатом став аналіз критичності даних. У межах практики було зроблено висновок, що витік паспортних даних здатний спричинити шахрайські дії та юридичну відповідальність підприємства, а порушення цілісності фінансових записів - некоректні нарахування та конфлікти з абонентами. Це означає, що для різних категорій інформації слід застосовувати різні критерії тяжкості наслідків. У межах моделі оцінювання ризиків персональні ідентифікаційні дані доцільно пов’язувати насамперед із наслідками для

конфіденційності, фінансові записи - з наслідками для цілісності, а резервні копії та доступність CRM - з наслідками для безперервності обслуговування. Таким чином, уже на стадії аналізу практики формується структурований погляд на активи та пріоритети захисту. Третій блок результатів стосується аналізу процесу обробки персональних даних. Під час практики було простежено шлях інформації від моменту її внесення до системи до архівування. Це дуже важливий спостережний матеріал, оскільки дозволяє перейти від статичної моделі активів до процесної моделі ризиків. Якщо дані розглядаються не просто як записи у базі, а як інформація, що проходить етапи введення, обробки, зберігання, використання та архівування, тоді можна точніше виявити місця виникнення загроз. У випадку досліджуваного підприємства такими місцями є веб-інтерфейс CRM, ролі операторів, адміністративні налаштування сервера, процедури резервування та механізм експорту. Четвертий важливий аспект – наявність базових технічних заходів захисту в поєднанні з помітними організаційними та прикладними недоліками. З одного боку, було підтверджено використання захищеного з'єднання та SSL-сертифіката. Це свідчить, що підприємство приділяє увагу захисту каналу передавання даних. З іншого боку, виявлені слабкі місця у механізмах автентифікації: недостатня складність паролів і відсутність блокування облікового запису після кількох невдалих спроб входу. У термінах оцінювання ризику це означає, що частина захисту реалізована на зовнішньому рівні, але не доведена до належного стану на рівні доступу користувачів. Отже, для побудови об'єктивної моделі ризиків недостатньо фіксувати наявність окремих заходів – необхідно оцінювати їх комплексність та узгодженість. П'ятий блок спостережень пов'язаний із ролями та правами користувачів. Під час практики було виявлено, що деякі оператори мали доступ до розділів, не потрібних для виконання посадових обов'язків, зокрема до фінансової інформації всіх клієнтів. Саме цей факт є ключовим для постановки задачі дипломної роботи, оскільки він дозволяє перевести проблему з площини загальних міркувань у площину конкретної системної вразливості. Якщо користувач має більший обсяг прав, ніж це потрібно для виконання його функцій, тоді будь-яка помилка, компрометація або

недобросовісна дія такого користувача автоматично набуває ширших наслідків. Це також свідчить, що на підприємстві необхідно не тільки налаштовувати ролі, а й періодично проводити аудит фактичних доступів. Шостий блок стосується резервного копіювання. На практиці було підтверджено факт автоматичного створення резервних копій бази даних, але також встановлено, що тестування процедури відновлення проводиться нерегулярно. Цей результат є особливо показовим, оскільки демонструє типову помилку в організації інформаційної безпеки: наявність заходу розглядається як достатня умова захисту, хоча насправді важлива його працездатність у реальному сценарії відновлення. Для клієнтоорієнтованої телекомунікаційної системи невідпрацьоване відновлення означає ризик тривалої зупинки сервісів, втрати історії взаємодії з абонентом і неможливості коректно обслуговувати клієнтські запити. Звідси випливає, що в системі оцінювання ризиків резервування має аналізуватися не як формальна наявність копії, а як перевірювана спроможність повернути систему до працездатного стану. Сьомим результатом практики є моделювання сценарію несанкціонованого копіювання клієнтської бази співробітником із правами доступу. Було з’ясовано, що експорт можливий, а контроль за обсягом вивантажених даних відсутній. Це один із найбільш критичних висновків, оскільки він указує на пряму можливість реалізації внутрішнього інциденту із великим масштабом наслідків. Для телекомунікаційного підприємства, у якому база клієнтів є одним із ключових активів, відсутність контролю масового експорту означає ризик одномоментного витоку значного масиву персональних, фінансових і технічних відомостей. У межах подальшого дослідження такий сценарій доцільно розглядати як один із базових еталонних випадків для оцінки критичності ризиків. Окремої уваги заслуговують рекомендації, сформовані за результатами практики. Серед технічних заходів запропоновано впровадження двофакторної автентифікації для користувачів із розширеними правами, автоматичне блокування облікового запису після п’яти невдалих спроб входу, посилення вимог до складності паролів та впровадження контролю масового експорту інформації. Серед організаційних заходів визначено регулярний перегляд прав доступу,

навчання з питань інформаційної безпеки та розроблення внутрішнього документа щодо порядку роботи з персональними даними клієнтів. Ці рекомендації виконують подвійну функцію: з одного боку, демонструють напрямки зниження ризиків, а з іншого - опосередковано підтверджують ті проблемні зони, які були виявлені в ході аналізу. На основі розглянутого практичного кейсу можна зробити кілька принципових висновків, важливих для постановки задачі дослідження. По-перше, безпека клієнтів у телекомунікаційному підприємстві значною мірою визначається станом CRM-системи як центрального вузла обробки персональних і сервісних даних. По-друге, критичні ризики породжуються не стільки відсутністю будь-якого захисту, скільки невідповідністю між окремими реалізованими засобами безпеки та реальними сценаріями доступу й використання даних. По-третє, внутрішні загрози та надлишкові повноваження співробітників мають не менше значення, ніж зовнішні атаки. По-четверте, якісна оцінка ризиків повинна спиратися на конкретні бізнес-процеси й фактичні спостереження, а не на загальний перелік загроз. Саме тому практичний матеріал не слід розглядати як додаток до теоретичного аналізу. Навпаки, він є основою формування дослідницької задачі. Завдання першого розділу полягає в тому, щоб на базі виявлених фактів перейти від констатації окремих недоліків до побудови цілісної логіки: визначити об’єкт і предмет дослідження, окреслити цілі оцінювання ризиків, виділити пріоритетні активи, сформувати перелік найнебезпечніших сценаріїв порушень і обґрунтувати потребу в розробленні підходу, який дозволить системно оцінювати рівень ризику для клієнтів телекомунікаційного підприємства.

Карту практично виявлених слабких місць CRM-системи наведено на рисунку 1.3.

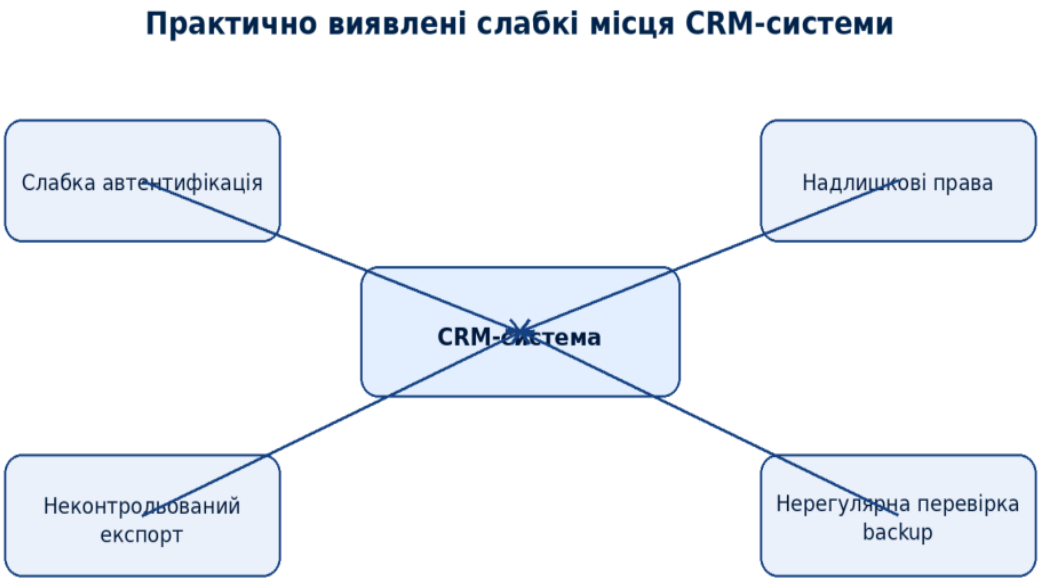

Рисунок 1.3 - Карта практично виявлених слабких місць CRM-системи

Виявлені під час практики слабкі місця та їх ризикові наслідки узагальнено в таблиці 1.2.

Таблиця 1.2 – Виявлені під час практики слабкі місця та їх ризикові наслідки

Слабке місце	**Сутність проблеми**	**Можливий наслідок**	**Пріоритет**
Слабка парольна політика	Мінімальна довжина пароля без посилених вимог до складності	Підвищення ймовірності компрометації облікового запису	Високий
Відсутність блокування після невдалих спроб	Обліковий запис не блокується після серії помилкових входів	Можливість підбору пароля та несанкціонованого входу	Високий
Надлишкові права операторів	Доступ до фінансової інформації всіх клієнтів без службової потреби	Внутрішній витік, помилкові дії, розширення масштабу інциденту	Критичний
Нерегулярне тестування відновлення	Є резервні копії, але процедура відновлення перевіряється не системно	Неможливість швидкого відновлення після збою, втрата доступності	Високий
Відсутність контролю масового експорту	Можливе вивантаження великих масивів даних без належного контролю	Масовий витік клієнтської бази, важкі репутаційні наслідки	Критичний

1.6. Формулювання проблеми, об’єкта, предмета, мети та завдань дослідження

Відповідно до методичних рекомендацій до виконання атестаційних випускних робіт перший розділ повинен містити опис проблеми, формулювання поставленої задачі, визначення об’єкта, предмета та мети дослідження, аналіз стану

вирішення задачі та обґрунтування доцільності подальшої розробки. Для теми даної дипломної роботи така логіка є цілком виправданою, оскільки досліджувана проблема має виразний прикладний характер і безпосередньо пов’язана з реальною практикою функціонування CRM-системи телекомунікаційного підприємства. Проблема дослідження полягає в тому, що телекомунікаційне підприємство обробляє великі обсяги критично важливих клієнтських даних у багаторівневому середовищі, де одночасно діють технічні, організаційні та людські чинники ризику, тоді як наявні засоби захисту не завжди забезпечують достатній контроль доступу, автентифікації, резервування, відновлення та запобігання масовому витоку інформації. За таких умов підприємство потребує впорядкованого підходу до оцінювання ризиків, який дозволить виявити найбільш небезпечні сценарії порушення безпеки клієнтів та визначити пріоритетні напрямки зниження ризиків. Об’єктом дослідження є процеси обробки та захисту клієнтських даних у телекомунікаційному підприємстві. Таке формулювання відображає проблемну сферу, у межах якої виникають ризики та відбувається взаємодія інформаційної системи, персоналу й клієнтських даних.

Предметом дослідження є методи, моделі та критерії оцінювання ризиків інформаційної безпеки клієнтів у процесі функціонування CRM-системи та пов’язаних із нею бізнес-процесів телекомунікаційного підприємства. Предмет фокусує увагу саме на механізмах виявлення, аналізу та ранжування ризиків, що виникають під час зберігання, обробки, перегляду, резервування й експорту клієнтської інформації. Метою дипломної роботи є підвищення обґрунтованості управління інформаційною безпекою клієнтів телекомунікаційного підприємства шляхом аналізу предметної області та розроблення підходу до оцінювання ризиків, який враховує критичність клієнтських даних, ролі користувачів, сценарії внутрішніх і зовнішніх загроз, а також виявлені у практичному середовищі вразливості CRM-системи.

Для досягнення поставленої мети необхідно вирішити такі основні завдання: 1) проаналізувати специфіку телекомунікаційного підприємства як середовища обробки клієнтських даних;

2) визначити основні категорії інформаційних активів, пов’язаних з клієнтами, та оцінити їх критичність;
3) виявити загрози і вразливості, характерні для CRM-системи та процесів роботи з персональними даними;
4) проаналізувати наслідки порушення конфіденційності, цілісності та доступності клієнтської інформації;
5) дослідити практично виявлені недоліки в механізмах автентифікації, керування доступом, резервного копіювання та контролю експорту даних;
6) обґрунтувати вибір підходу до оцінювання ризиків, придатного для умов телекомунікаційного підприємства;
7) сформувати основу для подальшого проєктування або вдосконалення системи зниження ризиків інформаційної безпеки клієнтів.

Постановка задачі дослідження може бути сформульована таким чином: необхідно розробити аналітичний підхід до оцінювання ризиків інформаційної безпеки клієнтів у телекомунікаційному підприємстві, який дозволяє на підставі аналізу інформаційних активів, процесів обробки даних, ролей користувачів, вразливостей та сценаріїв загроз визначати рівень критичності ризику й обґрунтовувати першочергові заходи щодо його зниження. Практичним обмеженням задачі є орієнтація на реальне CRM-середовище, у якому вже виявлено слабкі місця: недостатньо жорстку автентифікацію, надлишкові права доступу, нерегулярне тестування відновлення резервних копій і відсутність контролю масового експорту даних. Отже, у межах першого розділу сформовано теоретичне та прикладне підґрунтя для подальших етапів дипломної роботи. Далі дослідження має перейти від аналізу проблеми до побудови моделі оцінювання ризиків та розроблення практичних рішень, спрямованих на зниження рівня небезпеки для клієнтських даних і підвищення стійкості інформаційних процесів телекомунікаційного підприємства.

Висновки до розділу 1

У першому розділі здійснено комплексний аналіз задачі оцінювання ризиків інформаційної безпеки клієнтів у телекомунікаційних підприємствах. Показано, що

актуальність теми зумовлена високою концентрацією персональних, фінансових і технічних даних клієнтів у CRM-системах, багаторівневим характером їх обробки та суттєвими наслідками порушення конфіденційності, цілісності й доступності інформації. Встановлено, що в телекомунікаційній сфері ризик має не лише технічний, а й виразний організаційний та сервісний вимір, оскільки напряму впливає на якість обслуговування абонентів і рівень довіри до підприємства.

На основі аналізу предметної області визначено основні категорії клієнтських даних, життєвий цикл їх обробки та роль CRM-системи як центрального елемента інформаційної інфраструктури. Розглянуто типові загрози і вразливості, серед яких особливу небезпеку становлять слабкі механізми автентифікації, надлишкові права доступу, недоліки резервного копіювання та неконтрольований масовий експорт даних. Показано, що для об’єктивної оцінки ризиків необхідно враховувати не тільки наявність окремих засобів захисту, а й реальні сценарії взаємодії користувачів із системою. Переддипломна практика підтвердила прикладний характер проблеми та надала фактичну основу для формування дослідницької задачі. Отримані практичні результати засвідчили наявність слабких місць у процесах обробки персональних даних клієнтів, що обґрунтовує необхідність системного підходу до оцінювання ризиків. У результаті визначено об’єкт, предмет, мету та основні завдання дослідження, а також сформульовано постановку задачі, яка слугує підґрунтям для наступних розділів дипломної роботи, де має бути розроблено та застосовано підхід до оцінювання ризиків інформаційної безпеки клієнтів у телекомунікаційному підприємстві.

РОЗДІЛ 2
МЕТОДИКА ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КЛІЄНТІВ ТЕЛЕКОМУНІКАЦІЙНОГО ПІДПРИЄМСТВА

2.1. Принципи та вимоги до побудови методики оцінювання ризиків

У другому розділі здійснюється перехід від загального аналізу задачі до побудови власної методики оцінювання ризиків інформаційної безпеки клієнтів у телекомунікаційному підприємстві. Необхідність такого переходу зумовлена тим, що в межах першого розділу було визначено коло критичних активів, описано типові загрози та вразливості, а також підтверджено їх наявність результатами переддипломної практики. Однак сам по собі перелік проблем не дає підприємству інструменту для прийняття рішень. Підприємство потребує формалізованої процедури, яка дає змогу однаково оцінювати різні ризикові сценарії, порівнювати їх між собою, визначати пріоритетність захисних заходів та обґрунтовувати управлінські рішення щодо інвестування в безпеку. Запропонована методика орієнтована саме на клієнтський контур телекомунікаційного підприємства. Це означає, що в центрі оцінювання перебувають не будь-які інформаційні активи організації загалом, а ті активи, процеси та технічні засоби, які безпосередньо пов’язані зі збором, зберіганням, передаванням, коригуванням, архівуванням і видаленням персональних та пов’язаних з ними облікових даних абонентів. Такий акцент є принципово важливим, оскільки ризики для серверного обладнання, мережевої інфраструктури чи офісних робочих місць не завжди однаково впливають на інтереси клієнтів. Наприклад, короткочасний збій внутрішнього сервісу може бути критичним для бізнес-процесів компанії, але не становити прямої загрози конфіденційності клієнтських даних. Натомість надлишкові права доступу до фінансової історії абонента мають прямий і високий ризиковий ефект саме для клієнта.

При побудові методики вихідним є положення про те, що сучасне телекомунікаційне підприємство працює як багаторівнева соціотехнічна система. На рівні даних у ній циркулюють паспортні, контактні, фінансові та технічні

відомості про абонентів. На рівні процесів відбуваються укладення договорів, підключення послуг, ведення історії звернень, нарахування платежів, обробка заявок до технічної підтримки та формування аналітичної звітності. На рівні користувачів діють оператори, менеджери, адміністратори, співробітники підтримки, бухгалтерія та керівники. На рівні технологій використовуються CRM-система, база даних, засоби резервного копіювання, канали віддаленого доступу, інтерфейси експорту та засоби автентифікації. Тому методика повинна одночасно враховувати і властивості активів, і поведінку користувачів, і стан технічних та організаційних засобів захисту.

Запропонована методика спирається на такі базові принципи:

Загальну логіку методики оцінювання ризиків подано на рисунку 2.1.

Рисунок 2.1 - Загальна логіка методики оцінювання ризиків

1) системність: ризик оцінюється не як ізольований інцидент, а як результат взаємодії джерела загрози, вразливості, активу та можливого наслідку;

2) відтворюваність: різні експерти, маючи однакові вхідні дані, повинні отримувати близькі результати;

3) гнучкість: методика має застосовуватися як для невеликого оператора зв’язку, так і для більшого підприємства з розгалуженою структурою доступу;

4) практична придатність: етапи оцінювання мають виконуватися на основі реальних даних, доступних на підприємстві, без надмірно складних статистичних моделей;

5) орієнтація на рішення: результатом оцінювання має бути не лише числове значення ризику, а й перелік контрзаходів, які доцільно впроваджувати першочергово.

Окремо враховано вимогу до поєднання якісного та кількісного підходів. Суто якісна модель на рівні формулювань «низький - середній - високий» є зручною для швидкого опису стану безпеки, але недостатньо придатною для порівняння ризиків між собою. Суто кількісний підхід, навпаки, вимагає значного обсягу статистичних даних про частоту подій, економічний збиток, ймовірності реалізації атак та інші параметри, які на практиці часто відсутні або неповні. Саме тому запропоновано напівкількісну методику, у якій основні характеристики ризику оцінюються за шкалами від 1 до 5, а підсумкова величина ризику розраховується за простою формулою. Такий підхід дає змогу поєднати наочність, достатню точність і зручність застосування. Ще однією вимогою до методики є врахування трьох класичних цілей безпеки - конфіденційності, цілісності та доступності - але не лише в технічному, а й у бізнесовому вимірі. Для клієнтських даних наслідки інциденту майже завжди виходять за межі IT-підсистеми. Порушення конфіденційності персональних даних призводить до репутаційних втрат, юридичних претензій і зниження довіри абонентів. Порушення цілісності може спричинити хибні нарахування, помилки в договорах, некоректні технічні параметри підключення або неконсистентність історії обслуговування. Порушення доступності позбавляє оператора можливості швидко обслуговувати клієнта, а клієнта - можливості отримати послугу або підтримку. Тому в межах методики додається до класичних критеріїв також юридичний та репутаційний вплив як окремі складові наслідку.

На відміну від універсальних схем ризик-аналізу, у запропонованій методиці значна увага приділяється внутрішньому порушнику. Це безпосередньо випливає з результатів практики, під час якої було встановлено наявність надлишкових прав

доступу окремих операторів, можливість масового експорту інформації та відсутність достатнього контролю за такими діями. У телекомунікаційному підприємстві внутрішній порушник є не менш небезпечним, ніж зовнішній атакувальник, оскільки він вже має легітимний доступ до інформаційного середовища, розуміє структуру даних і може приховувати свою активність у потоці звичайних операцій. Саме тому запропонована методика оцінює не лише можливість технічного злому, а й ризики зловживання штатними повноваженнями, помилок персоналу та порушення процедур. Отже, вимоги до побудови методики можна узагальнити таким чином: вона повинна бути орієнтованою на клієнтські дані, процесно-рольовою, напівкількісною, придатною до регулярного застосування та здатною переводити результати аналізу в конкретний перелік пріоритетних заходів. У подальших підрозділах формується структура активів, описується механізм ідентифікації загроз і вразливостей, задаються шкали оцінювання та пропонується порядок розрахунку первинного і залишкового ризику. Саме така логіка відповідає темі дипломної роботи та дає змогу перетворити результати практики на формалізований дослідницький інструмент.

2.2. Формування моделі активів, ролей та процесів обробки клієнтських даних

Будь-яке оцінювання ризиків починається з визначення того, що саме потребує захисту. У межах даної роботи розглядається актив не тільки як файл, запис у таблиці бази даних або серверний ресурс. Для телекомунікаційного підприємства активом є будь-який елемент, втрата конфіденційності, цілісності або доступності якого здатна завдати шкоди клієнту, бізнес-процесу або правовому становищу підприємства. Такий підхід дозволяє перейти від вузького технічного бачення до комплексної моделі, у якій разом розглядаються дані, програмні засоби, бізнес-процеси, канали взаємодії з клієнтом і ролі персоналу. На підставі результатів практики виділено п’ять базових груп активів. До першої належать персональні ідентифікаційні дані клієнта: прізвище, ім’я, по батькові, реквізити документів, адреса проживання, дата народження, інші відомості, що дають змогу однозначно ідентифікувати особу. До другої групи належать контактні та

комунікаційні дані: номер телефону, електронна адреса, канали оповіщення, історія звернень у службу підтримки. Третю групу складають фінансові дані: історія оплат, заборгованість, нарахування, тарифи, інформація про послуги та платежі. Четверта група охоплює технічні параметри підключення: адреси вузлів, параметри обладнання, стан підключення, характеристики послуг. П’ята група містить службові журнали, записи аудиту, дані про автентифікацію та журнали операцій експорту, які хоча й не є клієнтськими даними у вузькому значенні, але безпосередньо визначають можливість контролю безпеки. Поряд із власне даними виділено технологічні активи, без яких неможливо забезпечити належний захист клієнтської інформації. До них належать CRM-система як центральна прикладна платформа, база даних як основне сховище, сервер автентифікації або модуль керування обліковими записами, система резервного копіювання, журнали подій, інтерфейс експорту та робочі місця співробітників, що мають доступ до клієнтського контуру. Наступним кроком формується модель ролей. Для досліджуваної предметної області ключовими є оператори абонентського відділу, технічні спеціалісти, співробітники служби підтримки, бухгалтерія, системні адміністратори, керівники підрозділів та аудитори або відповідальні за інформаційну безпеку. Кожна роль має власний профіль доступу, набір типових операцій та свою ризикову характеристику. Оператор, наприклад, часто працює з персональними даними у режимі реального часу, але не повинен мати широкого доступу до фінансових або системних налаштувань. Системний адміністратор має підвищені привілеї, але його дії повинні бути особливо прозорими, контрольованими та журналюваними. Керівник може бачити агреговані звіти, однак для нього небажаний доступ до детальних персональних полів без належного обґрунтування.

Після визначення активів і ролей здійснюється перехід до моделі процесів. Для цілей оцінювання ризиків доцільно розглядати такі основні процеси: первинне введення даних під час укладення договору; актуалізація клієнтських записів; обробка фінансових операцій; технічне обслуговування підключення; взаємодія зі службою підтримки; формування звітності; резервне копіювання та відновлення;

архівування і видалення даних. Саме процесний підхід дозволяє побачити точки входу загроз. Наприклад, ризик виникає не просто через факт існування таблиці з фінансовою інформацією, а під час її перегляду оператором, масового експорту керівником, резервного копіювання адміністратором або відновлення після збою. Для того щоб методика була практично придатною, активи, ролі та процеси об'єднуються в єдину аналітичну модель. Кожен ризиковий сценарій надалі описується через чотири компоненти: цільовий актив, процес, у межах якого відбувається подія, роль або джерело загрози, а також вразливість, що створює передумови для інциденту. Така структура дає змогу не просто перелічити активи, а пов'язати їх із реальними діями користувачів та технічними операціями. Побудована модель активів, ролей і процесів виконує одразу кілька функцій. По-перше, вона усуває розмитість предмета оцінювання. По-друге, вона створює основу для інвентаризації ризикових сценаріїв. По-третє, вона дає змогу пов'язати результати оцінювання з конкретними заходами захисту: керуванням доступом, автентифікацією, аудитом, резервуванням, навчанням персоналу або регламентацією процедур. Саме завдяки такій моделі запропонована методика не обмежується абстрактними міркуваннями про безпеку, а працює на рівні конкретних елементів телекомунікаційного підприємства.

Основні групи активів, ролей і процесів у межах оцінювання ризиків наведено в таблиці 2.1.

Таблиця 2.1 - Основні групи активів, ролей і процесів у межах оцінювання ризиків

Група	**Приклади активів/елементів**	**Основні ролі**	**Ключові процеси**
Персональні дані	ПІБ, реквізити документів, адреса, ідентифікаційні відомості	Оператор, менеджер, адміністратор	Укладення договору, актуалізація профілю, архівування
Контактні та сервісні дані	Телефон, e-mail, історія звернень, параметри комунікації	Оператор, служба підтримки	Комунікація з клієнтом, обробка заявок, сповіщення

Група	Приклади активів/елементів	Основні ролі	Ключові процеси
Фінансові дані	Нарахування, платежі, заборгованість, тарифні плани	Бухгалтерія, оператор, керівник	Розрахунки, звітність, перевірка платежів
Технічні дані	Параметри підключення, обладнання, статус послуги	Технічний фахівець, адміністратор	Підключення, налаштування, усунення несправностей
Засоби контролю та журнали	Логи входів, журнали змін, резервні копії, дані аудиту	Адміністратор, аудитор, ІБ-фахівець	Моніторинг, аудит, резервування, відновлення

2.3. Ідентифікація загроз, вразливостей та формування ризикових сценаріїв

Після визначення структури активів та процесів здійснюється перехід до ідентифікації загроз і вразливостей. Для потреб телекомунікаційного підприємства доцільно вважати недостатнім просте складання переліку «можливих небезпек». Такий перелік часто виявляється занадто загальним і не дає змоги оцінити реальний стан захисту. Тому в межах методики формується ризиковий сценарій як поєднання джерела загрози, конкретної вразливості, цільового активу, процесу реалізації та наслідку для клієнтських даних. Саме сценарний підхід дозволяє зв’язати фактичні спостереження, отримані під час практики, з формалізованим розрахунком ризику.

Джерела загроз поділено на чотири основні групи. Перша група - зовнішні порушники: кіберзлочинці, шахраї, сторонні особи, які намагаються отримати доступ до облікових записів, каналів зв’язку або даних через мережеві атаки, фішинг чи підбір паролів. Друга група - внутрішні порушники: штатні співробітники, підрядники або тимчасовий персонал, що вже мають легітимний доступ до системи і можуть свідомо або випадково порушити режим безпеки. Третя група - технічні та інфраструктурні фактори: відмови обладнання, програмні помилки, збої під час оновлення, пошкодження резервних копій, помилки адміністрування. Четверта група - організаційні фактори: відсутність регламентів, недостатнє навчання, невиконання процедур перевірки доступів, слабкий аудит операцій користувачів. На практиці саме поєднання внутрішніх та організаційних

чинників виявилося особливо значущим. Під час аналізу досліджуваної CRM-системи було встановлено, що політика паролів має обмежену жорсткість, не реалізоване блокування облікового запису після кількох невдалих спроб входу, окремі оператори мають ширші повноваження, ніж це необхідно, а контроль масового експорту даних відсутній. Окрім цього, перевірка процедури відновлення резервних копій проводиться нерегулярно. Усі ці факти свідчать, що ризики для клієнтських даних тут породжуються не лише складними зовнішніми атаками, а й повсякденними організаційними прогалинами. Щоб забезпечити повноту аналізу, використовується класифікацію вразливостей за трьома рівнями. На технологічному рівні до вразливостей належать слабка автентифікація, відсутність 2FA, недостатнє журналювання, відсутність обмежень на експорт, залежність від єдиного вузла або недостатній контроль цілісності резервних копій. На процедурному рівні це відсутність регулярного перегляду ролей, формалізованої процедури затвердження доступів, графіка тестового відновлення, правил реагування на підозрілу активність та процедур повідомлення про інциденти. На людському рівні вразливості пов’язані з помилками персоналу, недооцінкою вимог безпеки, використанням слабких паролів, спробами обійти регламенти або виконати операції «для зручності» без належного погодження. Наступним кроком є формування сценаріїв. Кожен сценарій повинен бути достатньо конкретним, щоб його можна було оцінити за однаковими шкалами. Наприклад, сценарій «внутрішній користувач виконує масовий експорт клієнтської бази без погодження» є придатним для оцінювання, оскільки має зрозуміле джерело загрози, актив, вразливість і наслідок. Натомість загальне формулювання «витік даних» є надто широким і не дозволяє встановити, які саме контролі необхідно впроваджувати. Для телекомунікаційного підприємства виділено щонайменше шість базових сценаріїв, що повинні оцінюватися в обов’язковому порядку. Перший сценарій - компрометація облікового запису співробітника через слабку автентифікацію. Другий - перегляд або модифікація фінансових даних через надлишкові права доступу. Третій - масовий експорт клієнтської бази без погодження. Четвертий - неможливість відновлення клієнтських даних після збою.

П’ятий - несанкціонована зміна критичних записів. Шостий - використання історії звернень клієнта для соціальної інженерії.

Окремо слід підкреслити, що ризиковий сценарій має описувати не лише технічну подію, а й механізм її виявлення. Якщо підприємство не здатне своєчасно побачити реалізацію загрози, фактичний ризик зростає. Саме тому при формуванні сценаріїв рекомендується одразу фіксувати, чи існує журнал аудиту відповідної дії, чи аналізуються аномалії, чи є автоматичні сповіщення, чи перевіряється правомірність операції постфактум. У випадку з масовим експортом або надлишковими правами відсутність якісного аудиту робить наслідки більш імовірними і більш масштабними.

Таким чином, етап ідентифікації загроз і вразливостей у запропонованій методиці є не довідковим, а конструктивним. На цьому етапі формується набір сценаріїв, який надалі перетворюється на основу для кількісного ранжування ризиків. Практична цінність такого підходу полягає в тому, що підприємство отримує не абстрактний перелік небезпек, а робочий реєстр ситуацій, для кожної з яких можна оцінити ймовірність, наслідок, ефективність чинних засобів контролю та пріоритетність захисних заходів.

Типові загрози та вразливості для клієнтського контуру CRM-системи наведено в таблиці 2.2.

Таблиця 2.2 - Типові загрози та вразливості для клієнтського контуру CRM-системи

Джерело загрози	**Вразливість**	**Цільовий актив**	**Можливий наслідок**
Зовнішній порушник	Слабка парольна політика, відсутність блокування після серії помилок	Облікові записи співробітників, персональні дані	Компрометація акаунта, перегляд або копіювання даних
Внутрішній користувач	Надлишкові права доступу	Фінансова історія, договори, профілі клієнтів	Несанкціонований перегляд або зміна записів
Працівник/підрядник	Відсутність контролю масового експорту	База клієнтських даних у цілому	Масовий витік, юридичні та репутаційні втрати

Джерело загрози	Вразливість	Цільовий актив	Можливий наслідок
Технічний збій	Нерегулярне тестування відновлення	Резервні копії, база даних	Втрата доступності та часткова втрата цілісності
Помилка персоналу	Відсутність регламентів та навчання	Історія звернень, контактні дані	Неправомірне розкриття, соціальна інженерія

2.4. Побудова критеріїв і шкал оцінювання

Щоб перейти від опису сценаріїв до зіставних результатів, необхідно ввести єдині критерії оцінювання. У межах даної роботи використовується напівкількісний підхід, у якому базові параметри ризику задаються за п’ятибальною шкалою. Перевага цього підходу полягає в тому, що він дозволяє працювати навіть за відсутності повних статистичних даних, але водночас забезпечує достатню деталізацію для ранжування загроз. П’ятирівнева шкала є оптимальною для досліджуваного підприємства, оскільки вона не є надмірно грубою, як трибальна, і не створює ілюзії надточності, як це іноді трапляється в семи- або десятибальних системах. Перший ключовий параметр - це імовірність реалізації сценарію. На відміну від спрощеного підходу, коли імовірність визначається «на око», запропоновано розкладати її на три компоненти: частоту або передумови появи події, експлуатованість вразливості та рівень доступності активу для джерела загрози. Частота відображає, наскільки часто умови для такої події виникають у поточному процесі. Експлуатованість характеризує, наскільки просто використати наявну вразливість. Рівень доступності показує, чи має порушник фактичну можливість дістатися до активу або функції системи. Саме поєднання цих трьох компонентів дозволяє уникнути ситуації, коли високий ризик приписується рідкісним, але емоційно яскравим загрозам. Другий параметр - наслідок реалізації ризику. Для клієнтського контуру телекомунікаційного підприємства доцільно вважати за доцільне визначати наслідок не як єдине число, а як зважену комбінацію п’яти складових: вплив на конфіденційність, вплив на цілісність, вплив на доступність, юридичний вплив і репутаційний вплив. Така структура пов’язана з тим, що одна й та сама подія може по-різному проявлятися в

різних площинах. Наприклад, компрометація пароля оператора насамперед загрожує конфіденційності, тоді як відмова процедури відновлення з резервної копії сильніше впливає на доступність і цілісність. Водночас обидві події можуть мати юридичні та репутаційні наслідки для підприємства. Окремого врахування потребує ефективність чинних засобів захисту. У традиційних матрицях ризику цей параметр часто залишається поза розрахунком: експерти оцінюють ризик так, ніби жодних захисних заходів не існує. На практиці це призводить до того, що однакову оцінку можуть отримати сценарії з принципово різним рівнем керованості. Тому в запропонованій методиці використовується параметр K - ефективність чинного контролю, який зменшує первинний ризик і дозволяє отримати залишковий ризик. Показник ефективності контролю доцільно оцінювати за п’ятибальною шкалою: 1 - контроль відсутній або суто декларативний; 2 - контроль існує частково, але реалізований нестабільно або не охоплює всі критичні випадки; 3 - контроль реалізований на базовому рівні, проте має прогалини в охопленні, автоматизації чи аудиті; 4 - контроль працює системно й перевіряється, але ще не є повністю інтегрованим у процес постійного моніторингу; 5 - контроль є технічно та організаційно зрілим, регулярно перевіряється, журналюється й має підтверджену ефективність. Для досліджуваного практичного кейсу це особливо важливо, оскільки наявність SSL-сертифіката або резервного копіювання сама по собі не означає, що рівень контролю високий: вирішальним є не факт наявності механізму, а ступінь його реальної дієвості.

Щоб уникнути суб’єктивності, задаються словесні інтерпретації для кожного рівня шкали. Наприклад, для наслідку рівень 1 означає мінімальні локальні незручності без впливу на клієнта та без правових наслідків; рівень 2 - обмежений вплив на окремий запис або невелику групу клієнтів; рівень 3 - відчутний вплив на бізнес-процес або на значиму частину даних; рівень 4 - серйозне порушення інтересів клієнтів, що потребує управлінського втручання; рівень 5 - критичні наслідки з масштабною компрометацією, суттєвими юридичними ризиками або тривалою недоступністю сервісу. Такий словесний супровід робить оцінювання прозорішим і зручнішим для повторного використання. У методиці важливо також

визначити межі зон ризику. Загальний ризиковий діапазон поділено на чотири рівні: прийнятний, контрольований, значний і критичний. Прийнятним є ризик, який не потребує негайних капіталовкладень і може бути прийнятий за умови моніторингу. Контрольований ризик потребує планових дій та регулярного перегляду. Значний ризик вимагає пріоритетного впровадження контрзаходів. Критичний ризик потребує негайного реагування, оскільки його реалізація може призвести до масштабного порушення безпеки клієнтських даних. Таким чином, система критеріїв і шкал, яку запропоновано, виконує дві функції. По-перше, вона забезпечує єдину мову для опису ризиків у CRM-системі телекомунікаційного підприємства. По-друге, вона створює основу для формул, за допомогою яких можна обчислити первинний і залишковий ризик. Далі використовується ці критерії для побудови власне методики розрахунку та для оцінювання конкретних ризикових сценаріїв, виявлених під час практики.

Шкали оцінювання імовірності, наслідків і ефективності чинного контролю наведено в таблицях 2.3-2.5.

Таблиця 2.3 - Шкала оцінювання імовірності за компонентами F, V, A

Рівень	**Частота/передумови (F)**	**Експлуатованість (V)**	**Доступність активу (A)**
1	Передумови виникають винятково рідко	Вразливість важко використати без спеціальних умов	Актив практично недоступний для джерела загрози
2	Подія малоймовірна, але можлива за поодиноких умов	Потрібні суттєві зусилля або спеціальні знання	Доступ обмежений і добре сегментований
3	Передумови з’являються періодично	Використання можливе за наявності мотивації або помірних ресурсів	Актив доступний частині користувачів чи каналів
4	Подія може виникати регулярно	Вразливість використовується відносно просто	Актив доступний широкому колу користувачів у процесі роботи

Рівень	Частота/передумови (F)	Експлуатованість (V)	Доступність активу (A)
5	Передумови присутні постійно або майже постійно	Використання дуже просте і майже не потребує додаткових умов	Актив безпосередньо доступний порушнику або масовому колу осіб

Таблиця 2.4 - Шкала оцінювання наслідків

Рівень	Характер наслідку	Інтерпретація для клієнтського контуру
1	Мінімальний	Локальна подія без відчутної шкоди для клієнта та без юридичних наслідків
2	Низький	Вплив на окремі записи або окрему функцію, швидко усувається
3	Помірний	Порушення роботи процесу або шкода для групи клієнтів, потрібне втручання відповідальних осіб
4	Високий	Серйозне порушення інтересів клієнтів, помітний репутаційний та операційний ефект
5	Критичний	Масштабна компрометація або тривала недоступність із високими юридичними та репутаційними наслідками

Таблиця 2.5 - Шкала оцінювання ефективності чинного контролю K

K	Стан контролю	Характеристика
1	Відсутній	Контроль або не впроваджено, або він суто декларативний
2	Слабкий	Контроль частковий, нестабільний, без належного аудиту
3	Базовий	Контроль існує, але має істотні прогалини в охопленні чи перевірці
4	Достатній	Контроль працює системно та періодично перевіряється

K	Стан контролю	Характеристика
5	Зрілий	Контроль інтегрований у процес, автоматизований і підтверджено ефективний

2.5. Запропонована методика розрахунку первинного та залишкового ризику

На основі визначених принципів, моделі активів і системи критеріїв запропоновано послідовну методику оцінювання ризиків інформаційної безпеки клієнтів. Вона складається з семи взаємопов’язаних етапів і може виконуватися як у межах окремого аудиту, так і на регулярній основі, наприклад щоквартально або перед суттєвими змінами в конфігурації CRM-системи. Кожен етап має власний результат: перелік активів, карту процесів, реєстр сценаріїв, оцінки імовірності, оцінки наслідків, інтегральні значення ризику та план реагування. Завдяки такій структурі методика є не одноразовою дослідницькою вправою, а управлінським циклом. Перший етап - визначення меж оцінювання. На цьому етапі встановлюється, які саме підсистеми, бізнес-процеси й категорії даних включаються до аналізу. Для теми даної дипломної роботи межі оцінювання охоплюють CRM-систему, базу даних, модулі автентифікації, засоби резервного копіювання, інтерфейси експорту та ролі користувачів, що працюють із клієнтськими даними. Якщо підприємство застосовує інтеграцію з білінговою системою, її також доцільно включати до контуру оцінювання, оскільки вона оперує критичними фінансовими даними клієнтів.

Другий етап - інвентаризація активів і прив’язка їх до процесів. На цьому кроці для кожного активу визначаються: його тип, власник, місце зберігання, користувачі, бізнес-функція, рівень критичності та взаємозв’язок з іншими активами. Саме на цьому етапі формується розуміння того, які активи є первинними носіями ризику. Наприклад, персональні дані клієнта і фінансова історія можуть зберігатися в одній базі, але використовуються різними ролями в різних процесах. Тому для кожної категорії даних слід зафіксувати контекст використання, а не лише місце зберігання.

Третій етап - формування реєстру ризикових сценаріїв. Для кожного активу й процесу описуються сценарії, у межах яких може бути порушено конфіденційність, цілісність або доступність. Сценарій обов'язково містить джерело загрози, вразливість, актив, процес, потенційний наслідок та чинні засоби контролю. Реєстр повинен бути достатньо деталізованим, але не перевантаженим дрібними варіантами одного й того самого інциденту. На практиці це означає, що сценарії потрібно об'єднувати за логікою джерела загрози та механізму реалізації, але розділяти, якщо відрізняються наслідки або спосіб управління ризиком.

Формування інтегральної оцінки ризику показано на рисунку 2.2.

Рисунок 2.2 - Формування інтегральної оцінки ризику

Четвертий етап - розрахунок інтегральної імовірності. Для цього використовуються три часткові показники: F - частота або регулярність виникнення умов для події; V - експлуатованість вразливості; A - доступність активу для джерела загрози. Кожен показник оцінюється за шкалою від 1 до 5. Інтегральна імовірність P визначається як зважене середнє цих величин. Більша вага надається частоті та експлуатованості, оскільки вони безпосередньо відображають, наскільки реальною є подія в поточних умовах підприємства, тоді як доступність активу є важливою, але дещо похідною характеристикою. П'ятим етапом є оцінювання наслідку. Для цього використовуються п'ять складових: C - вплив на конфіденційність; I - вплив на цілісність; D - вплив на доступність; J -

юридичний вплив; R - репутаційний вплив. Кожна складова оцінюється за шкалою від 1 до 5. З огляду на тему роботи найбільша вага надається конфіденційності, оскільки предметом дослідження є саме захист клієнтських даних. Водночас цілісність і доступність також залишаються важливими складовими, без яких обслуговування абонента втрачає якість і надійність. Юридичний та репутаційний впливи враховуються як окремі множники управлінської значущості. Шостим етапом є визначення первинного ризику. Він показує небезпеку сценарію за умови поточного стану вразливостей, але без поправки на реальну зрілість захисту. Така величина потрібна для того, щоб побачити вихідний масштаб проблеми. Після цього оцінюється ефективність чинного контролю K за шкалою від 1 до 5. На основі первинного ризику і K обчислюється залишковий ризик. Саме залишковий ризик є головним управлінським показником, оскільки демонструє, наскільки небезпека все ще актуальна після урахування тих механізмів захисту, які вже запроваджені на підприємстві. Сьомий етап - пріоритезація та формування плану реагування. Після розрахунку залишкових ризиків усі сценарії впорядковуються у спадному порядку, а для кожного визначається рекомендована стратегія: уникнення, зниження, передання або прийняття. Для контексту телекомунікаційного підприємства найбільш типовою є стратегія зниження через впровадження технічних і організаційних контролів. Проте для окремих критичних сценаріїв, зокрема масового експорту без погодження або невиправдано широких ролей доступу, можлива і стратегія уникнення - тобто повна відмова від певної практики або функції без спеціального контролю.

Формалізовано запропонована методика описується такими співвідношеннями. Інтегральна імовірність, інтегральний наслідок, первинний ризик і залишковий ризик розраховуються за формулами (2.1)–(2.4).

$$P = \text{round}(0{,}35F + 0{,}35V + 0{,}30A), \quad (2.1)$$

$$I\_total = \text{round}(0{,}30C + 0{,}20I + 0{,}20D + 0{,}15J + 0{,}15R), \quad (2.2)$$

$$R\_primary = P \times I\_total, \quad (2.3)$$

$$R\_residual = R\_primary \times (6 - K) / 5. \quad (2.4)$$

Обрання саме такої форми для розрахунку залишкового ризику пояснюється тим, що вона відображає інтуїтивно зрозумілу логіку. Якщо контроль практично відсутній і K = 1, залишковий ризик майже дорівнює первинному. Якщо ж контроль високоефективний і K = 5, залишковий ризик зменшується до однієї п’ятої від первинного. Водночас повне обнулення ризику не допускається, що відповідає реальній практиці інформаційної безпеки: навіть найкращі контрзаходи лише знижують небезпеку, але не усувають її абсолютним чином.

Запропонована методика має кілька важливих переваг. Вона враховує не лише факт існування загрози, а й силу наслідків саме для клієнта. Вона дозволяє відокремити первинну небезпеку від фактичного стану контролю. Вона є придатною для повторного застосування, оскільки працює на основі стабільних шкал і простих формул. Нарешті, вона дає змогу переводити результати аналізу в конкретні пріоритети захисту. У наступному підрозділі демонструється застосування цієї методики до тих сценаріїв, виявлених у межах переддипломної практики.

Інтерпретацію зон залишкового ризику наведено в таблиці 2.6.

Таблиця 2.6 - Інтерпретація зон залишкового ризику

Діапазон R_residual	**Рівень ризику**	**Управлінська дія**
до 5	Прийнятний	Моніторинг, планові перевірки, підтримання поточних заходів
понад 5 до 10	Контрольований	Планове вдосконалення контролів у межах операційної діяльності
понад 10 до 15	Значний	Пріоритетне впровадження коригувальних заходів
понад 15	Критичний	Негайні технічні й організаційні дії, посилений контроль керівництва

2.6. Практичне застосування методики до кейсу досліджуваного підприємства

Щоб перевірити прикладну придатність запропонованої методики, її застосовано до практичного кейсу телекомунікаційного підприємства,

проаналізованого під час проходження переддипломної практики. Для демонстрації обрано шість сценаріїв, що безпосередньо випливають із встановлених під час практики спостережень: слабка автентифікація користувачів CRM, надлишкові права доступу до фінансової інформації, неконтрольований масовий експорт клієнтських даних, недостатньо перевірені резервні копії, несанкціонована модифікація критичних записів та використання історії звернень клієнтів для соціальної інженерії. Усі ці сценарії мають різну природу, тому добре підходять для перевірки універсальності методики.

Перший сценарій - компрометація облікового запису співробітника через слабку автентифікацію. Підставою для його включення стала встановлена під час практики відсутність вимоги щодо обов’язкового використання спеціальних символів у паролях і відсутність блокування облікового запису після серії невдалих спроб входу. За цих умов частота виникнення передумов для події є помірно високою, експлуатованість вразливості також є високою, а доступність активу для порушника залежить від успішності підбору або компрометації пароля. Основний вплив тут спрямований на конфіденційність та частково на цілісність даних, оскільки захоплений обліковий запис може бути використаний і для перегляду, і для зміни записів. Другий сценарій - перегляд фінансової інформації користувачем із надлишковими правами доступу. Під час практики було встановлено, що окремі оператори мали доступ до розділів, які не є необхідними для виконання їх посадових обов’язків. У цьому випадку джерелом загрози виступає внутрішній користувач, а ключовою вразливістю є порушення принципу мінімально необхідних прав. Частота передумов є високою, оскільки оператор щоденно працює в системі. Експлуатованість максимально висока, бо йдеться не про подолання технічного бар’єра, а про зловживання вже наданими повноваженнями. Найвищий вплив стосується конфіденційності та репутації. Третій сценарій - масовий експорт клієнтської бази. Його доцільно розглядати одним із найбільш критичних, оскільки він поєднує високу масштабність наслідків із відсутністю контролю за обсягом вивантаження. Під час практики було встановлено, що експорт у системі можливий, проте дії такого типу не супроводжуються достатнім

контролем і не обмежуються пороговими значеннями. У випадку реалізації цього сценарію порушник може отримати не один клієнтський запис, а цілий масив персональних, контактних і фінансових відомостей. Саме тому для цього сценарію наслідок за критеріями конфіденційності, юридичного впливу та репутації є одним із найвищих у всьому реєстрі. Четвертий сценарій пов’язаний із резервним копіюванням. Хоча автоматичне створення резервних копій на підприємстві реалізоване, фактична перевірка відновлення проводиться нерегулярно. Це означає, що наявність копії ще не гарантує її працездатності та актуальності. У моделі ризику розглядається інцидент, за якого після технічного збою або логічного пошкодження бази даних підприємство не може вчасно відновити коректний стан клієнтської інформації. У цьому випадку домінуючим є вплив на доступність і цілісність, але другорядно виникають і репутаційні наслідки, оскільки клієнти стикаються з неможливістю отримати якісне обслуговування.

П’ятий сценарій - несанкціонована модифікація критичних записів. Він може реалізуватися як через компрометацію облікового запису, так і через свідомі дії внутрішнього користувача з надлишковими правами. Його характерною ознакою є не витік інформації, а зміна даних: фінансових нарахувань, статусу послуги, параметрів підключення, умов договору або історії взаємодії з клієнтом. З точки зору ризик-аналізу цей сценарій є особливо небезпечним тим, що наслідки можуть бути виявлені не відразу. Це збільшує бізнесову шкоду, оскільки помилки накопичуються й пізніше породжують конфлікти з абонентами. Шостий сценарій - використання історії звернень або контактних даних клієнтів для соціальної інженерії. На перший погляд, такий сценарій є менш очевидним, ніж масовий експорт або злам облікового запису, але він важливий, оскільки історія звернень у підтримку часто містить непрямі ознаки поведінки клієнта, параметри послуг, шаблони комунікації та інші деталі, які можуть бути використані для переконливого шахрайського контакту. У цьому випадку шкода для підприємства може проявлятися не лише як витік даних, а і як втрата довіри до каналів комунікації та зростання кількості скарг.

Для кожного зі сценаріїв виконується послідовне оцінювання за запропонованими шкалами. Спочатку встановлюються значення F, V і A, далі - C, I, D, J і R, потім оцінюється K. Отримані значення не претендують на абсолютну математичну точність, але є достатньо обґрунтованими для управлінського аналізу, оскільки спираються на факти, встановлені під час практики, а також на логіку функціонування досліджуваної CRM-системи. Завдяки цьому отримується не просто опис слабких місць, а ранжований перелік ризиків з чітким поясненням їхньої пріоритетності. За результатами обчислень найвищі залишкові ризики характерні для трьох сценаріїв: масового експорту даних, надлишкових прав доступу та компрометації облікового запису співробітника. Це закономірно, оскільки всі три сценарії поєднують відносно високу ймовірність із високим впливом на конфіденційність і репутацію. Сценарій із резервним копіюванням також демонструє суттєвий рівень залишкового ризику, але його профіль дещо інший: він сильніше впливає на доступність і цілісність, ніж на конфіденційність. Сценарій модифікації критичних записів посідає проміжне місце, тоді як використання історії звернень для соціальної інженерії має дещо нижчий, але все ще значущий показник. Перевага запропонованої методики на цьому етапі полягає в тому, що вона не лише виявляє проблеми, а й показує, за рахунок яких саме чинників формується підсумковий ризик. Наприклад, для масового експорту ключовим чинником є масштаб наслідку та низька зрілість контролю. Для надлишкових прав - дуже висока доступність активу для внутрішнього користувача. Для резервного копіювання - не стільки ймовірність події, скільки серйозність наслідків у разі збою та недостатня перевіреність процесу відновлення. Це дозволяє надалі призначати не універсальні, а адресні контрзаходи. Важливим результатом апробації є також те, що методика дозволяє порівнювати різні класи ризиків в одній системі координат. У межах традиційного описового аналізу порушення автентифікації, зловживання доступом і відмова резервного відновлення часто розглядаються як непорівнювані проблеми, оскільки належать до різних функціональних сфер безпеки. Запропонована ж система шкал і формул дозволяє оцінити їх за єдиним критерієм і побачити, який із ризиків потребує

першочергових дій саме з позиції захисту клієнта. це є однією з головних практичних переваг розробленої методики.

Результати оцінювання сценаріїв, деталізацію компонентів і узагальнений реєстр ризиків подано в таблицях 2.7-2.9.

Таблиця 2.7 - Результати оцінювання сценаріїв за запропонованою методикою

Сценарій	**P**	**I_total**	**K**	**R_primary**	**R_residual**	**Рівень**	**Пріоритет**
Компрометація облікового запису через слабку автентифікацію	4	4	2	16	12.8	Значний	Високий
Надлишкові права доступу до фінансових даних	5	4	2	20	16.0	Критичний	Високий
Масовий експорт клієнтської бази без контролю	4	4	1	16	16.0	Критичний	Високий
Невдале відновлення з резервної копії після збою	3	3	2	9	7.2	Контрольований	Середній
Несанкціонована модифікація критичних записів	4	4	2	16	12.8	Значний	Високий
Соціальна інженерія на основі історії звернень	3	3	2	9	7.2	Контрольований	Середній

Таблиця 2.8 - Деталізація компонентів оцінювання для вибраних сценаріїв

Сценарій	F	V	A	C	I	D	J	R	K
Компрометація облікового запису через слабку автентифікацію	4	4	3	5	3	2	4	4	2
Надлишкові права доступу до фінансових даних	5	5	5	5	3	2	4	5	2
Масовий експорт клієнтської бази без контролю	4	5	4	5	3	2	5	5	1
Невдале відновлення з резервної копії після збою	3	3	3	2	4	5	3	4	2
Несанкціонована модифікація критичних записів	3	4	4	3	5	3	4	4	2
Соціальна інженерія на основі історії звернень	3	3	4	4	2	2	3	4	2

Таблиця 2.9 - Узагальнений реєстр ризиків та рекомендовані стратегії реагування

Сценарій	Домінуючий вплив	Стратегія реагування	Коротке обґрунтування
Компрометація облікового запису	Конфіденційність, цілісність	Зниження	Ризик формується слабкою автентифікацією та недостатньою стійкістю доступу

Сценарій	Домінуючий вплив	Стратегія реагування	Коротке обґрунтування
Надлишкові права доступу	Конфіденційність, репутація	Уникнення/зниження	Необхідне перегрупування ролей і вилучення зайвих повноважень
Масовий експорт даних	Конфіденційність, юридичний вплив	Негайне зниження	Високий масштаб наслідків при слабкому контролі
Відновлення з резервної копії	Доступність, цілісність	Зниження	Потрібна регулярна перевірка працездатності backup/restore
Несанкціонована модифікація записів	Цілісність, репутація	Зниження	Потрібні превентивні та детективні контролі змін
Соціальна інженерія	Конфіденційність, репутація	Зниження	Важливі обмеження видимості й навчання персоналу

2.7. Пріоритезація контрзаходів та оптимізація управління ризиками

Після одержання значень залишкового ризику постає питання практичного використання результатів. Якщо методика завершується лише таблицею балів, її управлінська цінність буде обмеженою. Тому завершальним кроком запропоновано процедуру пріоритезації контрзаходів. Її суть полягає в тому, що кожному ризиковому сценарію ставиться у відповідність один або кілька заходів зниження ризику, причому пріоритетність їх впровадження визначається не лише рівнем залишкового ризику, а й очікуваною ефективністю, складністю реалізації та організаційною доцільністю. Для сценарію компрометації облікового запису ключовими контрзаходами є посилення політики паролів, введення двофакторної автентифікації для користувачів із розширеними правами, блокування після серії невдалих спроб входу, моніторинг аномальної активності та перегляд сесій доступу. Ці заходи безпосередньо знижують показники експлуатованості й доступності активу для порушника. Їхня перевага полягає в тому, що вони відносно швидко впроваджуються і мають чіткий ефект на зниження ризику. Саме тому для даного сценарію доцільно віднести їх до короткострокових пріоритетів.

Для сценарію надлишкових прав доступу основним напрямом оптимізації є впровадження формалізованої рольової моделі доступу. Запропоновано визначити стандартні профілі ролей, затвердити матрицю «роль - ресурс - дозволена дія», розмежувати доступ до фінансових і технічних даних, запровадити процедуру погодження розширених привілеїв та виконувати регулярний перегляд фактичних прав користувачів. Додатково слід запровадити журналювання операцій читання критичних розділів і вибірковий аудит дій співробітників. Саме ці заходи знижують ризик зловживання штатними повноваженнями. Для сценарію масового експорту інформації першочерговим доцільно вважати впровадження окремого контуру контролю вивантаження. Йдеться про обмеження обсягу експорту за замовчуванням, запровадження погодження великих вивантажень, журналювання кожної експортної операції, автоматичні сповіщення про аномальні масиви даних, маркування критичних наборів даних та, за можливості, прив’язку експорту до конкретної службової підстави. У стратегічній перспективі такі функції можуть бути доповнені DLP-підходами, однак навіть базовий контроль уже суттєво зменшує залишковий ризик. Для ризику, пов’язаного з резервним копіюванням, оптимізація повинна бути спрямована не стільки на збільшення кількості копій, скільки на підвищення довіри до процедури відновлення. Рекомендується ввести календарний графік тестових відновлень, визначити нормативний показник часу відновлення, фіксувати результати тестів у журналі, перевіряти цілісність резервних копій та розмежувати права на створення, зберігання й відновлення. Такий підхід зменшує невизначеність щодо фактичної працездатності backup-механізмів і переводить їх із суто технічної функції у контрольований процес забезпечення доступності даних.

Ризик несанкціонованої модифікації записів доцільно знижувати за рахунок поєднання двох груп заходів. Перша група - це запобіжні контролі: розмежування прав, сегментація критичних функцій, підтвердження змін для окремих категорій полів, багатофакторна автентифікація, обмеження адміністративних сесій. Друга група - це детективні контролі: журнал змін, історія версій записів, сповіщення про модифікацію критичних полів, регулярне звіряння фінансових і договорних даних.

Саме комбінація попередження і виявлення дозволяє суттєво зменшити залишковий ризик за цим сценарієм. Для сценарію соціальної інженерії на основі історії звернень необхідні насамперед організаційні заходи. До них належать внутрішнє навчання персоналу, обмеження видимості чутливих фрагментів історії комунікацій, стандартизація сценаріїв роботи з клієнтом, правила використання контактної інформації, а також інформування самих абонентів щодо перевірки офіційних каналів зв’язку. Хоча цей ризик часто сприймається як другорядний, він має виражений репутаційний потенціал, а тому не повинен ігноруватися в загальній системі управління ризиками. Усі заходи доцільно розділити на короткострокові, середньострокові та стратегічні. До короткострокових належать ті, що можуть бути впроваджені без перебудови архітектури системи: налаштування блокування, посилення політики паролів, базове журналювання, обмеження ролей, графік тестового відновлення. До середньострокових - інтеграція 2FA, механізми погодження експорту, формалізація матриці доступу, аудит прав і навчання персоналу. До стратегічних - впровадження централізованої системи моніторингу, DLP-компонентів, автоматизація контролю аномальної активності, розширення функцій внутрішнього аудиту та побудова постійного процесу управління ризиками.

Цикл управління залишковим ризиком після впровадження контролів показано на рисунку 2.3.

Рисунок 2.3 - Цикл управління залишковим ризиком після впровадження контролів

Отже, запропонована методика не завершується числовою оцінкою, а природно переходить у модель оптимізації. Вона дозволяє побачити, які саме контрзаходи здатні найбільш ефективно знизити ризик, у якому порядку їх доцільно впроваджувати та які слабкі місця підприємства потребують негайного управлінського втручання. така орієнтація на практичну реалізацію є ключовою перевагою методики, оскільки саме вона перетворює результати дослідження на інструмент покращення реального стану захисту клієнтських даних.

Пріоритетні заходи оптимізації та дорожню карту впровадження методики наведено в таблицях 2.10-2.11.

Таблиця 2.10 - Пріоритетні заходи оптимізації за результатами оцінювання ризиків

Напрям	**Конкретний захід**	**Який ризик знижує**	**Горизонт**	**Очікуваний ефект**
Автентифікація	2FA, блокування після 5 невдалих спроб, посилення паролів	Компрометація акаунтів	Короткостроковий	Зменшення P та підвищення K

Напрям	Конкретний захід	Який ризик знижує	Горизонт	Очікуваний ефект
Розмежування доступу	Матриця ролей, регулярний review прав	Надлишкові права, модифікація записів	Коротко-/середньостроковий	Зменшення A та масштабу наслідків
Контроль експорту	Ліміти, погодження, журналювання, сповіщення	Масовий експорт	Коротко-/середньостроковий	Зниження K-пов'язаного дефіциту контролю
Backup/restore	Графік тестових відновлень, контроль цілісності копій	Втрата доступності й цілісності	Короткостроковий	Підвищення K та скорочення часу відновлення
Аудит змін	Журнали, версійність, сповіщення про критичні поля	Несанкціонована модифікація	Середньостроковий	Поліпшення виявлення та стримування
Організаційні заходи	Навчання персоналу, внутрішні регламенти, контроль інцидентів	Соціальна інженерія, людський фактор	Постійний	Зниження помилок та підвищення дисципліни

Таблиця 2.11 - Рекомендована дорожня карта впровадження методики

Етап	Зміст робіт	Відповідальні ролі	Результат
1. Підготовка	Інвентаризація активів, формування реєстру ролей і процесів	Керівник IT, адміністратор, ІБ-відповідальний	Паспорт активів та межі оцінювання
2. Оцінювання	Заповнення шкал, розрахунок P, I_total, R_primary, R_residual	Робоча група з ризик-аналізу	Реєстр ризиків із ранжуванням
3. Планування	Вибір пріоритетних заходів, бюджетування, визначення KPI	Керівництво, IT, ІБ	План зниження ризиків
4. Впровадження	Технічні налаштування та організаційні регламенти	IT-відділ, власники процесів	Посилені контролі та регламенти

Етап	Зміст робіт	Відповідальні ролі	Результат
5. Перевірка	Повторна оцінка, аудит прав, тестові відновлення, аналіз журналів	ІБ-відповідальний, аудит	Оновлені показники залишкового ризику

2.8. Організація повторного оцінювання та показники ефективності методики

Розроблена методика буде справді корисною для телекомунікаційного підприємства лише тоді, коли її застосування не обмежиться одноразовим заповненням реєстру ризиків. Ризиковий профіль клієнтського контуру є динамічним: змінюються тарифи, бізнес-процеси, ролі користувачів, канали інтеграції, вимоги регулювання та самі способи зловживань. Саме тому після первинної апробації методики підприємство повинно перейти до циклічного режиму повторного оцінювання. Найбільш доцільним є поєднання планового та подієвого підходів: планове оцінювання проводиться через фіксовані інтервали часу, а позапланове - після змін архітектури системи, інцидентів, аудиту або перегляду ролей. Циклічність оцінювання дає змогу вирішити кілька важливих завдань. По-перше, вона дозволяє відстежувати реальну динаміку залишкового ризику після впровадження контрзаходів. По-друге, вона виявляє нові вразливості, які могли не існувати на момент першого аналізу. По-третє, вона забезпечує прив’язку ризик-аналізу до управління змінами: кожне суттєве оновлення CRM, розширення експорту, інтеграція нового сервісу або делегування доступів повинні автоматично запускати перегляд відповідних сценаріїв. Без цього навіть добре побудована методика швидко перетворюється на статичний документ, який не відображає реальний стан безпеки. Для практичного впровадження запропоновано використовувати набір контрольних показників ефективності. До них належать: частка переглянутих ролей доступу за звітний період; кількість сценаріїв із критичним або значним залишковим ризиком; середній час виявлення підозрілої дії користувача; відсоток успішно виконаних тестових відновлень; кількість невдалих спроб входу, які були коректно заблоковані; кількість експортних

операцій, що пройшли процедуру погодження; частка співробітників, які пройшли навчання з безпеки; кількість інцидентів, за якими було оновлено реєстр ризиків. Саме такі показники дозволяють оцінювати не лише рівень небезпеки, а й результативність процесу управління ризиками. На рівні організації робіт доцільно закріпити відповідальність за виконання методики між кількома ролями. Власники бізнес-процесів повинні описувати зміни у процесах та підтверджувати доцільність доступів. IT-підрозділ відповідає за технічну реалізацію контролів і надання фактичних даних для оцінювання. Відповідальний за інформаційну безпеку або уповноважена робоча група координує перегляд сценаріїв, розрахунок показників і підготовку звіту для керівництва. Саме розподіл відповідальності перетворює методику з аналітичної схеми на сталий управлінський процес.

Показники контролю ефективності повторного оцінювання ризиків наведено в таблиці 2.12.

Таблиця 2.12 - Показники контролю ефективності повторного оцінювання ризиків

Показник	**Зміст**	**Періодичність**	**Управлінське значення**
Частка переглянутих ролей доступу	Відношення фактично переглянутих профілів до всіх активних ролей	Щоквартально	Показує дисципліну контролю принципу мінімально необхідних прав
Середній залишковий ризик критичних сценаріїв	Середнє значення R_residual для сценаріїв із високою пріоритетністю	Щоквартально	Дозволяє бачити загальну тенденцію зниження або зростання небезпеки
Успішність тестового відновлення	Частка успішних процедур відновлення з резервних копій	Щомісячно/щоквартально	Характеризує реальну готовність до інцидентів доступності
Частка погоджених експортів	Відсоток великих вивантажень, що пройшли формальне погодження	Щомісячно	Показує керованість ризику масового копіювання

Показник	Зміст	Періодичність	Управлінське значення
Рівень навчання персоналу	Частка співробітників, які пройшли актуальне навчання з ІБ	Щопівроку	Відображає стійкість до помилок та соціальної інженерії

Наявність таких показників дозволяє замкнути контур управління ризиками: оцінювання - впровадження заходів - вимірювання результату - повторне оцінювання. У цьому полягає практична завершеність методики, яку запропоновано в межах дипломної роботи. Вона не тільки описує, як визначити рівень ризику, а й задає механізм перевірки, чи справді впроваджені рішення покращили стан захисту клієнтських даних. Отже, методика оцінювання ризиків інформаційної безпеки клієнтів телекомунікаційного підприємства повинна працювати як безперервний цикл. Саме за такої умови результати аналізу залишаються актуальними, а заходи захисту - економічно та організаційно обґрунтованими.

Висновки до розділу 2

У другому розділі розроблено методику оцінювання ризиків інформаційної безпеки клієнтів телекомунікаційного підприємства, що ґрунтується на поєднанні процесного, рольового та напівкількісного підходів. На відміну від загального опису загроз, запропонована методика дозволяє системно пов’язати активи, процеси, ролі, вразливості, наслідки та чинні засоби контролю в єдину модель управління ризиками. У межах розділу було сформовано модель активів і процесів обробки клієнтських даних, визначено підхід до ідентифікації загроз і вразливостей, побудовано шкали оцінювання імовірності, наслідку та ефективності контролю, а також запропоновано формули для обчислення первинного й залишкового ризику. Це дозволило перейти від якісних спостережень, отриманих під час практики, до формалізованої процедури ранжування ризикових сценаріїв.

Практичне застосування методики до кейсу досліджуваного підприємства показало, що найвищий рівень небезпеки характерний для сценаріїв масового

експорту клієнтських даних, надлишкових прав доступу та компрометації облікових записів. Водночас ризики, пов’язані з резервним копіюванням, несанкціонованою модифікацією записів і соціальною інженерією, також мають значущий вплив і потребують цілеспрямованого управління. Отримані результати створюють підґрунтя для наступного етапу дипломної роботи - практичного вдосконалення механізмів управління ризиками та обґрунтування конкретних технічних і організаційних заходів, здатних знизити залишковий ризик для клієнтських даних у телекомунікаційному підприємстві.

РОЗДІЛ 3
ПРАКТИЧНА РЕАЛІЗАЦІЯ ЗНИЖЕННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КЛІЄНТІВ ТЕЛЕКОМУНІКАЦІЙНОГО ПІДПРИЄМСТВА

3.1. Обґрунтування практичного рішення для зниження ризиків

У третьому розділі виконується практичне розв’язання проблематики, сформованої у попередніх частинах роботи. У першому розділі було визначено, що найбільш небезпечними для клієнтських даних телекомунікаційного підприємства є слабка автентифікація, надлишкові права доступу, неконтрольований масовий експорт, нерегулярна перевірка резервного відновлення, недостатній аудит змін і людський фактор. У другому розділі ці проблеми були переведені у формалізовані ризикові сценарії та оцінені за напівкількісною методикою. Тому логічним продовженням є не повторний опис загроз, а створення практичного механізму, який дозволяє підприємству керовано знижувати залишковий ризик. Практичне рішення доцільно розглядати як допоміжний програмний модуль оцінювання та контролю ризиків клієнтського контуру CRM-системи. Такий модуль не замінює саму CRM і не виконує дії з реальними персональними даними клієнтів. Його призначення полягає у веденні реєстру ризиків, автоматизованому розрахунку первинного та залишкового ризику, перевірці відповідності ролей принципу мінімально необхідних прав, контролі небезпечних операцій експорту, відстеженні стану backup/restore та формуванні звітних показників для відповідального за інформаційну безпеку.

Вибір саме такого рішення пояснюється тим, що виявлені проблеми мають змішаний характер. Наприклад, слабка парольна політика усувається технічними налаштуваннями автентифікації, але її результативність потрібно контролювати через кількість невдалих входів і заблокованих акаунтів. Надлишкові права доступу вирішуються матрицею ролей, але ця матриця має регулярно порівнюватися з фактичними правами користувачів. Масовий експорт знижується лімітами, погодженням і журналюванням, однак сам факт експорту має

перетворюватися на подію контролю. Тобто потрібна не одна окрема рекомендація, а зв’язана система правил і розрахунків.

У межах розділу практичне рішення подається у вигляді прототипу програмного модуля. Для демонстрації використано мову Python, оскільки вона зручна для швидкої реалізації аналітичних моделей, роботи зі структурованими даними та формування звітів. При цьому логіка рішення не прив’язана жорстко до Python: ті самі класи та алгоритми можуть бути перенесені у веб-модуль CRM, реалізовані як окремий сервіс у середовищі .NET або інтегровані з базою даних через API. Головним є не конкретна мова програмування, а структура даних, алгоритм і правила контролю.

Розроблений прототип вирішує п’ять прикладних задач, кожна з яких безпосередньо пов’язана з ризиками, визначеними у попередніх розділах:

1) автоматизує розрахунок ризику за формулами, запропонованими у другому розділі, що зменшує ймовірність помилок ручного оцінювання;

2) виконує повторний розрахунок після впровадження контрзаходів і дає змогу порівняти стан ризику «до» та «після»;

3) формалізує матрицю доступу та допомагає виявляти зайві повноваження користувачів CRM-системи;

4) задає правила контролю експорту, завдяки яким звичайний службовий звіт відокремлюється від небезпечного масового вивантаження клієнтських даних;

5) забезпечує базову перевірку стану резервних копій і тестового відновлення, що важливо для підтримання доступності клієнтської інформації.

Важливо, що запропоноване рішення відповідає обмеженням дипломної роботи. Воно не потребує доступу до реальної клієнтської бази, не містить механізмів атаки або обходу захисту, а працює з узагальненими ризиковими сценаріями. Це дозволяє продемонструвати практичну реалізацію без порушення конфіденційності клієнтів і без ризику впливу на виробничу CRM-систему. Усі

приклади даних у розділі є модельними та побудовані на основі проблем, описаних у попередніх розділах.

3.2. Функціональні та нефункціональні вимоги до модуля

Перед програмною реалізацією необхідно визначити вимоги до модуля, оскільки саме вони показують, які практичні задачі має закривати рішення. Основною функціональною вимогою є підтримка реєстру ризикових сценаріїв. Кожний сценарій повинен містити код, назву, актив, джерело загрози, вразливість, бізнес-процес, поточні значення критеріїв F, V, A, C, I, D, J, R, K, перелік запропонованих контролів і результат розрахунку. Така структура прямо продовжує методику другого розділу та не вимагає створення нової системи оцінювання.

Другою функціональною вимогою є автоматизація обчислень. У ручному режимі ризики можна розраховувати в таблиці, але при регулярному повторному оцінюванні це створює ризик помилок і неузгодженості. Програмний модуль повинен самостійно перевіряти, чи належать оцінки до діапазону від 1 до 5, виконувати округлення за обраним правилом, визначати рівень ризику та сортувати сценарії за критичністю. Завдяки цьому різні оцінюваннвиконуєтьсяться однаково, а результати стають відтворюваними. Третьою вимогою є підтримка контролю доступу. Модуль має зберігати еталонну матрицю дозволів для основних ролей: оператора, працівника підтримки, бухгалтера, технічного спеціаліста, адміністратора, керівника та аудитора. Для кожної ролі задаються допустимі операції над категоріями даних: перегляд, редагування, експорт, видалення або адміністрування. Порівняння еталонної матриці з фактичними правами дозволяє виявляти надлишкові доступи, які у попередніх розділах були визначені як один із найнебезпечніших ризиків.

Четверта вимога стосується контролю експорту. Проблема масового експорту полягає в тому, що з технічної точки зору він може виглядати як легітимна функція формування звіту. Тому модуль має класифікувати експорт за кількістю записів, чутливістю даних і наявністю погодження. Невеликі службові вивантаження можуть дозволятися автоматично, вивантаження чутливих або

значних масивів повинні вимагати погодження, а дуже великі операції мають блокуватися і створювати подію для аудиту. П’ята вимога пов’язана з резервним копіюванням. Модуль має оцінювати не сам факт існування backup-файлу, а готовність процесу відновлення: актуальність копії, правильність контрольної суми, давність останнього тестового відновлення та орієнтовний час відновлення. Саме такий підхід усуває слабкість, описану в попередніх розділах, де резервні копії створювалися автоматично, але процедура відновлення перевірялася нерегулярно. До нефункціональних вимог належать простота інтеграції, прозорість логіки, відсутність потреби в обробці реальних персональних даних, можливість повторного застосування, зрозумілість результатів для керівництва та відповідність принципу мінімізації даних. Модуль не повинен дублювати CRM або зберігати надмірні відомості про клієнтів. Йому достатньо працювати з технічними метаданими, ролями, ризиковими сценаріями та агрегованими показниками.

Функціональні вимоги до модуля та відповідність виявлених проблем практичним компонентам рішення наведено в таблицях 3.1-3.2.

Таблиця 3.1 - Функціональні вимоги до практичного модуля управління ризиками

Вимога	**Зміст реалізації**	**Практичне значення**
Реєстр ризиків	Зберігання сценаріїв, активів, джерел загроз, вразливостей і контролів	Дозволяє підтримувати єдину базу ризиків
Розрахунок ризику	Автоматичне обчислення P, I_total, R_primary, R_residual	Зменшує помилки ручного розрахунку
Матриця доступу	Порівняння еталонних і фактичних прав ролей	Виявляє надлишкові повноваження
Контроль експорту	Ліміти, погодження, журналювання великих вивантажень	Знижує ризик масового витоку
Backup/restore	Перевірка актуальності, checksum і тестового відновлення	Підтверджує готовність до відновлення
Звітність	Формування таблиць до/після та KPI	Підтримує управлінські рішення

Таблиця 3.2 - Відповідність виявлених проблем практичним компонентам рішення

Проблема	**Компонент рішення**	**Контрзахід**	**Показники, що змінюються**
Слабка автентифікація	AuthenticationControl	Парольна політика, блокування, 2FA	F, V, K
Надлишкові права	AccessMatrixValidator	RBAC, регулярний review ролей	A, K
Масовий експорт	ExportControlService	Пороги експорту, погодження, аудит	V, A, K
Нерегулярне відновлення	BackupControlService	Checksum, тестове відновлення, RTO/RPO	D, K
Модифікація записів	AccessMatrixValidator + аудит змін	Версійність, журнал змін, подвійний контроль	A, K
Соціальна інженерія	Регламенти + навчання	Мінімізація видимості, інструктаж персоналу	F, A, K

3.3. Архітектура практичного рішення та модель даних

Архітектура запропонованого рішення побудована за модульним принципом. Центральним компонентом є RiskAssessmentEngine, який виконує розрахунок імовірності, наслідку, первинного та залишкового ризику. Навколо нього розміщені спеціалізовані модулі контролю: AuthenticationControl, AccessMatrixValidator, ExportControlService та BackupControlService. Кожний з них відповідає за конкретну групу проблем, визначених у практичному кейсі підприємства. Такий поділ є важливим, оскільки різні ризики мають різну природу. Ризик компрометації облікового запису пов’язаний із політикою паролів, блокуванням і багатофакторною автентифікацією. Ризик надлишкових прав пов’язаний із моделлю ролей і повноважень. Ризик масового експорту пов’язаний із поведінкою користувача та обсягом вивантаження. Ризик невдалого відновлення пов’язаний із життєвим циклом резервних копій. Об’єднання цих задач у один великий нерозділений блок ускладнило б підтримку системи, тому в реалізації застосовано окремі класи. Модель даних базується на сутності RiskScenario. Вона

описує сценарій як комбінацію активу, джерела загрози, вразливості, процесу, числових оцінок та наявних контролів. Така сутність є універсальною: через неї можна описати як зовнішню атаку на обліковий запис, так і внутрішнє зловживання доступом або помилку резервного відновлення. Результатом обробки сценарію є сутність RiskResult, у якій зберігаються розраховані показники і рівень ризику. Окремою частиною моделі є матриця доступу. Вона подається як словник, де ключем першого рівня є роль користувача, ключем другого рівня - об’єкт або категорія даних, а значенням - множина дозволених операцій. Такий формат зручний для програмної перевірки і водночас легко переноситься у табличний вигляд для дипломної роботи або внутрішнього регламенту підприємства. Для контролю експорту використовується сутність ExportRequest. Вона не містить реальних даних клієнтів, а лише описує операцію: користувач, роль, кількість записів, наявність ідентифікаційних або фінансових даних, а також факт погодження. Це відповідає принципу мінімізації даних: система може приймати рішення про небезпечність операції без перегляду змісту клієнтських записів. Для резервного копіювання використовується сутність BackupCheck. Вона включає ідентифікатор копії, давність створення, результат перевірки контрольної суми, дату останнього тестового відновлення та очікуваний час відновлення. На основі цих параметрів модуль визначає, чи backup-процес перебуває в робочому стані, чи потребує негайної перевірки.

Узагальнену класову модель програмного модуля подано на рисунку 3.1.

Рисунок 3.1 - Узагальнена класова модель програмного модуля

Класова модель на рисунку 3.1 доповнюється таблицею 3.3, яка пояснює не лише назви класів, а й їхню практичну роль у процесі оцінювання ризиків. Така таблиця потрібна для того, щоб показати, який компонент відповідає за введення сценарію, розрахунок показників, перевірку доступів, контроль експорту та оцінку резервного копіювання.

Таблиця 3.3 - Основні класи програмного рішення

Клас або компонент	**Що описує або перевіряє**	**Практична роль у модулі оцінювання ризиків**
RiskScenario	Один ризиковий сценарій: актив, джерело загрози, вразливість, процес, оцінки F, V, A, C, I, D, J, R, K.	Є основною вхідною одиницею оцінювання; пов’язує конкретний ризик із активом, процесом і числовими критеріями.
RiskResult	Підсумок розрахунку: P, I_total, R_primary, R_residual, рівень ризику та рекомендація.	Перетворює набір оцінок у зрозумілий управлінський результат, який можна включити до звіту або реєстру ризиків.
RiskAssessmentEngine	Алгоритмічне ядро для розрахунку імовірності,	Забезпечує однакове застосування формул для всіх сценаріїв і усуває

	наслідку, первинного та залишкового ризику.	неоднозначність ручних обчислень.
AuthenticationControl	Перевіряє вимоги до пароля, кількість невдалих входів і потребу в блокуванні облікового запису.	Знижує ризик компрометації акаунтів через слабку автентифікацію та повторні спроби входу.
AccessMatrixValidator	Порівнює фактичні права користувача з еталонною матрицею ролей.	Виявляє надлишкові повноваження, зокрема доступ до фінансових або персональних даних без службової потреби.
ExportControlService	Оцінює операцію експорту за кількістю записів, чутливістю даних і наявністю погодження.	Допомагає запобігти масовому витоку клієнтської бази через неконтрольоване вивантаження інформації.
BackupControlService	Перевіряє актуальність резервної копії, контрольну суму, дату тестового відновлення та очікуваний час відновлення.	Показує, чи може підприємство реально відновити клієнтські дані після збою, а не лише формально має backup-файл.

3.4. Алгоритм роботи модуля оцінювання ризиків

На вхід алгоритму надходять відомості про інформаційні активи, ролі користувачів, ризикові сценарії, наявні контролі та експертні оцінки за шкалами методики. Спочатку модуль перевіряє повноту вхідних даних і коректність діапазонів оцінювання. Якщо дані неповні або виходять за допустимі межі, формується повідомлення про помилку; якщо дані коректні, виконується розрахунок імовірності, наслідку, первинного та залишкового ризику.

Після визначення рівня ризику модуль зіставляє сценарій із типом вразливості, добирає відповідні контрзаходи, виконує повторний розрахунок після їх упровадження та формує вихідні результати: реєстр ризиків, пріоритет реагування, рекомендовані контролі й показники ефективності.

Алгоритм роботи модуля, поданий на рисунку 3.2, складається з послідовних етапів, які відповідають логіці методики другого розділу, але переведені у програмну форму. На першому етапі завантажуються вхідні дані: реєстр активів, перелік ролей, ризикові сценарії, чинні контролі та порогові правила. У демонстраційній реалізації ці дані задаються безпосередньо у коді, але в реальній

системі вони можуть зберігатися у JSON-файлі, CSV-таблиці або в базі даних. На другому етапі виконується валідація. Вона потрібна для того, щоб у розрахунок не потрапили некоректні значення. Усі оцінки F, V, A, C, I, D, J, R, K повинні перебувати в діапазоні від 1 до 5. Якщо значення виходить за межі шкали, модуль повинен зупинити розрахунок і показати помилку. Це важливо для академічної коректності методики, оскільки використання шкал має бути однаковим для всіх сценаріїв. На третьому етапі обчислюється інтегральна імовірність P. Для цього використовується зважене середнє частоти, експлуатованості та доступності активу. На четвертому етапі обчислюється інтегральний наслідок I_total. Він враховує конфіденційність, цілісність, доступність, юридичний і репутаційний вплив. На п’ятому етапі обчислюється первинний ризик, а далі - залишковий ризик з урахуванням зрілості контролю K. На шостому етапі модуль інтерпретує результат. Для кожного сценарію визначається зона ризику: прийнятний, контрольований, значний або критичний. Саме цей етап перетворює числову оцінку на управлінський висновок. Якщо ризик критичний, він потребує негайного реагування. Якщо значний - пріоритетного впровадження контрзаходів. Якщо контрольований - планового вдосконалення. Якщо прийнятний - моніторингу та підтримання чинних заходів. На сьомому етапі виконується повторний розрахунок після впровадження контрзаходів. Для цього задається оновлений набір параметрів: зменшені значення F, V або A, якщо знижено ймовірність події, а також підвищене значення K, якщо контроль став ефективнішим. Порівняння двох наборів результатів дозволяє кількісно показати ефективність запропонованого рішення. Останній етап - формування звіту. У звіті відображається перелік ризиків, початкові та оновлені значення, різниця між ними, відсоток зниження і рекомендований режим подальшого контролю. Завдяки цьому програмний модуль може бути використаний не лише як навчальний приклад, а і як основа для внутрішнього аудиторського інструменту телекомунікаційного підприємства.

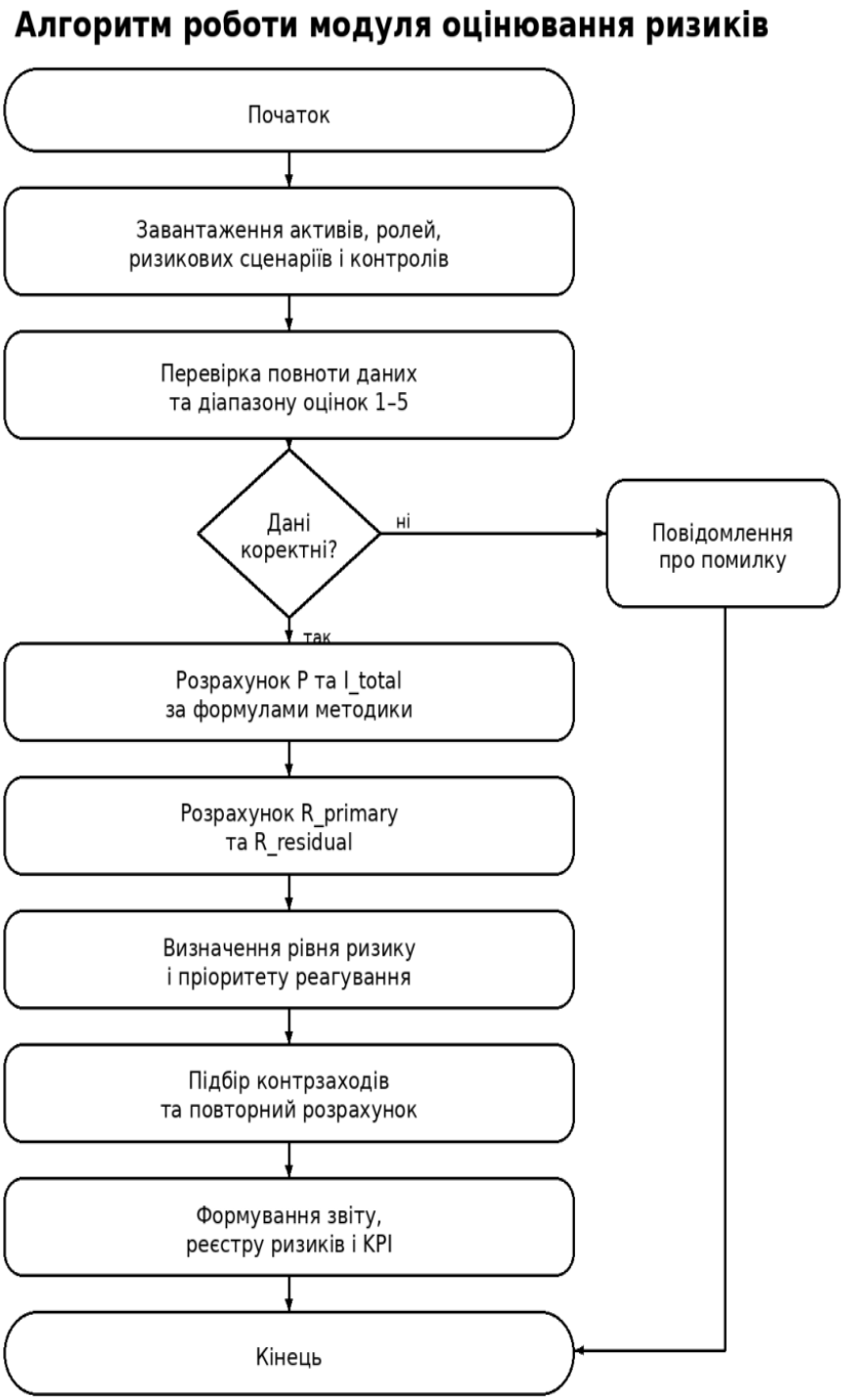

Рисунок 3.2 - Алгоритм роботи модуля оцінювання ризиків

$$P = \text{round}(0{,}35F + 0{,}35V + 0{,}30A)$$

(3.1)

$$I\_total = \text{round}(0{,}30C + 0{,}20I + 0{,}20D + 0{,}15J + 0{,}15R)$$

(3.2)

$$R_{primary} = P \times I_{total} \quad (3.3)$$

$$R_{residual} = R_{primary} \times (6 - K) / 5 \quad (3.4)$$

$$E = ((R_{before} - R_{after}) / R_{before}) \times 100\% \quad (3.5)$$

Послідовність етапів алгоритму роботи модуля наведено в таблиці 3.4.

Таблиця 3.4 - Послідовність програмного алгоритму оцінювання

Етап	**Вхідні дані**	**Операція**	**Результат**
1	Активи, ролі, процеси	Завантаження довідників	Контекст оцінювання
2	Оцінки 1..5	Валідація діапазону	Коректний набір даних
3	F, V, A	Обчислення P	Інтегральна імовірність
4	C, I, D, J, R	Обчислення I_total	Інтегральний наслідок
5	P, I_total, K	Обчислення ризиків	R_primary і R_residual
6	R_residual	Визначення зони ризику	Управлінська дія
7	Контрзаходи	Повторний розрахунок	Оцінка ефективності

3.5. Реалізація розрахунків ризику в програмному модулі

У цьому підрозділі описано частину програмного модуля, яка безпосередньо виконує розрахунки ризику за формулами (3.1)–(3.5). Простими словами, це розрахунковий блок: він приймає опис ризикового сценарію, перевіряє числові оцінки, обчислює імовірність, наслідок, первинний та залишковий ризик, а потім повертає зрозумілий результат для звіту. У коді використовується функція half_up для звичного академічного округлення, оскільки стандартна функція round у деяких мовах програмування може застосовувати банківське округлення. Клас RiskScenario описує вхідний сценарій і зберігає не лише числові оцінки, а й

пояснювальні поля: актив, джерело загрози, вразливість і процес. Клас RiskResult містить підсумок оцінювання: P, I_total, R_primary, R_residual, рівень ризику та запропоновані контролі. Клас RiskAssessmentEngine реалізує основні дії: probability обчислює імовірність, impact обчислює наслідок, level визначає рівень ризику, а assess об’єднує ці кроки для одного сценарію. Для групового оцінювання використовується assess_many, який розраховує всі сценарії та сортує їх за залишковим ризиком. Такий підхід зручний тим, що новий ризиковий сценарій можна додати до реєстру без зміни формул і структури програми.

Лістинг 3.1 - Опис сутності ризикового сценарію

```
from dataclasses import dataclass, field
from enum import Enum
from math import floor
from typing import Iterable, List, Sequence


def half_up(value: float) -> int:
    return int(floor(value + 0.5))


class RiskLevel(str, Enum):
    ACCEPTABLE = "Прийнятний"
    CONTROLLED = "Контрольований"
    SIGNIFICANT = "Значний"
    CRITICAL = "Критичний"


@dataclass(frozen=True)
class RiskScenario:
code: str
name: str
asset: str
source: str
```

```
    vulnerability: str
    process: str
    f: int
    v: int
    a: int
    c: int
    i: int
    d: int
    j: int
    r: int
    k: int
        controls: Sequence[str] = field(default_factory=list)
```

У наведеному фрагменті кожний сценарій зберігає не лише числові критерії, а й пояснювальні атрибути. Це важливо для подальшого формування реєстру ризиків, оскільки відповідальний працівник повинен бачити, який саме актив і який процес пов’язаний із конкретним числовим показником.

Лістинг 3.2 - Реалізація основних формул оцінювання ризику

```
class RiskAssessmentEngine:
    def probability(self, scenario: RiskScenario) -> int:
        value = 0.35 * scenario.f + 0.35 * scenario.v + 0.30 * scenario.a
        return half_up(value)

    def impact(self, scenario: RiskScenario) -> int:
        value = (
      0.30 * scenario.c
      + 0.20 * scenario.i
      + 0.20 * scenario.d
      + 0.15 * scenario.j
      + 0.15 * scenario.r
```

```
        )
        return half_up(value)

    def level(self, residual_risk: float) -> RiskLevel:
        if residual_risk <= 5:
            return RiskLevel.ACCEPTABLE
        if residual_risk <= 10:
            return RiskLevel.CONTROLLED
        if residual_risk <= 15:
            return RiskLevel.SIGNIFICANT
        return RiskLevel.CRITICAL

    def assess(self, scenario: RiskScenario) -> RiskResult:
        probability = self.probability(scenario)
        impact = self.impact(scenario)
        primary = probability * impact
        residual = primary * (6 - scenario.k) / 5
        return RiskResult(
            code=scenario.code,
            name=scenario.name,
            probability=probability,
            impact=impact,
            primary_risk=primary,
            residual_risk=round(residual, 2),
            level=self.level(residual),
            controls=scenario.controls,
        )
```

Реалізація не використовує прихованих коефіцієнтів, тому результати можна легко перевірити вручну.

3.6. Реалізація контролю автентифікації та блокування облікових записів

Перший практичний контрзахід спрямований на ризик компрометації облікового запису. У попередніх розділах було показано, що проблема формується слабкою парольною політикою та відсутністю блокування після кількох невдалих спроб входу. Тому в програмній моделі реалізовано клас AuthenticationControl, який перевіряє складність пароля і веде стан невдалих спроб входу.

Логіку контролю автентифікації користувачів CRM подано на рисунку 3.3.

Рисунок 3.3 - Контроль автентифікації користувачів CRM

Політика автентифікації у прототипі задає мінімальну довжину пароля 12 символів, обов’язкову наявність великих і малих літер, цифр та спеціальних символів. Також встановлюється блокування облікового запису після п’яти невдалих спроб на 15 хвилин. Для адміністративних облікових записів окремо фіксується вимога багатофакторної автентифікації. Саме такі правила дозволяють зменшити експлуатованість вразливості та підвищити зрілість контролю К. З погляду впровадження в CRM-систему цей механізм може працювати на рівні модуля авторизації або як частина зовнішнього сервісу ідентифікації. Основна вимога полягає в тому, щоб невдалі спроби входу журналювалися, а блокування не можна було обійти повторним відкриттям сесії або зміною браузера. Крім того, події блокування повинні потрапляти до журналу аудиту, оскільки велика кількість таких подій може свідчити про спробу підбору пароля. Практичний ефект цього

контролю проявляється у зменшенні показників F та V для сценарію компрометації облікового запису. Частота передумов зменшується, оскільки прості паролі більше не допускаються. Експлуатованість зменшується, оскільки після кількох помилок атака блокується. Показник K збільшується, бо контроль стає системним і технічно примусовим.

Параметри політики автентифікації після впровадження контролю наведено в таблиці 3.5.

Таблиця 3.5 - Політика автентифікації після впровадження контролю

Параметр	**Рекомендоване значення**	**Який ризик знижує**
Мінімальна довжина пароля	12 символів	Підбір простих паролів
Складність пароля	Великі/малі літери, цифри, спецсимволи	Використання шаблонних комбінацій
Блокування після помилок	5 невдалих спроб	Brute-force та credential stuffing
Час блокування	15 хвилин або більше	Швидке повторення атак
2FA для адміністраторів	Обов’язково	Компрометація привілейованих акаунтів
Журналювання	Усі успішні та невдалі входи	Виявлення підозрілої активності

Лістинг 3.3 - Фрагмент контролю парольної політики

```
@dataclass(frozen=True)
class AuthPolicy:
  min_length: int = 12
   require_upper: bool = True
   require_lower: bool = True
   require_digit: bool = True
   require_special: bool = True
  max_failed_attempts: int = 5
  lockout_minutes: int = 15
   mfa_required_for_admins: bool = True
```

```
class AuthenticationControl:
    SPECIALS = set("!@#$%^&*()_-+=[]{}:;,.?/|~")

    def __init__(self, policy: AuthPolicy) -> None:
        self.policy = policy

    def password_is_valid(self, password: str) -> tuple[bool, list[str]]:
      errors: list[str] = []
        if len(password) < self.policy.min_length:
            errors.append("password_length")
        if self.policy.require_upper and not any(ch.isupper() for ch in password):
            errors.append("missing_uppercase")
        if self.policy.require_lower and not any(ch.islower() for ch in password):
            errors.append("missing_lowercase")
        if self.policy.require_digit and not any(ch.isdigit() for ch in password):
            errors.append("missing_digit")
        if self.policy.require_special and not any(ch in self.SPECIALS for ch in
password):
            errors.append("missing_special")
        return len(errors) == 0, errors
```

3.7. Реалізація матриці доступу та виявлення надлишкових прав

Другий практичний контрзахід стосується надлишкових прав доступу. У досліджуваному кейсі окремі оператори мали доступ до фінансової інформації всіх клієнтів, хоча така функція не була необхідною для виконання їхніх прямих обов’язків. Це створювало критичний залишковий ризик, оскільки внутрішній користувач мав легітимний шлях до перегляду чутливої інформації. Для вирішення цієї проблеми у прототипі створено AccessMatrixValidator. Він приймає еталонну матрицю доступу та порівнює її з фактичними дозволами. Якщо у фактичній матриці є дозвіл, якого не повинно бути в еталонній моделі, система повертає його як надлишковий. Це дозволяє не вручну переглядати всі ролі, а автоматизувати

первинну перевірку відповідності. Еталонна матриця доступу повинна формуватися за участю власників бізнес-процесів, IT-відділу та відповідального за інформаційну безпеку. Наприклад, оператор може переглядати персональні контактні дані клієнта для обслуговування звернення, але не повинен експортувати фінансову історію. Працівник бухгалтерії може працювати з фінансовими записами, але не повинен змінювати технічні параметри підключення. Адміністратор може обслуговувати систему, але його дії мають бути повністю журналювані. Реалізація матриці доступу безпосередньо знижує ризик надлишкових прав і несанкціонованої модифікації записів. Після впровадження такого контролю показник A для внутрішнього порушника зменшується, оскільки актив стає менш доступним для ролей, яким він не потрібен. Показник K збільшується, оскільки контроль перестає бути декларативним і переходить у регулярну процедуру перевірки.

Приклад еталонної матриці доступу для клієнтського контуру CRM наведено в таблиці 3.6.

Таблиця 3.6 - Приклад еталонної матриці доступу для клієнтського контуру CRM

Роль	**Персональні дані**	**Сервісні звернення**	**Фінансові дані**	**Технічні параметри**	**Експорт**
Оператор	читання	читання	немає	немає	немає
Служба підтримки	читання	читання/запис звернення	немає	читання технічного статусу	немає
Бухгалтерія	немає/обмежено	немає	читання/запис фінансових операцій	немає	експорт агрегованих звітів
Технічний фахівець	немає/обмежено	читання звернення	немає	читання/запис технічних параметрів	немає
Адміністратор	технічний доступ за заявкою	технічний доступ за заявкою	технічний доступ за заявкою	адміністрування	експорт лише за погодженням
Аудитор/ІБ	читання журналів	читання журналів	читання журналів	читання журналів	контроль і звіти

Лістинг 3.4 - Фрагмент перевірки надлишкових прав доступу

```
 class Permission(str, Enum):
    READ = "read"
    WRITE = "write"
    EXPORT = "export"
    DELETE = "delete"
    ADMIN = "admin"


 @dataclass(frozen=True)
 class AccessRequest:
role: str
object_name: str
permission: Permission
   reason: str = ""


 class AccessMatrixValidator:
    def __init__(self, matrix: dict[str, dict[str, set[Permission]]]) -> None:
       self.matrix = matrix

    def allowed(self, request: AccessRequest) -> bool:
       role_rules = self.matrix.get(request.role, {})
       return request.permission in role_rules.get(request.object_name, set())

    def find_excess_permissions(self, current_matrix):
       excess = []
       for role, objects in current_matrix.items():
          for object_name, permissions in objects.items():
             allowed = self.matrix.get(role, {}).get(object_name, set())
             for permission in permissions:
                if permission not in allowed:
              excess.append((role, object_name, permission))
```

```
return excess
```

3.8. Реалізація контролю масового експорту клієнтських даних

Третій ключовий контрзахід спрямований на ризик масового експорту клієнтської бази. Саме цей сценарій у другому розділі отримав один із найвищих залишкових ризиків, оскільки поєднує великий масштаб наслідків і слабкий контроль операції. Особливість цього ризику полягає в тому, що експорт може виконуватися через штатну функцію системи, тому його не можна розглядати лише як зовнішню атаку.

Логіку контролю масового експорту клієнтських даних показано на рисунку 3.4.

Рисунок 3.4 - Логіка контролю масового експорту клієнтських даних

У прототипі створено ExportControlService. Він аналізує запит на експорт за трьома параметрами: кількість записів, наявність фінансових даних і наявність ідентифікаційних даних. Якщо вивантаження невелике і не містить чутливої інформації, воно дозволяється. Якщо вивантаження перевищує м’який ліміт або містить чутливі поля, потрібне погодження керівника або відповідального за процес. Якщо обсяг перевищує жорсткий ліміт, операція блокується і створюється подія для аудиту. Такий підхід дозволяє не забороняти експорт повністю, оскільки він може бути потрібний для звітності чи обслуговування, але переводить його у

контрольований процес. Кожна значна операція має залишати слід у журналі: хто ініціював експорт, яка роль користувача, скільки записів вивантажено, які категорії даних входили до набору, хто погодив операцію і коли вона була виконана. За потреби до цього механізму можна додати сповіщення відповідального за інформаційну безпеку. Практичний ефект контролю експорту проявляється у зниженні експлуатованості вразливості та підвищенні зрілості контролю. Навіть якщо користувач має службовий доступ до певних даних, він уже не може непомітно вивантажити великий масив клієнтських записів. Це суттєво зменшує залишковий ризик найбільш небезпечного сценарію.

Правила прийняття рішення щодо експорту клієнтських даних наведено в таблиці 3.7.

Таблиця 3.7 - Правила прийняття рішення щодо експорту клієнтських даних

Умова	**Рівень небезпеки**	**Рішення модуля**	**Пояснення**
до 100 записів без чутливих полів	Низький	allow	Операція дозволяється з базовим журналюванням
понад 100 записів або наявні фінансові/ідентифікаційні дані	Середній/високий	require_approval	Потрібне погодження відповідального
понад 1000 записів	Критичний	deny_and_alert	Операція блокується, створюється подія аудиту
будь-який експорт із погодженням	Контрольований	allow_with_audit	Дозволяється за умови розширеного журналювання

Лістинг 3.5 - Фрагмент контролю масового експорту даних

```
@dataclass(frozen=True)
class ExportRequest:
user_id: str
role: str
record_count: int
contains_financial_data: bool
```

```
    contains_identity_data: bool
    approved_by: str | None = None


class ExportControlService:
    def __init__(self, soft_limit: int = 100, hard_limit: int = 1000) -> None:
        self.soft_limit = soft_limit
        self.hard_limit = hard_limit

    def decision(self, request: ExportRequest) -> str:
        sensitive = request.contains_financial_data or
request.contains_identity_data
        if request.record_count > self.hard_limit:
            return "deny_and_alert"
        if request.record_count > self.soft_limit or sensitive:
            if request.approved_by:
                return "allow_with_audit"
            return "require_approval"
        return "allow"
```

3.9. Реалізація контролю резервного копіювання та відновлення

Четвертий практичний напрям пов’язаний із доступністю та цілісністю клієнтських даних. У межах аналізу було встановлено, що автоматичне створення резервних копій саме по собі не гарантує готовність до відновлення. Якщо копія пошкоджена, застаріла або ніколи не перевірялася шляхом тестового відновлення, підприємство може втратити доступ до клієнтської інформації саме в момент інциденту. Для вирішення цієї проблеми у прототипі реалізовано BackupControlService. Він оцінює стан резервної копії за чотирма ознаками: давність створення, правильність контрольної суми, дата останнього тестового відновлення та час відновлення. Результатом перевірки є статус: ready, outdated_backup, corrupted_backup, restore_never_tested або restore_test_required.

Така класифікація дозволяє швидко зрозуміти, яка саме частина backup-процесу потребує втручання. Рекомендований режим для телекомунікаційного підприємства передбачає щоденне створення резервних копій критичних даних CRM, перевірку контрольних сум після створення, щомісячне тестове відновлення у контрольованому середовищі та фіксацію фактичного часу відновлення. Для критичних сценаріїв також доцільно визначити цільові показники RTO та RPO, тобто допустимий час відновлення і допустимий обсяг втрати даних. У моделі ризику цей контрзахід підвищує показник K і зменшує невизначеність щодо наслідків інциденту. Підприємство вже не просто вірить у наявність backup-файлу, а має підтвердження, що дані можуть бути відновлені. Це особливо важливо для клієнтських фінансових записів і договорів, де помилка або втрата даних прямо впливає на якість обслуговування абонента.

Рекомендований порядок контролю backup/restore наведено в таблиці 3.8.

Таблиця 3.8 - Рекомендований порядок контролю backup/restore

Операція	**Періодичність**	**Відповідальний**	**Очікуваний результат**
Створення резервної копії CRM	щоденно	Адміністратор/автоматичний процес	Наявна актуальна копія
Перевірка контрольної суми	після кожного створення	Backup-сервіс	Виявлення пошкодженої копії
Тестове відновлення	щомісячно	IT-відділ	Підтвердження працездатності відновлення
Фіксація RTO/RPO	після кожного тесту	ІБ-відповідальний + IT	Оцінка реальної готовності до інциденту
Аналіз невдалих тестів	після кожної помилки	Робоча група	Коригувальний план

Лістинг 3.6 - Фрагмент перевірки стану резервної копії

```
@dataclass(frozen=True)
class BackupCheck:
  backup_id: str
age_hours: int
```

```
    checksum_valid: bool
    restore_tested_days_ago: int | None
    recovery_time_minutes: int | None


     class BackupControlService:
        def __init__(self, max_age_hours: int = 24, max_restore_test_age_days: int
= 30) -> None:
            self.max_age_hours = max_age_hours
            self.max_restore_test_age_days = max_restore_test_age_days

        def status(self, check: BackupCheck) -> str:
            if check.age_hours > self.max_age_hours:
                return "outdated_backup"
            if not check.checksum_valid:
                return "corrupted_backup"
            if check.restore_tested_days_ago is None:
                return "restore_never_tested"
            if check.restore_tested_days_ago > self.max_restore_test_age_days:
                return "restore_test_required"
            return "ready"
```

3.10. Апробація модуля на ризикових сценаріях підприємства

Для перевірки практичної придатності модуля використано ті самі шість ризикових сценаріїв, які були оцінені у другому розділі. Такий підхід дозволяє коректно порівняти результати: спочатку фіксується вихідний стан ризику, потім до сценаріїв застосовуються контрзаходи, а після цього виконується повторний розрахунок. У результаті можна показати, що запропоновані заходи не є абстрактними рекомендаціями, а змінюють числові показники ризику. У демонстраційній реалізації початкові сценарії задано як BASELINE_SCENARIOS. Для кожного з них збережено значення F, V, A, C, I, D, J, R та K, які відповідають

результатам другого розділу. Оновлений набір IMPROVED_SCENARIOS відображає стан після впровадження контролів: посиленої автентифікації, матриці доступу, контролю експорту, регулярних тестових відновлень, журналювання змін і навчання персоналу. Важливо підкреслити, що під час повторного розрахунку не зменшується сам потенційний масштаб шкоди там, де він об’єктивно залишається високим. Наприклад, якщо масовий витік клієнтської бази все ж відбудеться, наслідки для конфіденційності та репутації залишаться серйозними. Проте зменшується ймовірність реалізації сценарію і зростає ефективність контролю, а саме це і повинно відображатися в залишковому ризику. Результати запуску модуля показали, що найбільше зниження отримали ризики, для яких були впроваджені адресні технічні засоби: контроль експорту, матриця доступу та посилена автентифікація. Менш різке, але також суттєве зниження отримав ризик соціальної інженерії, оскільки для нього значна частина заходів має організаційний характер і потребує постійного підтримання.

Контрзаходи, застосовані до ризикових сценаріїв, наведено в таблиці 3.9.

Таблиця 3.9 - Контрзаходи, застосовані до ризикових сценаріїв

Код	**Сценарій**	**Основні контрзаходи після впровадження**
R1	Компрометація акаунта	2FA, складні паролі, блокування після помилок, журналювання входів
R2	Надлишкові права	Матриця RBAC, щоквартальний review, вилучення зайвих дозволів
R3	Масовий експорт	Ліміти, погодження, аудит, сповіщення про великі вивантаження
R4	Невдале відновлення	Checksum, тестове відновлення, контроль RTO/RPO
R5	Модифікація записів	Журнал змін, версійність, сповіщення про критичні поля
R6	Соціальна інженерія	Мінімізація видимості даних, навчання, регламент комунікації

Лістинг 3.7 - Результат демонстраційного запуску модуля

BASELINE

R2 16.0 Критичний

R3 16.0 Критичний

R1 12.8 Значний

R5 12.8 Значний

R4 7.2 Контрольований

R6 7.2 Контрольований

IMPROVED

R2 4.8 Прийнятний

R3 4.8 Прийнятний

R5 4.8 Прийнятний

R6 3.6 Прийнятний

R1 3.2 Прийнятний

R4 2.4 Прийнятний

3.11. Повторний розрахунок залишкового ризику після впровадження контрзаходів

Повторний розрахунок виконується за тими самими формулами, що й первинне оцінювання. Це принципово важливо, оскільки зміна методики між першим і другим вимірюванням зробила б порівняння некоректним. У цьому розділі змінюються лише вхідні параметри, які відображають фактичне вдосконалення контролів. Наприклад, для сценарію слабкої автентифікації зменшується експлуатованість вразливості V, оскільки введено вимоги до складності пароля і блокування після невдалих входів. Також зростає K, оскільки контроль стає системним. Для сценарію надлишкових прав доступу зменшуються F та A, тому що перегляд фінансових даних більше не є доступним для широкого кола операторів. Для масового експорту зменшуються V та A, оскільки з’являються ліміти, погодження і журналювання. Для резервного копіювання зростає K, тому

що процедура відновлення починає регулярно перевірятися. Для несанкціонованої модифікації критичних записів покращення забезпечують журнал змін, версійність і сповіщення. Для соціальної інженерії вплив мають навчання, мінімізація видимості даних і регламенти комунікації. Після повторного розрахунку сумарне значення залишкового ризику для шести сценаріїв зменшилося з 72,0 до 23,6. Середній залишковий ризик знизився з 12,0 до 3,93. Це означає, що ризиковий профіль клієнтського контуру переходить із зони значного ризику до зони прийнятного або близького до прийнятного стану. При цьому результати не означають повної відсутності ризику, а лише показують, що після впровадження контролів він стає керованим. Найважливішим результатом є зникнення критичних сценаріїв у повторному реєстрі. На початковому етапі критичними були надлишкові права доступу та масовий експорт клієнтської бази. Після впровадження матриці доступу, контролю експорту, погодження великих вивантажень і журналювання ці сценарії переходять до прийнятного рівня за числовою шкалою. У практичній роботі підприємства це означає, що вони більше не потребують аварійного реагування, але повинні залишатися під постійним моніторингом.

Порівняння залишкового ризику та узагальнені показники ефективності практичного рішення наведено в таблицях 3.10-3.11.

Таблиця 3.10 - Порівняння залишкового ризику до та після впровадження контрзаходів

Код	**Сценарій**	**До**	**Рівень до**	**Після**	**Рівень після**	**Зниження**
R1	Компрометація облікового запису	12,8	Значний	3,2	Прийнятний	75,0%
R2	Надлишкові права доступу	16,0	Критичний	4,8	Прийнятний	70,0%
R3	Масовий експорт бази	16,0	Критичний	4,8	Прийнятний	70,0%

R4	Невдале відновлення	7,2	Контрольований	2,4	Прийнятний	66,7%
R5	Модифікація критичних записів	12,8	Значний	4,8	Прийнятний	62,5%
R6	Соціальна інженерія	7,2	Контрольований	3,6	Прийнятний	50,0%

Таблиця 3.11 - Узагальнені показники ефективності практичного рішення

Показник	**До впровадження**	**Після впровадження**	**Висновок**
Сумарний залишковий ризик	72,0	23,6	Зменшення на 48,4 пункту
Середній залишковий ризик	12,0	3,93	Перехід до прийнятної зони
Кількість критичних ризиків	2	0	Критичні сценарії усунено як невідкладні
Кількість значних ризиків	2	0	Ризики переведено в керований стан
Кількість прийнятних ризиків	0	6	Усі сценарії перебувають у зоні моніторингу

3.12. Організаційне впровадження програмного рішення в роботу підприємства

Програмний модуль сам по собі не може забезпечити сталий результат, якщо не буде включений до організаційного процесу. Тому практичне впровадження повинно мати чіткий регламент. На першому етапі підприємство формує робочу групу, до якої входять представники IT-відділу, власники бізнес-процесів, відповідальний за інформаційну безпеку та за потреби представник юридичного напряму. Саме ця група затверджує шкали, матрицю доступу, правила експорту та періодичність перегляду ризиків. На другому етапі виконується первинне наповнення реєстру. До нього вносяться основні активи, ролі, процеси та ризикові сценарії. Для дипломної роботи використано шість базових сценаріїв, але в

реальному підприємстві їх може бути більше. Наприклад, окремо можна додати ризики інтеграції з білінговою системою, помилки API, компрометації адміністративної консолі, втрати журналів аудиту або несанкціонованого доступу підрядника. На третьому етапі модуль застосовується в тестовому режимі. У цей період важливо не блокувати роботу бізнес-процесів, а зібрати інформацію про фактичні права, експортні операції, стан резервних копій і типові події автентифікації. Після цього робоча група може уточнити порогові значення та усунути помилкові спрацьовування. Наприклад, якщо певна роль справді потребує регулярного експорту невеликих звітів, для неї можна передбачити окреме правило без зниження загального контролю. На четвертому етапі починається промислове використання. Тут модуль має працювати як частина регулярного циклу: щомісячний аналіз експорту та backup/restore, щоквартальний перегляд ролей, піврічне навчання персоналу та позапланове оцінювання після інцидентів або змін у CRM. Результати роботи повинні фіксуватися у звіті, який містить зміну залишкового ризику, перелік відкритих проблем і відповідальних за їх усунення. На п’ятому етапі модуль може бути інтегрований із технічними журналами CRM, системою моніторингу або SIEM. Це дозволить автоматично отримувати події про невдалі входи, зміну ролей, експорт великих обсягів даних і помилки резервного копіювання. Однак навіть без повної інтеграції прототип уже корисний як інструмент структурованого аудиту та повторного оцінювання.

Дорожню карту впровадження та KPI для контролю ефективності наведено в таблицях 3.12-3.13.

Таблиця 3.12 - Дорожня карта впровадження практичного рішення

№	**Етап**	**Зміст робіт**	**Орієнтовний строк**	**Результат**
1	Підготовка	Інвентаризація активів, ролей і сценаріїв	1-2 тижні	Початковий реєстр ризиків
2	Реалізація ядра	Налаштування розрахунків і шаблонів звітів	1 тиждень	Працюючий модуль оцінювання

3	Контроль доступу	Формування матриці RBAC і review прав	2-3 тижні	Зменшення надлишкових доступів
4	Контроль експорту	Пороги, погодження, журналювання	2 тижні	Зниження ризику масового витоку
5	Backup/restore	Checksum, тестове відновлення, RTO/RPO	1 місяць	Підтверджена готовність відновлення
6	Повторне оцінювання	Порівняння до/після і KPI	щоквартально	Оновлений ризиковий профіль

Таблиця 3.13 - KPI для контролю ефективності впровадження

Показник	**Цільове значення**	**Призначення**
Частка ролей, перевірених за матрицею доступу	не менше 95% щоквартально	Контроль надлишкових прав
Частка великих експортів із погодженням	100% щомісячно	Контроль масового витоку
Кількість критичних залишкових ризиків	0 після впровадження	Загальна керованість ризиків
Успішність тестового відновлення	не менше 95%	Готовність backup/restore
Частка співробітників, які пройшли навчання	не менше 90% щопівроку	Зниження людського фактору
Середній залишковий ризик за критичними сценаріями	тренд на зниження	Ефективність циклу управління

3.13. Обмеження реалізації та напрями подальшого розвитку

Запропонована реалізація є прототипом, тому має певні обмеження. По-перше, вона працює з модельними даними і не підключається безпосередньо до виробничої CRM. Для реального впровадження потрібна інтеграція з джерелами подій, довідником ролей, журналами експорту та системою резервного копіювання. По-друге, значення критеріїв після впровадження контролів задаються експертно. У подальшому їх можна уточнювати на основі фактичних метрик: кількості заблокованих входів, частки погоджених експортів, часу відновлення, кількості виявлених зайвих прав. По-третє, прототип не містить повноцінного

користувацького інтерфейсу. У практичній системі доцільно створити веб-інтерфейс для введення сценаріїв, перегляду реєстру ризиків, побудови динаміки залишкового ризику та формування звітів для керівництва. Однак для цілей дипломної роботи достатньо показати ядро логіки, оскільки саме воно підтверджує практичну реалізацію методики. По-четверте, у поточній версії не застосовуються складні статистичні або машинні методи. Це зроблено свідомо, оскільки в умовах невеликого або середнього телекомунікаційного підприємства часто відсутній достатній обсяг якісних історичних даних для навчання моделей. Натомість напівкількісна модель є прозорою, пояснюваною та прийнятною для аудиту. Подальший розвиток рішення може відбуватися у кількох напрямах. Перший напрям - інтеграція з базою даних CRM для автоматичного отримання ролей і дозволів без доступу до змісту персональних даних. Другий напрям - інтеграція з журналами подій для автоматичного виявлення масового експорту, серій невдалих входів і змін критичних полів. Третій напрям - створення панелі показників, де керівництво бачить не лише перелік ризиків, а і зміну ризикового профілю в часі. Четвертий напрям - розширення моделі на інші контури підприємства, наприклад білінг, мобільний застосунок або особистий кабінет клієнта. Таким чином, розроблений прототип є достатнім для демонстрації практичного вирішення поставленої проблеми та водночас має потенціал для розвитку. Він поєднує методику оцінювання ризиків, технічні контрзаходи та організаційний цикл повторного контролю.

3.14. Тестування програмного модуля та перевірка коректності розрахунків

Після реалізації програмного модуля необхідно перевірити, що він справді коректно виконує розрахунки та не спотворює методику другого розділу. Для цього тестування доцільно розділити на три рівні: перевірку формул, перевірку прикладних контролів і перевірку звітного результату. Перший рівень підтверджує, що значення P, I_total, R_primary і R_residual обчислюються відповідно до визначених формул. Другий рівень показує, що класи автентифікації, матриці доступу, експорту та резервного копіювання повертають очікувані рішення. Третій рівень перевіряє, що після впровадження контрзаходів реєстр ризиків правильно

ранжується і відображає зменшення залишкового ризику. Для перевірки формул використовуються контрольні сценарії з відомим очікуваним результатом. Наприклад, якщо для ризику масового експорту задано F=4, V=5, A=4, то інтегральна імовірність повинна дорівнювати 4. Якщо наслідок має значення C=5, I=3, D=2, J=5, R=5, то інтегральний наслідок дорівнює 4. Первинний ризик дорівнює 16, а за K=1 залишковий ризик дорівнює 16. Такі контрольні приклади дозволяють швидко виявити помилку в коефіцієнтах або в округленні. Тестування контролю автентифікації передбачає перевірку слабкого і сильного пароля, а також моделювання серії невдалих входів. Слабкий пароль повинен відхилятися з поясненням причини: недостатня довжина, відсутність цифри або спеціального символу. Після п’ятої невдалої спроби акаунт повинен отримати статус тимчасово заблокованого. Це підтверджує, що контроль не є лише описовою рекомендацією, а має конкретну програмну поведінку. Тестування матриці доступу виконується через порівняння еталонної та фактичної моделі прав. Якщо в ролі оператора з’являється дозвіл export для фінансових даних, модуль повинен повернути його у списку надлишкових прав. Якщо ж роль має лише дозволи, передбачені еталонною матрицею, перевірка не повинна генерувати зауваження. Така логіка важлива для регулярного review доступів, бо вона зменшує залежність від ручного перегляду кожного профілю. Тестування контролю експорту виконується за трьома типовими ситуаціями: малий експорт без чутливих полів, експорт чутливих даних без погодження та великий експорт понад жорсткий ліміт. У першому випадку очікуване рішення - allow, у другому - require_approval, у третьому - deny_and_alert. Це дає змогу переконатися, що модуль не блокує звичайну роботу, але реагує на операції з підвищеним ризиком. Тестування backup/restore перевіряє, чи правильно модуль відрізняє робочу резервну копію від проблемної. Якщо копія старіша за допустиме значення, повертається статус outdated_backup. Якщо контрольна сума не підтверджена - corrupted_backup. Якщо тестове відновлення ніколи не виконувалося або виконувалося занадто давно, модуль повертає відповідний попереджувальний статус. Таке тестування прямо пов’язане з практичною проблемою, виявленою під час аналізу підприємства.

Набір тестових випадків для перевірки практичного модуля наведено в таблиці 3.14.

Таблиця 3.14 - Набір тестових випадків для перевірки практичного модуля

№	Об’єкт тестування	Вхідні умови	Очікуваний результат
1	Формула ризику	R3: F=4, V=5, A=4, C=5, I=3, D=2, J=5, R=5, K=1	R_residual = 16,0; рівень - критичний
2	Парольна політика	Пароль коротший за 12 символів без спецсимволу	password_is_valid = False
3	Блокування входу	5 невдалих спроб входу поспіль	акаунт тимчасово заблоковано
4	Матриця доступу	Оператор має export для фінансових даних	дозвіл визначено як надлишковий
5	Контроль експорту	1500 записів без погодження	deny_and_alert
6	Backup/restore	копія старша за 24 години	outdated_backup
7	Повторний розрахунок	застосовано контрзаходи для R1-R6	критичних ризиків немає

Лістинг 3.8 - Приклад тесту контролю експорту

```
def test_export_control() -> None:
    service = ExportControlService(soft_limit=100, hard_limit=1000)

    normal = ExportRequest(
        user_id="u101", role="operator", record_count=20,
        contains_financial_data=False, contains_identity_data=False,
    )
    assert service.decision(normal) == "allow"

    sensitive = ExportRequest(
        user_id="u102", role="accounting", record_count=150,
        contains_financial_data=True, contains_identity_data=False,
```

```
)
assert service.decision(sensitive) == "require_approval"

massive = ExportRequest(
    user_id="u103", role="operator", record_count=1500,
    contains_financial_data=True, contains_identity_data=True,
)
assert service.decision(massive) == "deny_and_alert"
```

Наведений тест демонструє очікувану поведінку модуля для трьох рівнів експортної операції. У реальному середовищі такі тести можуть виконуватися автоматично після оновлення правил контролю або після зміни логіки CRM. Це зменшує ризик того, що нове оновлення випадково вимкне важливий захисний механізм.

3.15. Схема зберігання даних і можливість інтеграції з CRM-системою

Щоб практичне рішення могло бути використане не лише як окремий скрипт, а і як частина внутрішнього процесу підприємства, необхідно визначити схему зберігання даних. Найпростішим варіантом є зберігання сценаріїв у CSV або JSON-файлі, але для регулярного використання доцільніше застосувати невелику реляційну базу даних. Вона може містити таблиці risk_scenarios, risk_results, controls, access_matrix, export_events і backup_checks. Таблиця risk_scenarios зберігає опис ризикового сценарію та його поточні оцінки. Таблиця risk_results містить результати розрахунку для кожного періоду оцінювання. Завдяки цьому можна бачити не лише поточне значення залишкового ризику, а й динаміку в часі. Таблиця controls описує контрзаходи, пов’язані зі сценаріями. Таблиця access_matrix використовується для зберігання еталонних прав, а export_events і backup_checks - для технічних подій контролю. Інтеграція з CRM не повинна вимагати копіювання персональних даних клієнтів у модуль ризиків. Для аналізу достатньо технічних і агрегованих даних: роль користувача, тип операції, кількість записів, категорія даних, факт погодження, час події, статус резервної копії. Це

дозволяє зберегти принцип мінімізації даних і не створювати нову базу, яка сама по собі стане додатковим ризиковим активом. У реальній експлуатації модуль може отримувати події через API або через періодичний імпорт журналів. Наприклад, CRM може передавати подію про спробу експорту, а модуль повертає рішення: дозволити, вимагати погодження або заблокувати. Для матриці доступу може виконуватися щоденне порівняння фактичних ролей із еталонними. Для backup/restore модуль може отримувати службові записи від системи резервного копіювання. Нижче наведено приклад спрощеної SQL-структури. Вона не є повною промисловою схемою, але показує, як результати третього розділу можуть бути перенесені з прототипу у реальне інформаційне середовище. Така схема також може бути використана як основа для подальшого розвитку дипломної роботи або для створення демонстраційної бази даних.

Лістинг 3.9 - Приклад структури таблиць для зберігання ризиків і подій контролю

```
CREATE TABLE risk_scenarios (
    id INT PRIMARY KEY AUTO_INCREMENT,
    code VARCHAR(20) NOT NULL UNIQUE,
    name VARCHAR(255) NOT NULL,
    asset VARCHAR(255) NOT NULL,
    source VARCHAR(255) NOT NULL,
    vulnerability VARCHAR(255) NOT NULL,
    process_name VARCHAR(255) NOT NULL,
    f TINYINT NOT NULL,
    v TINYINT NOT NULL,
    a TINYINT NOT NULL,
    c TINYINT NOT NULL,
    i TINYINT NOT NULL,
    d TINYINT NOT NULL,
    j TINYINT NOT NULL,
    r TINYINT NOT NULL,
```

```
    k TINYINT NOT NULL,
    created_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP
);

CREATE TABLE risk_results (
    id INT PRIMARY KEY AUTO_INCREMENT,
    scenario_id INT NOT NULL,
    assessment_date DATE NOT NULL,
    probability_score TINYINT NOT NULL,
    impact_score TINYINT NOT NULL,
    primary_risk DECIMAL(5,2) NOT NULL,
    residual_risk DECIMAL(5,2) NOT NULL,
    risk_level VARCHAR(50) NOT NULL,
    FOREIGN KEY (scenario_id) REFERENCES risk_scenarios(id)
);

CREATE TABLE export_events (
    id INT PRIMARY KEY AUTO_INCREMENT,
    user_id VARCHAR(80) NOT NULL,
    user_role VARCHAR(80) NOT NULL,
    record_count INT NOT NULL,
    contains_identity_data BOOLEAN NOT NULL,
    contains_financial_data BOOLEAN NOT NULL,
    decision VARCHAR(50) NOT NULL,
    approved_by VARCHAR(80),
    event_time TIMESTAMP DEFAULT CURRENT_TIMESTAMP
);
```

Варіанти інтеграції модуля з CRM-системою наведено в таблиці 3.15.

Таблиця 3.15 - Варіанти інтеграції модуля з CRM-системою

Варіант інтеграції	**Сутність**	**Переваги**	**Обмеження**

Окремий audit-скрипт	Періодичне завантаження CSV/JSON	Швидке впровадження, мінімальний вплив на CRM	Немає реакції в реальному часі
Внутрішній веб-модуль	Робота через інтерфейс для ІБ-відповідального	Зручність для регулярного оцінювання	Потрібна розробка UI
API-сервіс контролю	CRM надсилає події, модуль повертає рішення	Можливість блокування небезпечних дій	Потрібна інтеграція з CRM
SIEM/моніторинг	Передача подій у систему моніторингу	Централізований аудит і кореляція	Потребує зрілої інфраструктури журналювання

Найбільш реалістичним для початкового впровадження є комбінований варіант: спочатку модуль працює як окремий audit-інструмент для повторного **оцінювання ризиків, а після перевірки логіки поступово інтегрується з CRM через API або через імпорт технічних журналів**. Такий підхід зменшує ризик впровадження і не створює різкого навантаження на роботу підприємства.

Висновки до розділу 3

У третьому розділі виконано практичне розв’язання проблематики, сформованої у попередніх розділах дипломної роботи. Якщо перший розділ визначав предметну область і ключові ризики, а другий розділ формалізував методику оцінювання, то третій розділ переводить ці результати у практичний програмний механізм. Було запропоновано прототип модуля управління ризиками клієнтського контуру CRM-системи телекомунікаційного підприємства.

Його ядро реалізує розрахунок інтегральної імовірності, інтегрального наслідку, первинного та залишкового ризику. Це забезпечує відтворюваність оцінювання і дозволяє виконувати повторний аналіз після впровадження контрзаходів. У межах практичного рішення реалізовано окремі компоненти для найбільш важливих ризикових напрямів: посилення автентифікації, перевірка матриці доступу, контроль масового експорту, перевірка стану резервних копій і формування повторного реєстру ризиків.

Така структура відповідає фактичним слабким місцям, виявленим під час

аналізу CRM-середовища. Апробація на шести ризикових сценаріях показала, що після впровадження запропонованих контролів сумарний залишковий ризик зменшується з 72,0 до 23,6, а середній залишковий ризик - з 12,0 до 3,93. Критичні та значні ризики переводяться до прийнятної зони, що підтверджує ефективність запропонованого підходу.

Практична цінність розділу полягає в тому, що запропоноване рішення не обмежується загальними рекомендаціями. Воно має алгоритм, класову модель, фрагменти коду, правила контролю і показники ефективності, які можуть бути використані як основа для внутрішнього аудиторського інструменту або для подальшої інтеграції з CRM-системою телекомунікаційного підприємства.

ВИСНОВКИ

У кваліфікаційній роботі вирішено прикладну задачу оцінювання ризиків інформаційної безпеки клієнтів у телекомунікаційному підприємстві. На основі аналізу предметної області встановлено, що найбільш критичними для захисту є персональні ідентифікаційні дані, контактна інформація, фінансові записи, технічні параметри підключення, історія звернень до підтримки, облікові записи співробітників, журнали подій і резервні копії. У першому розділі обґрунтовано актуальність теми, визначено об’єкт, предмет, мету та завдання дослідження, а також проаналізовано загрози й вразливості, характерні для клієнтського контуру CRM-системи телекомунікаційного підприємства.

У другому розділі розроблено методику оцінювання ризиків, яка поєднує процесно-рольовий підхід, сценарний аналіз і напівкількісні шкали. Запропонована методика дозволяє враховувати ймовірність реалізації загрози, тяжкість наслідків для клієнта та підприємства, а також коефіцієнт зрілості наявних контролів. Завдяки цьому первинний і залишковий ризик можуть бути порівняні в єдиній системі координат.

У третьому розділі виконано практичну реалізацію запропонованого підходу у вигляді прототипу програмного модуля. Модуль автоматизує розрахунок ризику, перевіряє дотримання парольної політики, аналізує матрицю доступу, контролює масовий експорт клієнтських даних, оцінює стан резервного копіювання та формує повторний реєстр ризиків після впровадження контрзаходів.

Апробація на типових ризикових сценаріях підтвердила практичну придатність запропонованого рішення. Після застосування контрзаходів рівень залишкового ризику для критичних сценаріїв знижується, а найбільш небезпечні події переводяться до прийнятної або контрольованої зони. Це підтверджує, що методика може бути використана для пріоритезації заходів захисту та підтримки управлінських рішень у сфері інформаційної безпеки.

Практичне значення роботи полягає в тому, що запропонований підхід може бути використаний як основа для внутрішнього аудиту клієнтського контуру CRM-

системи, формування реєстру ризиків і контролю залишкового ризику після впровадження захисних заходів. Подальший розвиток роботи може передбачати інтеграцію модуля з реальними журналами CRM-системи, автоматичне оновлення матриці доступу, розширення переліку контрольних правил і накопичення історичних даних для аналізу динаміки залишкового ризику.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection - Information security management systems - Requirements. Geneva: International Organization for Standardization, 2022. [с. 5-8, 12-16].

2. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection - Information security controls. Geneva: International Organization for Standardization, 2022. [с. 40-42, 45-48, 66-80].

3. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection - Guidance on managing information security risks. Geneva: International Organization for Standardization, 2022. [с. 15-16, 23-28, 50-62].

4. ISO 31000:2018. Risk management - Guidelines. Geneva: International Organization for Standardization, 2018. [с. 5-8, 11-14].

5. Ross R., McEvilley M., Oren J. Guide for Conducting Risk Assessments. NIST Special Publication 800-30 Revision 1. Gaithersburg: National Institute of Standards and Technology, 2012. [с. 15-20, 24-28, 50-66].

6. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. Gaithersburg: National Institute of Standards and Technology, 2024. [с. 3-7, 20-25, 29-31].

7. Joint Task Force. Security and Privacy Controls for Information Systems and Organizations. NIST Special Publication 800-53 Revision 5. Gaithersburg: National Institute of Standards and Technology, 2020. [с. 23-28, 46-49, 81-85].

8. Swanson M., Bowen P., Phillips A. W., Gallup D., Lynes D. Contingency Planning Guide for Federal Information Systems. NIST Special Publication 800-34 Revision 1. Gaithersburg: National Institute of Standards and Technology, 2010. [с. 20-24, 35-41, 70-76].

9. Grassi P. A., Garcia M. E., Fenton J. L. Digital Identity Guidelines: Authentication and Lifecycle Management. NIST Special Publication 800-63B. Gaithersburg: National Institute of Standards and Technology, 2017. [с. 15-20, 40-47, 62-70].

10. Center for Internet Security. CIS Critical Security Controls Version 8.1 [Електронний ресурс]. Center for Internet Security, 2024. URL: https://www.cisecurity.org/controls. (дата звернення: 05.05.2026)

11. OWASP Foundation. Application Security Verification Standard 4.0.3 [Електронний ресурс]. OWASP Foundation, 2021. URL: https://owasp.org/www-project-application-security-verification-standard/.

12. OWASP Foundation. OWASP Risk Rating Methodology [Електронний ресурс].URL: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology . (дата звернення: 05.05.2026)

13. ENISA. ENISA Threat Landscape 2024 [Електронний ресурс]. Athens: European Union Agency for Cybersecurity, 2024. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 . (дата звернення: 05.05.2026)

14. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text . (дата звернення: 10.05.2026)

15. Про електронні комунікації : Закон України від 16.12.2020 № 1089-IX [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text .

16. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
(дата звернення: 10.05.2026).

17. Про інформацію : Закон України від 02.10.1992 № 2657-XII [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 10.05.2026).

18. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
(дата звернення: 10.05.2026).

19. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd ed. Indianapolis: Wiley, 2020. [с. 35-48, 210-225, 641-655].

20. Bishop M. Computer Security: Art and Science. 2nd ed. Boston: Addison-Wesley, 2019. [с. 25-37, 125-140, 390-405].

21. Stallings W., Brown L. Computer Security: Principles and Practice. 5th ed. Pearson, 2023. [с. 45-58, 180-196, 420-435].

22. Pfleeger C. P., Pfleeger S. L., Margulies J. Security in Computing. 5th ed. Boston: Prentice Hall, 2015. [с. 50-65, 210-224, 480-492].

23. Whitman M. E., Mattord H. J. Principles of Information Security. 7th ed. Boston: Cengage Learning, 2021. [с. 38-52, 145-160, 310-326].

24. The Open Group. Risk Taxonomy (O-RT): Technical Standard [Електронний ресурс]. Reading: The Open Group, 2009. [с. 15-16, 23-28, 46-49, 50-52]. URL: https://pubs.opengroup.org/onlinepubs/9699919899/toc.pdf
(дата звернення: 12.05.2026).

25. Python Software Foundation. Python 3.12 Documentation [Електронний ресурс]. Python Software Foundation, 2024. URL: https://docs.python.org/3.12/ (дата звернення: 12.05.2026)..

26. Oracle. MySQL 8.0 Reference Manual [Електронний ресурс]. Oracle Corporation, 2024. URL: https://dev.mysql.com/doc/refman/8.0/en/)
(дата звернення: 12.05.2026)..

ДОДАТОК

Програмний прототип модуля оцінювання ризиків

У додатку подано призначення програмного прототипу, розробленого у третьому розділі. Повні фрагменти коду наведено у лістингах 3.1-3.9, а додаток фіксує склад основних компонентів модуля та їх зв’язок із практичними задачами оцінювання ризиків.

Компонент	**Призначення**	**Пов’язаний ризик**
RiskScenario	Описує актив, загрозу, вразливість, процес і оцінки ризику	Усі ризикові сценарії
RiskCalculator	Обчислює інтегральну ймовірність, наслідок, первинний і залишковий ризик	Помилки ручного оцінювання
PasswordPolicyChecker	Перевіряє складність пароля та стан блокування	Компрометація облікового запису
AccessMatrixService	Порівнює фактичні й еталонні права доступу	Надлишкові права операторів
ExportControlService	Оцінює операції експорту за кількістю та чутливістю даних	Масовий витік клієнтської бази
BackupHealthChecker	Перевіряє актуальність і тестування відновлення	Втрата доступності та неможливість відновлення