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:

«Система управління ризиками інформаційної безпеки нотаріальної контори»

Охріменко Єлизавета Валентинівна

(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

«Система управління ризиками інформаційної безпеки нотаріальної контори»

(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 Охріменко Єлизавета Валентинівна

(прізвище, ім'я та по батькові повністю)

125 «Кібербезпека»

(спеціальність)

Безпека інформаційних та комунікаційних систем

(освітня програма)

Група БІКС-22

Керівник Ізмайлова О.В.

(прізвище та ініціали)

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

(вчене звання, науковий ступінь)

Рецензент_____

(прізвище та ініціали)

Ідентичність підтверджую

Київ 2026

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

Охріменко Єлизавета Валентинівна
(прізвище, ім'я та по батькові здобувача)

1. Тема роботи «Система управління ризиками інформаційної безпеки нотаріальної контори»
затверджена наказом ректора КНУБА № 576/52/-15/13.2/26 від «14» травня 2026 року
2. Керівник роботи
доцент кафедри кібербезпеки та комп'ютерної інженерії, кандидат технічних наук Ізмайлова Ольга Василівна
(прізвище, ім'я та по батькові, науковий ступінь, вчене звання)

3. Термін подання здобувачем роботи до захисту 30 травня 2026
4. Зміст пояснювальної записки за розділами:
Р. 1. Аналіз предметної області та нормативно-правове регулювання управління ризиками інформаційної безпеки нотаріальної контори
Р. 2. Ідентифікація активів, загроз, вразливостей та оцінювання ризиків інформаційної безпеки нотаріальної контори
Р. 3. Програмна реалізація системи оцінювання ризиків інформаційної безпеки нотаріальної контори

5. Календарний план виконання роботи:

Види робіт та їх зміст	Дата виконання
Розділ 1	03.05.2025
Розділ 2	15.05.2026
Розділ 3	25.05.2026
Остаточне оформлення роботи	01.06.2026
Направлення роботи для перевірки на плагіат	08.06.2026
Попередній захист роботи	08.06.2026
Направлення роботи на рецензування	08.06.2026

6. Дата видачі завдання 10.02.2026

Керівник Ізмайлова О.В. _____

Здобувач Охріменко Є.В. _____

Анотація

Охріменко Є. В. Система управління ризиками інформаційної безпеки нотаріальної контори. Дипломна робота на здобуття освітнього ступеня бакалавр за спеціальністю 125 «Кібербезпека та захист інформації». — Київський національний університет будівництва та архітектури — Київ, 2026. — 125 с., 12 табл., список використаних джерел із 21 найменування, три розділи, 22 підрозділи.

Дипломну роботу присвячено автоматизації процесу управління ризиками інформаційної безпеки нотаріальної контори. Метою роботи є розробка програмної системи оцінювання ризиків, яка дозволить підвищити ефективність та об’єктивність прийняття рішень щодо захисту інформаційних активів. Для оцінювання ризиків застосовано експертне ранжування активів, коефіцієнт конкордації Кендала, метод аналізу ієрархій та лінійну згортку критеріїв. Розроблено програмну систему на мові C#, яка дозволяє автоматизувати ранжування активів, розраховувати рівень ризику, визначати категорію ризику та формувати рекомендації щодо обробки ризиків. Систему протестовано на реальних даних нотаріальної контори.

Ключові слова: управління ризиками, інформаційна безпека, нотаріальна контора, ранжування активів, коефіцієнт конкордації, оцінка ризиків, C#.

Abstract

Okhrimenko E. V. Information security risk management system of a notary office. Thesis for the degree of bachelor in specialty 125 "Cybersecurity and information protection". — Kyiv National University of Construction and Architecture — Kyiv, 2026. — 125 p., 12 tables, list of sources used with 21 titles, three sections, 22 subsections.

The thesis is devoted to the automation of the process of information security risk management of a notary office. The purpose of the work is to develop a software system for risk assessment, which will allow to increase the efficiency and objectivity

of decision-making regarding the protection of information assets. Expert asset ranking, Kendall concordance coefficient, the method of analysis of hierarchies and linear convolution of criteria were used to assess risks. A software system in the C# language was developed, which allows to automate asset ranking, calculate the risk level, determine the risk category and generate recommendations for risk processing. The system was tested on real data of a notary office.

Keywords: risk management, information security, notary office, asset ranking, concordance coefficient, risk assessment, C#.

РЕЗЮМЕ (SUMMARY) *до кваліфікаційної випускової роботи здобувача*	ПІБ *Охріменко Єлизавета Валентинівна Okhrimenko Yelyzaveta Valentynivna*		
ЗВО	Київський національний університет будівництва і архітектури		
Тема *(українською та англійською)*	«Система управління ризиками інформаційної безпеки нотаріальної контори» «Information security risk management system of a notary office»		
Освітній ступінь	Бакалавр		
Факультет	Автоматизації і інформаціних технологій		
Випускова кафедра	Кібербезпеки та комп'ютерної інженерії		
Спеціальність	125 «Кібербезпека»		
Освітня програма	Безпека інформаційних і комунікаційних систем		
Керівник	Ізмайлова Ольга Василівна		
Обсяг роботи:	*Поснювальна записка, стор.*	*Розділів*	*Презентація, кількість слайдів*
	125	3	18
Розділ 1	Аналіз предметної області та нормативно-правове регулювання управління ризиками інформаційної безпеки нотаріальної контори		
Розділ 2	Ідентифікація активів, загроз, вразливостей та оцінювання ризиків інформаційної безпеки нотаріальної контори		
Розділ 3	Програмна реалізація системи оцінювання ризиків інформаційної безпеки нотаріальної контори		
Висновки по роботі	Проведено аналіз предметної області, нормативно-правової бази та існуючих підходів до управління ризиками. Розроблено шкали оцінювання ймовірності та наслідків, визначено критерії прийнятності ризиків. Проведено ідентифікацію та ранжування активів нотаріальної контори. Побудовано модель загроз та модель порушника. Реалізовано програмну систему компонентів оцінки ризиків інформаційної безпеки нотаріальної контори.		

Ключові слова:	управління ризиками, інформаційна безпека, нотаріальна контора, ранжування активів, коефіцієнт конкордації, оцінка ризиків, C#
Keywords:	risk management, information security, notary office, asset ranking, concordance coefficient, risk assessment, C#

Здобувач Охріменко Є.В. _____/ _____

Керівник Ізмайлова О.В. _____/ _____

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ, ТЕРМІНІВ

СУІБ — система управління інформаційною безпекою.

КЕП — кваліфікований електронний підпис.

РНОКПП — реєстраційний номер облікової картки платника податків.

ДП «НАІС» — Державне підприємство «Національні інформаційні системи».

NIST — Стандарти Національного інституту стандартів і технологій США.

ПЗ — програмне забезпечення.

ПК — персональний комп'ютер.

БФП — багатофункціональний пристрій (принтер, сканер).

CSV - Comma-Separated Values (текстовий формат для табличних даних).

ІТ — інформаційні технології.

Актив - все, що має цінність для нотаріальної контори та потребує захисту.

Вразливість - слабке місце в системі захисту, яке може бути використане для реалізації загрози.

Загроза - потенційна подія або дія, яка може призвести до порушення конфіденційності, цілісності або доступності інформації.

Ризик - ймовірність реалізації загрози з урахуванням потенційних наслідків.

Управління ризиками - систематичний процес ідентифікації, аналізу, оцінювання, обробки, моніторингу та перегляду ризиків, пов’язаних із забезпеченням інформаційної безпеки.

Нотаріальна таємниця - відомості, які стали відомі нотаріусу у зв’язку з вчиненням нотаріальних дій і не підлягають розголошенню.

Персональні дані - відомості, що дозволяють ідентифікувати фізичну особу, зокрема паспортні дані, реєстраційний номер облікової картки платника податків (РНОКПП), місце проживання тощо.

Ранжування активів - процес визначення пріоритетності захисту активів на основі їх цінності, отриманої шляхом експертного опитування.

Лінійна згортка - метод зведення багатокритеріальної оцінки до одного числа шляхом зваженого підсумовування оцінок за кожним критерієм.

Коефіцієнт конкордації Кендалла - статистичний показник узгодженості думок кількох експертів при ранжуванні об’єктів.

Матриця ризиків - двовимірна таблиця розміром 5×5, де по горизонтальній осі відкладається ймовірність реалізації ризику (P), по вертикальній - наслідки (A), а в клітинах зазначаються номери ризиків, що потрапили до відповідної комбінації.

STRIDE — Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege - методологія класифікації загроз, розроблена компанією Microsoft.

ВСТУП

Сучасний нотаріат в Україні зазнає стрімкої цифровізації. Нотаріальні контори інтегруються з державними електронними реєстрами, використовують кваліфікований електронний підпис та обробляють значні масиви конфіденційної інформації, зокрема нотаріальну таємницю та персональні дані клієнтів. Цей процес, з одного боку, підвищує ефективність нотаріальної діяльності, а з іншого — створює нові загрози інформаційній безпеці, які раніше не були характерними для нотаріату. Водночас практика показує, що в багатьох нотаріальних конторах заходи захисту інформації впроваджуються безсистемно, без попереднього аналізу ризиків та обґрунтування доцільності тих чи інших захисних механізмів. Таким чином, **основна проблема**, яка розглядається в роботі, полягає у суперечності між зростаючою залежністю нотаріальної діяльності від інформаційно-комунікаційних технологій, високою цінністю інформації, що обробляється, підвищеними вимогами законодавства до її захисту та недостатнім рівнем впровадження системних підходів до управління ризиками в практичній дільності нотаріальних контор.

Метою дипломної роботи є розробка та обґрунтування практичних рекомендацій щодо впровадження процесу управління ризиками як ключового елементу системи управління інформаційною безпекою для нотаріальної контори.

Об’єктом дослідження є система управління інформаційною безпекою нотаріальної контори, а **предметом дослідження** — методи та засоби оцінювання та управління ризиками інформаційної безпеки в діяльності нотаріальної контори.

У ході виконання роботи проаналізовано нормативно-правову базу України щодо захисту інформації в діяльності нотаріусів; визначено особливості нотаріальної контори як об’єкта інформаційної діяльності; ідентифіковано актуальні загрози та вразливості для типової нотаріальної контори; розроблено та застосовано методику оцінювання ризиків інформаційної безпеки для нотаріальної контори; запропоновано заходи з обробки ідентифікованих ризиків;

а також розроблено рекомендації щодо впровадження процесу управління ризиками в систему управління інформаційною безпекою нотаріальної контори.

Методологічною основою роботи є міжнародні стандарти серії ISO/IEC 27000, адаптовані в Україні як національні ДСТУ, зокрема ДСТУ ISO/IEC 27001, ДСТУ ISO/IEC 27002 та ДСТУ ISO/IEC 27005. Для оцінювання ризиків застосовується комбінований (напівкількісний) підхід, який дозволяє отримати наочні результати при відносній простоті реалізації. У роботі також використовуються методи системного аналізу, порівняльного аналізу та експертного оцінювання.

Напрями подальшого вдосконалення, запропоновані в роботі, мають практичну цінність та можуть бути безпосередньо впроваджені в діяльність нотаріальних контор. Запропоновані заходи враховують реальні ресурсні обмеження типової нотаріальної контори. Практичними результатами роботи є реєстр активів нотаріальної контори з визначенням їх цінності, перелік актуальних загроз та вразливостей, матриця ризиків, план обробки ризиків з визначенням пріорітетних заходів, які нотаріус може адаптувати під свої потреби. В рамках виконання дипломної роботи встановлено, що робота повинна базуватися на чинній нормативно-правовій базі України та міжнародних стандартах, результати мають бути практично цінними та придатними для безпосереднього використання, а основний фокус дослідження спрямовано на процес оцінювання ризиків.

В рамках дипломного проекту пропонується адаптувати методологію оцінювання ризиків, визначену в ДСТУ ISO/IEC 27005, до специфіки нотаріальної контори із застосуванням комбінованого (напівкількісного) підходу. Основний фокус дослідження зосереджено на етапі оцінювання ризиків як найбільш критичному для прийняття обґрунтованих рішень щодо захисту інформації. Запропонований підхід дозволяє отримати наочні та зрозумілі визначення проритетів.

1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА НОРМАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НОТАРІАЛЬНОЇ КОНТОРИ

1.1 Нотаріальна контора як об’єкт інформаційної діяльності

1.1.1 Сутність та структура нотаріальної контори

Нотаріальна контора — це організаційно-правова форма здійснення нотаріальної діяльності, яка представляє собою сукупність матеріально-технічних, інформаційних, кадрових та організаційних ресурсів, що забезпечують виконання нотаріальних дій у встановленому законодавством порядку.

Для цілей даного дослідження нотаріальна контора розглядається як об’єкт інформаційної діяльності, тобто як система, в якій здійснюється збирання, накопичення, зберігання, обробка, передача та знищення інформації, що має різний ступінь конфіденційності та юридичну значущість.

Ключові особливості нотаріальної контори як об’єкта інформаційної діяльності:

1. Поєднання паперового та електронного документообігу. Нотаріальна діяльність передбачає одночасне введення як традиційних паперових нотаріальних справ так і електронних документів, які підписується кваліфікованим електронним підписом.
2. Інтеграція з державними електронними реєстрами. Нотаріус має доступ до Єдиного реєстру нотаріальних дій, Державного реєстру речових прав на нерухоме майно, Єдиного державного реєстру юридичних осіб, Спадкового реєстру та інших державних інформаційних систем.
3. Високий ступінь конфіденційності інформації. Відповідно до статті 8 Закону України «Про нотаріат», нотаріус зобов’язаний зберігати в таємниці відомості, які стали йому відомі у зв’язку з вчиненням нотаріальних дій. Порушення нотаріальної таємниці є злочином.

4. Використання засобів електронної ідентифікації. Кваліфікований електронний підпис нотаріуса є ключовим елементом доступу до державних реєстрів та засвідчення електронних документів.
5. Тривалі терміни зберігання інформації. Нотаріальні справи зберігаються протягом 75 років, що висуває особливі вимоги до довгострокового зберігання інформації як на паперових, так і на електронних носіях.

1.1.2 Технологія обробки інформації в нотаріальній конторі

Технологічний процес обробки інформації нотаріальній конторі можна представити у вигляді декількох взаємопов'язаних етапів. На етапі прийому та первинної обробки звернень клієнтів здійснюється ідентифікація клієнта, з'ясування предмета звернення, попереднє ознайомлення з документами. Інформація, що обробляється, включає персональні дані клієнта, відомості про предмет правочину, зміст документів. На етапі перевірки інформації в державних реєстрах нотаріус здійснює доступ до Єдиних та Державних реєстрів через спеціалізоване програмне забезпечення з використанням кваліфікованого електронного підпису (КЕП). Передача даних відбувається через мережу Інтернет, що створює додаткові ризики перехоплення або модифікації інформації. На етапі підготовки та оформлення документів нотаріус готує тексти нотаріальних документів, які містять конфіденційну інформацію. Цей етап включає роботу з текстовим редактором, системи електронного документообігу, а також використання спеціалізованого нотаріального програмного забезпечення. Етап вчинення нотаріальної дії та посвідчення документів є найбільш відповідальним, під час якого відбувається остаточне оформлення документа, його підписання сторонами та нотаріальне посвідчення; електронні документи підписується КЕП нотаріуса. На етапі реєстрації та архівування вчинені нотаріальні дії підлягають обов'язковій реєстрації в Єдиному реєстрі нотаріальних дій; паперові примірники документів формуються в нотаріальні справи та передаються до архіву; електронні копії документів зберігаються на електронних носіях. Завершальним етапом є видача документів клієнтам, на

якому клієнту передаються оформлені документи; у разі використання електронних документів, їх передачі може здійснюватися через не захищені канали зв’язку або на фізичних носіях.

Особливістю технології обробки інформації в нотаріальній конторі є під’єднання традиційного паперового документообігу з електронним. Це створює додаткові ризики, пов’язані з синхронізацію даних між паперовими та електронними носіями, а також з необхідністю забезпечення однакового рівня захисту для обох форм існування інформації.

1.1.3 Види інформації, що підлягають захисту

Відповідно до законодавства України та специфіки нотаріальної діяльності, до інформації, що підлягає захисту в нотаріальній конторі, належать декілька категорій.

Нотаріальна таємниця є фундаментальною категорією. Стаття 8 Закону України «Про нотаріат» встановлює, що нотаріус зобов’язаний зберігати в таємниці відомості, які стали йому відомі у зв’язку з вчиненням нотаріальних дій. Розголошення нотаріальної таємниці є порушенням закону та тягне за собою дисциплінарну, цивільно-правову та кримінальну відповідальність. Нотаріальна таємниця поширюється на зміст нотаріальних документів, відомості про осіб, які звернулися за вчиненням нотаріальних дій, відомості про майно, що є предметом правочинів, та іншу інформацію, отриману нотаріусом при виконанні професійних обов’язків.

Персональні дані є наступною важливою категорією. Нотаріальна контора є володільцем та розпорядником персональних даних клієнтів. Відповідно до Закону України «Про захист персональних даних» (з урахуванням тенденцій гармонізації з європейським законодавством, зокрема GDPR), нотаріус зобов’язаний забезпечити захист персональних даних від несанкціонованого доступу, витоку, знищення або модифікації. Перелік персональних даних, що обробляються нотаріусом, є надзвичайно широким і включає прізвище, ім’я, по батькові, дату та місце народження, місце проживання (перебування), реквізити

паспортного документа, реєстраційний номер облікової картки платника податків (РНОКПП) та інші відомості, що дозволяють ідентифікувати особу.

Конфіденційна інформація клієнтів також потребує захисту. Окрім персональних даних, нотаріус отримує доступ до інформації, яка становить комерційну або банківську таємницю клієнтів. Це можуть бути відомості про фінансовий стан, джерела походження коштів, структуру бізнесу, інтелектуальну власність тощо.

Інформація з обмеженим доступом, що міститься в державних реєстрах, також є об’єктом захисту. Доступ до державних реєстрів надає нотаріусу можливість отримувати інформацію, яка має обмежений доступ і не підлягає розголошенню третім особам. Нотаріус несе відповідальність за нерозголошення такої інформації.

Інформація про систему захисту інформації є конфіденційною. Відомості про організацію захисту інформації в нотаріальній конторі (політики безпеки, регламенти доступу, паролі, ключі шифрування) також потребують захисту, оскільки їх розкриття може сприяти реалізації загроз.

1.1.4 Фізичне середовище нотаріальної контори

Фізичне середовище нотаріальної контори є важливою складовою загальної системи захисту інформації. Відповідно до Положення про вимоги до робочого місця приватного нотаріуса, затвердженого наказом Міністерства юстиції України, робоче місце нотаріуса повинно забезпечувати належні умови для зберігання документів, нотаріальних справ та архіву, а також виключати можливість доступу сторонніх осіб до документів.

Приміщення контори повинно розташовуватися в окремому приміщенні, що виключає вільний доступ сторонніх осіб. Приміщення повинно мати надійні вхідні двері з замками, вікна з протизламними конструкціями, а також систему охоронної сигналізації. Робоча зона нотаріуса має бути організована таким чином, щоб унеможливити несанкціонований доступ до документів та технічних засобів під час відсутності нотаріуса; робочий стіл, шафи для зберігання

документів повинні замикатися. У разі використання власного серверного обладнання (наприклад, для зберігання електронного архіву), серверна зона повинна бути ізольована та мати обмежений доступ. Слід передбачити фізичний захист серверів від несанкціонованого доступу, а також забезпечити стабільне електроживлення та підтримання температурного режиму. Архівне приміщення, як місце зберігання нотаріальних справ, які містять інформацію з обмеженим доступом, повинно бути обладнане металевими шафами або сейфами, мати обмежений доступ, систему охоронної та протипожежної сигналізації. Термін зберігання нотаріальних справ становить 75 років, що висуває підвищені вимоги до довгострокової фізичної безпеки архівних документів.

1.1.5 Середовище користувачів

Людський фактор є одним з найбільш критичних елементів системи захисту інформації. Від обізнаності, кваліфікації та добросовісності персоналу нотаріальної контори безпосередньо залежить ефективність усіх заходів захисту.

Нотаріус є ключовою фігурою, яка несе повну відповідальність за захист інформації. Нотаріус є кінцевим користувачем більшості інформаційних систем, володіє ключами електронного підпису, має доступ до всіх реєстрів та конфіденційної інформації. Рівень його компетенції у питаннях інформаційної безпеки, дотримання правил безпечної роботи, здатність розпізнавати загрози (наприклад, спроби соціальної інженерії) є критичними факторами.

Помічники нотаріуса — це особи, які мають допуск до виконання окремих нотаріальних дій та, відповідно, до конфіденційної інформації. Вони працюють з програмним забезпеченням, готують проекти документів, взаємодіють з клієнтами. Рівень їхньої підготовки та добросовісності безпосередньо впливає на загальний рівень безпеки.

Технічний персонал включає системних адміністраторів, осіб, відповідальних за обслуговування комп’ютерної техніки, програмного забезпечення, засобів зв’язку. Технічний персонал має доступ до інфраструктури контори, що створює ризики зловживань або ненавмисного порушення безпеки.

Клієнти та інші відвідувачі, хоча і не є безпосередніми користувачами інформаційної системи нотаріальної контори, перебувають у приміщенні, можуть бачити екрани комп’ютерів, чути розмови, що створює ризики ненавмисного розголошення інформації. Крім того, клієнти можуть бути джерелом загроз (наприклад, спроби впливу на нотаріуса з метою отримання несанкціонованого доступу до інформації).

Аналіз середовища користувачів показує, що забезпечення інформаційної безпеки неможливе без систематичної роботи з персоналом. Це включає проведення навчань з інформаційної безпеки, ознайомлення з політиками безпеки, підписання зобов’язань про нерозголошення конфіденційної інформації, регулярне тестування на виявлення вразливостей, пов’язаних з людським фактором.

1.2 Проблематика дослідження та актуальність обраного напряму

1.2.1 Основна проблема дослідження

Сучасний етап розвитку суспільства характеризується стрімкою цифровізацією всіх сфер діяльності, включаючи нотаріат. Нотаріальна контора, яка традиційно асоціювалася з паперовим документообігом та фізичним зберіганням справ, сьогодні перетворюється на складний інформаційний центр, інтегрований у загальнодержавні електронні реєстри та системи. Цей процес, з одного боку, підвищує ефективність нотаріальної діяльності, а з іншого — створює нові, раніше невідомі загрози інформаційній безпеці.

Основна проблема, яка розглядається в даній роботі, полягає в наявності суперечності між зростаючою залежністю нотаріальної діяльності від інформаційно-комунікаційних технологій та державних електронних реєстрів, високою цінністю інформації, що обробляється (нотаріальна таємниця, персональні дані, комерційна таємниця клієнтів), підвищеними вимогами законодавства до захисту такої інформації та недостатнім рівнем впровадження системних підходів до управління інформаційною безпекою, зокрема управління ризиками, в практичній діяльності нотаріальних контор.

1.2.2 Актуальність напряму

Актуальність обраного напряму дослідження підтверджується декількома факторами. По-перше, спостерігається зростання кіберзагроз. За даними Державної служби спеціального зв'язку та захисту інформації України, кількість кіберінцидентів щорічно зростає. Нотаріальні контори, які володіють конфіденційною інформацією та мають доступ до державних реєстрів, стають привабливою ціллю для зловмисників. По-друге, відбувається посилення законодавчих вимог. Законодавство України, зокрема Закон «Про нотаріат», «Про захист персональних даних», «Про електронну ідентифікацію та електронні довірчі послуги», встановлює чіткі вимоги до захисту інформації, недотримання яких тягне за собою юридичну відповідальність. По-третє, практика показує відсутність системного підходу в багатьох нотаріальних конторах, де заходи захисту інформації впроваджуються фрагментарно, без системного аналізу ризиків та обґрунтування необхідності тих чи інших захисних механізмів. По-четверте, існує нагальна необхідність забезпечення безперервності діяльності, оскільки блокування доступу до державних реєстрів, компрометація ключів електронного підпису або знищення архівних даних можуть паралізувати роботу нотаріальної контори, що матиме серйозні наслідки як для самого нотаріуса, так і для клієнтів.

1.2.3 Основні проблеми інформаційної безпеки нотаріальних контор

На основі аналізу практики діяльності нотаріальних контор, а також з урахуванням специфіки їх функціонування, можна визначити ключові проблеми інформаційної безпеки.

Перша проблема — ідентифікація та автентифікація. Використання кваліфікованого електронного підпису створює ризики, пов'язані з компрометацією закритих ключів, несанкціонованим доступом до носіїв ключової інформації, а також з можливістю використання КЕП третіми особами.

Друга проблема — захист інформації в державних реєстрах. Доступ до державних реєстрів здійснюється через мережу Інтернет, що створює ризики

перехоплення даних, модифікації інформації, а також блокування доступу (DDoS-атаки, технічні збої).

Третя проблема — захист архівної інформації. Нотаріальні справи містять конфіденційну інформацію і підлягають зберіганню протягом 100 років. Забезпечення фізичного захисту паперових справ (пожежа, затоплення, несанкціонований доступ) та довгострокового зберігання електронних копій є складним завданням.

Четверта проблема — забезпечення безперервності діяльності. Відсутність резервних каналів доступу до державних реєстрів, неналежне резервне копіювання, відсутність планів відновлення після інцидентів можуть призвести до тривалої зупинки діяльності нотаріальної контори.

П’ята проблема — людський фактор. Недостатня обізнаність нотаріусів та їх помічників з питань кібербезпеки, низька культура безпеки, недотримання елементарних правил захисту інформації створюють значні вразливості, які можуть бути використані зловмисниками, зокрема методами соціальної інженерії.

Шоста проблема — відсутність системного підходу до управління ризиками. У багатьох нотаріальних конторах відсутній системний процес ідентифікації, аналізу та оцінки ризиків інформаційної безпеки. Заходи захисту впроваджуються безсистемно, що призводить або до надмірних витрат, або до недостатнього рівня захисту.

1.3 Аналіз нормативно-правової бази у сфері захисту інформації для нотаріальної контори

1.3.1 Загальне законодавство у сфері захисту інформації

Базові принципи захисту інформації в Україні закріплені в Конституції України. Стаття 31 Основного Закону гарантує таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції, а стаття 32 встановлює право на невтручання в особисте та сімейне життя. Ці конституційні положення створюють фундамент для всього подальшого законодавства у сфері захисту

інформації та є безпосередньо застосовними до діяльності нотаріуса, оскільки нотаріальна діяльність нерозривно пов'язана з обробкою інформації про особисте та сімейне життя громадян.

Закон України «Про інформацію» визначає правові засади інформаційної діяльності. Цей закон встановлює режими доступу до інформації, визначає види інформації з обмеженим доступом, до яких належать конфіденційна, таємна та службова інформація. Для нотаріальної діяльності принциповим є те, що нотаріальна таємниця, відповідно до цього закону, належить до конфіденційної інформації, що потребує спеціальних заходів захисту. Закон також встановлює, що доступ до конфіденційної інформації надається лише за згодою її власника або у випадках, передбачених законом, що створює правову основу для обмеження доступу до нотаріальних документів.

Закон України «Про захист персональних даних» (у новій редакції, що набрала чинності відповідно до Закону України № 2849-IX від 1 грудня 2022 року) встановлює вимоги до обробки персональних даних. Нотаріальна контора, як власник та розпорядник персональних даних клієнтів, зобов'язана забезпечити їх захист від несанкціонованого доступу, витоку, знищення або модифікації. Цей закон наближає українське законодавство до європейських стандартів, зокрема до Загального регламенту про захист даних (GDPR), та встановлює обов'язок повідомляти про порушення безпеки персональних даних. Для нотаріальної контори це означає необхідність наявності відповідних процедур виявлення та реагування на інциденти, а також ведення документації щодо обробки персональних даних.

Закон України «Про основні засади забезпечення кібербезпеки України» встановлює правові та організаційні засади забезпечення кібербезпеки. Хоча цей закон спрямований переважно на об'єкти критичної інформаційної інфраструктури, його положення щодо загальних принципів забезпечення кібербезпеки, реагування на кіберінциденти та обміну інформацією про загрози є важливими для будь-якого суб'єкта інформаційної діяльності, включаючи

нотаріальні контори. Нотаріус, який має доступ до державних реєстрів через мережу Інтернет, повинен розуміти свою роль у забезпеченні кібербезпеки та дотримуватися відповідних вимог, зокрема щодо захисту власної інформаційної інфраструктури.

Закон України «Про електронну ідентифікацію та електронні довірчі послуги» є найбільш важливим для нотаріальної діяльності в контексті цифровізації. Цей закон регулює використання кваліфікованого електронного підпису (КЕП) для доступу до державних реєстрів та посвідчення електронних документів. Він визначає вимоги до засобів електронної ідентифікації, порядок надання довірчих послуг, а також правові наслідки використання електронних підписів. Для нотаріуса дотримання вимог цього закону є критичним, оскільки саме КЕП забезпечує юридичну значущість електронних документів та можливість доступу до державних реєстрів. Компрометація закритих ключів нотаріуса або порушення правил їх зберігання можуть призвести до серйозних юридичних наслідків, включаючи визнання електронних документів недійсними.

1.3.2 Галузеве законодавство: Закон України «Про нотаріат»

Закон України «Про нотаріат» є базовим галузевим законом, який встановлює основи організації нотаріальної діяльності. У контексті захисту інформації особливе значення мають кілька його статей, які безпосередньо впливають на формування вимог до системи управління інформаційною безпекою.

Стаття 8 «Нотаріальна таємниця» є фундаментальною для визначення обсягу інформації, що підлягає захисту. Ця стаття встановлює, що нотаріус зобов’язаний зберігати в таємниці відомості, які стали йому відомі у зв’язку з вчиненням нотаріальних дій. Розголошення нотаріальної таємниці є порушенням закону та тягне за собою дисциплінарну, цивільно-правову та кримінальну відповідальність. Для цілей управління ризиками це означає, що нотаріальна таємниця має найвищу цінність серед усіх активів, що захищаються, а будь-який

ризик її розголошення має розглядатися як неприйнятний. Стаття також визначає випадки, коли нотаріус може надавати інформацію, що становить нотаріальну таємницю (за запитом суду, правоохоронних органів тощо), що вимагає наявності процедур контролю за такими запитами.

Стаття 2-1 «Контроль за організацією нотаріальної діяльності» визначає повноваження Міністерства юстиції України та його територіальних органів щодо контролю за дотриманням порядку вчинення нотаріальних дій та виконанням правил нотаріального діловодства. Це положення створює нормативну основу для державного нагляду за захистом інформації в нотаріальних конторах. Міністерство юстиції має право проводити перевірки, у тому числі з питань захисту інформації, що вимагає від нотаріуса здатності продемонструвати відповідність встановленим вимогам. Для СУІБ це означає необхідність ведення документації, що підтверджує виконання вимог законодавства, а також готовність до проведення перевірок.

Стаття 43 «Вимоги до робочого місця (контори) приватного нотаріуса» встановлює, що робоче місце приватного нотаріуса повинно відповідати вимогам, затвердженим Міністерством юстиції України. Ці вимоги стосуються організації зберігання документів, забезпечення нерозголошення відомостей, що становлять нотаріальну таємницю, а також фізичного захисту приміщення. Виконання цих вимог є обов’язковим і має бути враховане при розробці заходів захисту інформації. Крім того, ця стаття надає Міністерству юстиції повноваження встановлювати додаткові вимоги до організації роботи нотаріуса, що створює динамічне нормативне середовище, яке потребує постійного моніторингу.

1.3.3 Підзаконні нормативно-правові акти

Деталізація вимог до захисту інформації в нотаріальній діяльності здійснюється на рівні підзаконних актів, які затверджуються Міністерством юстиції України та іншими уповноваженими органами.

Положення про вимоги до робочого місця (контори) приватного нотаріуса та здійснення контролю за організацією нотаріальної діяльності, затверджене наказом Міністерства юстиції України, встановлює конкретні вимоги до організації робочого місця. До них належать: наявність окремого приміщення, яке виключає вільний доступ сторонніх осіб; наявність сейфів або металевих шаф для зберігання документів, нотаріальних справ та архіву; забезпечення фізичної безпеки приміщення (охоронна сигналізація, засоби пожежогасіння); порядок допуску осіб до приміщення контори, включаючи ведення журналу відвідувачів. Цей документ також встановлює порядок здійснення контролю за організацією нотаріальної діяльності, включаючи періодичність та процедуру проведення перевірок.

Порядок вчинення нотаріальних дій нотаріусами України містить вимоги до оформлення нотаріальних документів, у тому числі електронних. Цей документ визначає порядок посвідчення електронних документів, вимоги до їх форми та змісту, а також порядок зберігання електронних документів. Для захисту інформації важливим є те, що Порядок встановлює вимоги до використання кваліфікованого електронного підпису нотаріуса, а також до забезпечення цілісності та автентичності електронних документів.

Правила ведення нотаріального діловодства встановлюють порядок формування, обліку та зберігання нотаріальних справ. Цей документ визначає, які документи підлягають включенню до нотаріальної справи, порядок їх формування, нумерації, прошивки та опечатування. Для захисту інформації важливими є вимоги щодо зберігання нотаріальних справ (у сейфах або металевих шафах), порядку видачі справ для ознайомлення, а також процедури знищення справ після закінчення строку зберігання.

Нормативні акти з технічного захисту інформації, які затверджуються Міністерством юстиції України спільно з Адміністрацією Державної служби спеціального зв’язку та захисту інформації України, встановлюють вимоги до технічного захисту інформації в інформаційних системах, що використовуються

для доступу до державних реєстрів. Ці акти визначають вимоги до засобів криптографічного захисту інформації, порядку їх застосування, а також вимоги до захисту інформації під час її передачі каналами зв'язку. Для нотаріальної контори це означає необхідність використання сертифікованих засобів технічного захисту інформації та дотримання встановлених правил їх експлуатації.

1.3.4 Зацікавлені сторони системи управління інформаційною безпекою нотаріальної контори

Аналіз нормативно-правової бази дозволяє визначити коло зацікавлених сторін, чиї вимоги та очікування мають бути враховані при побудові системи управління інформаційною безпекою нотаріальної контори. Відповідно до вимог ДСТУ ISO/IEC 27001, розуміння потреб та очікувань зацікавлених сторін є необхідною умовою визначення контексту організації.

Клієнти (суб'єкти персональних даних) є найважливішою зацікавленою стороною. Вони очікують забезпечення конфіденційності наданої інформації, захисту персональних даних, збереження нотаріальної таємниці. Клієнти мають право знати, яка інформація про них збирається, з якою метою та як захищається. Відповідно до законодавства про захист персональних даних, клієнти мають право на доступ до своїх даних, їх виправлення, а також на припинення обробки. Недотримання цих прав може призвести до скарг, судових позовів та репутаційних втрат.

Міністерство юстиції України є головним регулятором нотаріальної діяльності. Воно встановлює вимоги до організації нотаріальної діяльності, здійснює контроль за їх дотриманням, має право проводити перевірки, у тому числі з питань захисту інформації. Міністерство юстиції також затверджує підзаконні акти, які деталізують вимоги до захисту інформації. Очікування цієї сторони полягають у дотриманні нотаріусом усіх встановлених вимог, готовності до перевірок та наданні необхідної інформації.

Технічні адміністратори державних реєстрів (ДП «НАІС») відповідають за функціонування державних інформаційних систем, з якими взаємодіє нотаріальна контора. Вони встановлюють технічні вимоги до підключення та роботи з реєстрами, забезпечують захист інформації на рівні централізованих ресурсів. Очікування цієї сторони включають дотримання технічних умов підключення, використання сертифікованих засобів захисту інформації, своєчасне оновлення програмного забезпечення, а також взаємодію у разі виникнення інцидентів.

Постачальники програмного забезпечення є важливою зацікавленою стороною, оскільки від якості їх продуктів залежить рівень захисту інформації. Це розробники та постачальники спеціалізованого нотаріального програмного забезпечення, систем електронного документообігу, засобів криптографічного захисту інформації. Очікування нотаріальної контори до постачальників включають надання якісного, безпечного програмного забезпечення, своєчасне оновлення та усунення вразливостей, технічну підтримку.

Кваліфіковані надавачі електронних довірчих послуг забезпечують функціонування інфраструктури електронного підпису. Від стабільності та безпеки їх послуг залежить можливість доступу до державних реєстрів та юридична значущість електронних документів. Очікування нотаріальної контори до надавачів включають надійність, безперервність надання послуг, захист ключової інформації, а також оперативне реагування у разі компрометації.

Співробітники нотаріальної контори (помічники, технічний персонал) є внутрішніми зацікавленими сторонами. Їх обізнаність, кваліфікація та добросовісність безпосередньо впливають на рівень захисту інформації. Вони очікують чітких правил роботи, навчання, а також розуміння своєї відповідальності за захист інформації.

1.4 Аналіз існуючих підходів до управління ризиками інформаційної безпеки

1.4.1 Огляд міжнародних стандартів

Методологічним підґрунтям для розбудови ефективної системи управління інформаційною безпекою (СУІБ) в нотаріальній конторі слугує комплекс міжнародних стандартів серії ISO/EC 27000, адаптованих в Україні як національні ДСТУ.

ДСТУ ISO/IEC 27001 є базовим стандартом, який встановлює вимоги до СУІБ. Він визначає модель системи, заснованої на процесному підході та циклі Демінга (PDCA: Plan-Do-Check-Act). Стандарт містить вимоги до контексту організації, лідерства, планування (включаючи управління ризиками), підтримки, операційної діяльності, оцінювання результатів діяльності та вдосконалення.

ДСТУ ISO/IEC 27002 виступає практичним довідником найкращих світових практик. Він надає детальні рекомендації щодо вибору та впровадження заходів безпеки (контролів) для забезпечення інформаційної безпеки. Ці заходи охоплюють політики інформаційної безпеки, організацію інформаційної безпеки, безпеку персоналу, управління активами, контроль доступу, криптографію, фізичну безпеку, безпеку експлуатації, безпеку комунікацій, розробку та супроводження систем, відносини з постачальниками, управління інцидентами, управління безперервністю та відповідність вимогам.

ДСТУ ISO/IEC 27005 є ключовим стандартом для управління ризиками інформаційної безпеки. Він надає системний підхід до ідентифікації, аналізу, оцінки та обробки ризиків. Стандарт встановлює загальну структуру процесу управління ризиками, яка включає встановлення контексту (визначення критеріїв прийнятності ризику, обсягу та меж процесу), оцінювання ризиків (ідентифікація ризиків: визначення активів, загроз, вразливостей та існуючих заходів контролю; аналіз ризиків: оцінка ймовірності реалізації загрози та потенційних наслідків; оцінка ризиків: порівняння рівнів ризиків з критеріями прийнятності), обробку ризиків (вибір та впровадження заходів для зменшення, уникнення, передачі або прийняття ризиків), прийняття ризиків (формальне

затвердження залишкових ризиків керівництвом), моніторинг та аналіз (постійне спостереження за ризиками та ефективністю заходів), комунікацію та консультування (обмін інформацією про ризики між зацікавленими сторонами). Особливістю ISO/IEC 27005 є його гнучкість: він не нав'язує конкретних методів оцінки ризиків, а надає методологічну основу, яка може бути адаптована до потреб будь-якої організації, включаючи нотаріальну контору.

Стандарти Національного інституту стандартів і технологій США (NIST), хоча не є обов'язковими в Україні, є цінним методичним ресурсом, оскільки пропонують деталізовані процедури. Зокрема, NIST SP 800-39 визначає інтегрований підхід до управління ризиками інформаційної безпеки на рівні всієї організації, NIST SP 800-30 містить детальні керівництва з проведення оцінки ризиків, включаючи конкретні методики ідентифікації загроз та вразливостей, а NIST SP 800-37 регламентує процедури впровадження захисних механізмів та їх моніторингу.

IEC 31010:2019 (Методи оцінювання ризиків) є допоміжним стандартом для ISO/IEC 27005 та ISO 31000. Він містить широкий спектр інструментів для оцінювання ризиків, таких як аналіз «мозкового штурму», метод Дельфі, аналіз «дерева подій» (ETA), аналіз «дерева відмов» (FTA), аналіз видів та наслідків відмов (FMEA), аналіз сценаріїв, аналіз впливу на бізнес (BIA).

1.4.2 Порівняльний аналіз підходів

Методи оцінювання ризиків, передбачені стандартами, можна розділити на три основні категорії.

Якісний підхід заснований на експертних оцінках та використанні порядкових шкал (наприклад, «високий», «середній», «низький»). Ймовірність та наслідки визначаються не в числових значеннях, а в категоріях. Цей підхід є найбільш поширеним у практиці управління ризиками завдяки своїй простоті та зрозумілості. Він не вимагає складних розрахунків та великих обсягів статистичних даних. Основним недоліком є високий рівень суб'єктивності.

Кількісний підхід заснований на використанні числових значень для оцінки ймовірності та наслідків. Ймовірність реалізації загрози виражається у відсотках або частоті, наслідки — у грошовому вимірі. Кількісний підхід дозволяє отримати більш об’єктивні результати, обґрунтувати економічну доцільність впровадження заходів захисту (співвідношення вартості захисту та потенційних збитків). Однак він потребує значних зусиль для збору даних, наявності статистики інцидентів та високої - кваліфікації персоналу.

Комбінований (напівкількісний) підхід поєднує елементи якісного та кількісного підходів. Як і в якісному підході, використовуються категорії, але кожній категорії присвоюються числові значення (наприклад, «високий» = 3, «середній» = 2, «низький» = 1). Це дозволяє здійснювати математичні операції (наприклад, перемножувати бали для отримання числового значення ризику) та ранжувати ризики, зберігаючи при цьому відносну простоту застосування.

1.4.3 Визначення прийнятної методики для нотаріальної контори

Враховуючи специфіку діяльності нотаріальної контори (невеликий колектив, обмежені ресурси, висока цінність інформації, що захищається), доцільно обрати методику управління ризиками, засновану на ДСТУ ISO/IEC 27005 з використанням комбінованого (напівкількісного) підходу.

Така методика повинна включати наступні етапи. Встановлення контексту передбачає визначення меж СУІБ (вся діяльність нотаріальної контори), визначення критеріїв прийнятності ризику (наприклад, ризики, що загрожують безперервності нотаріальної діяльності або можуть призвести до розголошення нотаріальної таємниці, є неприйнятними) та визначення шкал оцінювання (шкала ймовірності від 1 (малоймовірно) до 5 (дуже ймовірно); шкала наслідків від 1 (незначні) до 5 (катастрофічні), де наслідки можуть оцінюватися за різними критеріями: фінансові втрати, репутаційні втрати, порушення законодавства, припинення діяльності).

Ідентифікація ризиків передбачає складання реєстру активів (інформаційних, апаратних, програмних, людських, сервісних) з визначенням їх

цінності, ідентифікацію актуальних загроз для кожного активу, виявлення вразливостей, які можуть бути використані для реалізації загроз, та визначення існуючих заходів контролю.

Аналіз та оцінювання ризиків полягає в тому, що для кожної пари «загроза-актив-вразливість» визначається рівень ризику як добуток (або інша функція) значення ймовірності та значення наслідків, отримані рівні ризиків порівнюються з критеріями прийнятності, та визначаються пріоритетні ризики, що потребують обробки.

Обробка ризиків передбачає для кожного ризику вибір стратегії: зменшення (впровадження додаткових заходів), уникнення (зміна діяльності), передача (страхування), прийняття (документування), а також розробку плану обробки ризиків.

Моніторинг та перегляд встановлюють періодичність переоцінки ризиків (наприклад, щорічно, а також при зміні законодавства, технологій або структури діяльності).

Така методика дозволить нотаріальній конторі створити адаптивну та адекватну реальним викликам систему управління інформаційною безпекою.

1.5 Управління ризиками як основа системи управління інформаційною безпекою

1.5.1 Сутність управління ризиками інформаційної безпеки

Управління ризиками є центральним елементом будь-якої сучасної системи управління інформаційною безпекою. Саме через управління ризиками забезпечується пропорційність витрат на захист цінності активів, що захищаються, та досягається баланс між потребою в безпеці та операційною ефективністю діяльності. Відповідно до ДСТУ ISO/IEC 27001, вимоги до СУІБ базуються на систематичному підході до управління ризиками, який охоплює всі аспекти діяльності організації.

Управління ризиками інформаційної безпеки (Information Security Risk Management) - це систематичний процес ідентифікації, аналізу, оцінювання,

обробки, моніторингу та перегляду ризиків, пов’язаних із забезпеченням конфіденційності, цілісності та доступності інформації. Метою управління ризиками є не повне усунення всіх ризиків (що є практично неможливим та економічно недоцільним), а приведення їх до прийнятного рівня з урахуванням потреб та ресурсних обмежень організації.

Для нотаріальної контори управління ризиками набуває особливого значення з огляду на кілька факторів. По-перше, нотаріальна контора обробляє інформацію винятково високої цінності (нотаріальна таємниця, персональні дані), компрометація якої може мати катастрофічні наслідки. По-друге, нотаріальна контора, як правило, є невеликим підприємством з обмеженими ресурсами, що не може дозволити собі впровадження всіх можливих заходів захисту без обґрунтування їх доцільності. По-третє, законодавство прямо вимагає від нотаріуса вжиття заходів для захисту інформації, але не визначає конкретний перелік таких заходів, залишаючи нотаріусу право вибору на основі аналізу ризиків.

1.5.2 Нормативно-правове закріплення управління ризиками

Вимога щодо управління ризиками в контексті захисту інформації закріплена в кількох нормативно-правових актах. Закон України «Про захист персональних даних» вимагає від власника персональних даних вживати організаційних та технічних заходів, необхідних для захисту персональних даних від несанкціонованого доступу, що передбачає попередній аналіз ризиків для визначення адекватності таких заходів. Закон України «Про основні засади забезпечення кібербезпеки України» визначає управління ризиками як один з основних принципів забезпечення кібербезпеки. На міжнародному рівні ДСТУ ISO/EC 27001 прямо вимагає, щоб організація визначила та застосовувала процес управління ризиками інформаційної безпеки.

1.5.3 Структура процесу управління ризиками

Відповідно до ДСТУ ISO/EC 27005, процес управління ризиками включає шість основних етапів, кожен з яких має своє значення для нотаріальної контори.

Перший етап — встановлення контексту. На цьому етапі визначаються межі СУІБ, критерії прийнятності ризику, а також основні принципи, якими керуватиметься нотаріус при прийнятті рішень щодо захисту інформації. Важливим є визначення того, які ризики є неприйнятними (наприклад, ті, що загрожують розголошенню нотаріальної таємниці або блокуванню доступу до державних реєстрів), а які можуть бути прийняті.

Другий етап — ідентифікація ризиків. На цьому етапі здійснюється визначення активів нотаріальної контори (інформаційних, апаратних, програмних, людських), оцінка їх цінності, ідентифікація актуальних загроз для кожного активу, виявлення вразливостей, які можуть бути використані для реалізації загроз, а також визначення існуючих заходів контролю. Для нотаріальної контори ключовими активами є нотаріальна таємниця, кваліфікований електронний підпис, доступ до державних реєстрів, архівні справи.

Третій етап — аналіз ризиків. На цьому етапі оцінюється ймовірність реалізації кожної загрози та потенційні наслідки для нотаріальної контори. Для цього можуть застосовуватися різні методи: якісні (використання категорій «високий», «середній», «низький»), кількісні (числові значення ймовірності та збитків) або комбіновані. Для нотаріальної контори найбільш доцільним є комбінований підхід, який дозволяє отримати наочні результати без складних розрахунків.

Четвертий етап — оцінка ризиків. На цьому етапі отримані рівні ризиків порівнюються з критеріями прийнятності, визначеними на етапі встановлення контексту. Ризики, що перевищують прийнятний рівень, потребують обробки. Ризики, що знаходяться в межах прийнятного рівня, можуть бути прийняті без додаткових заходів.

П’ятий етап — обробка ризиків. На цьому етапі для кожного неприйнятного ризику обирається стратегія обробки: зменшення (впровадження додаткових заходів захисту), уникнення (зміна діяльності, наприклад, відмова

від певної операції), передача (страхування ризику) або прийняття (документування свідомого рішення прийняти ризик). Для нотаріальної контори найбільш поширеною стратегією є зменшення ризиків шляхом впровадження організаційно-технічних заходів.

Шостий етап — моніторинг та перегляд. Управління ризиками не є одноразовою дією, а постійним процесом. Ризики змінюються з часом — з'являються нові загрози, змінюється законодавство, впроваджуються нові технології. Тому нотаріальна контора повинна регулярно (наприклад, щорічно) переглядати та актуалізувати оцінку ризиків, а також проводити позапланову переоцінку у разі суттєвих змін (оновлення програмного забезпечення, зміна персоналу, нові вимоги законодавства).

1.5.4 Документування процесу управління ризиками

Відповідно до вимог ДСТУ ISO/IEC 27001, результати управління ризиками підлягають документуванню. Для нотаріальної контори рекомендовано вести наступні документи: реєстр активів (перелік усіх активів з визначенням їх цінності), реєстр загроз та вразливостей, методику оцінювання ризиків (з описом шкал та процедур), матрицю ризиків, план обробки ризиків (з переліком заходів, термінами та відповідальними), а також протоколи прийняття ризиків (для ризиків, які вирішено прийняти без додаткової обробки).

1.5.5 Зв'язок управління ризиками з іншими елементами СУІБ

Управління ризиками є не ізольованим процесом, а основою, на якій будується вся система управління інформаційною безпекою.

Результати оцінки ризиків визначають необхідність впровадження конкретних заходів контролю (згідно з ДСТУ ISO/IEC 27002), пріоритетність їх впровадження, обсяг ресурсів, що виділяються на захист, а також цілі інформаційної безпеки та критерії їх досягнення. Крім того, управління ризиками тісно пов'язане з управлінням інцидентами (аналіз інцидентів дозволяє виявити нові ризики) та управлінням безперервністю діяльності (оцінка ризиків

є основою для визначення допустимого часу простою та необхідних заходів для забезпечення безперервності).

Таким чином, управління ризиками є не просто однією з функцій СУІБ, а її методологічним підґрунтям, яке забезпечує обґрунтованість, ефективність та пропорційність усіх заходів захисту інформації в нотаріальній конторі. Саме на цьому процесі буде зосереджено основну увагу в наступних розділах дипломної роботи, де буде проведено практичну ідентифікацію активів, загроз та вразливостей для типової нотаріальної контори, здійснено оцінювання ризиків та запропоновано заходи їх обробки.

1.6 Висновок до розділу 1

У першому розділі «Аналіз предметної області та нормативно-правове регулювання управління ризиками інформаційної безпеки нотаріальної контори» проведено аналіз предметної області, нормативно-правової бази та існуючих підходів до управління ризиками інформаційної безпеки нотаріальної контори. Своєчасність дослідження обумовлена інтенсивним впровадженням інформаційних технологій в нотаріальну діяльність та недостатнім рівнем захищеності нотаріальних контор від сучасних кіберзагроз.

Нотаріальна контора як об’єкт інформаційної діяльності характеризується високою цінністю інформації, що обробляється (нотаріальна таємниця, персональні дані), інтеграцією з державними електронними реєстрами та тривалими термінами зберігання даних. Ключовими проблемами інформаційної безпеки є захист кваліфікованого електронного підпису, захист інформації в реєстрах, забезпечення безперервності діяльності, людський фактор та відсутність системного управління ризиками.

Аналіз нормативно-правової бази показав, що діяльність нотаріуса регулюється комплексом актів: загальним законодавством (Конституція України, Закони «Про інформацію», «Про захист персональних даних», «Про електронну ідентифікацію та електронні довірчі послуги»), галузевим законодавством (Закон України «Про нотаріат») та підзаконними актами

(Положення про вимоги до робочого місця приватного нотаріус, Порядок вчинення нотаріальних дій). Визначено зацікавлені сторони СУІБ нотаріальної контори: клієнти, Міністерство юстиції України, технічні адміністратори державних реєстрів, постачальники програмного забезпечення та надавачі електронних довірчих послуг.

Методологічну основу управління ризиками складають стандарти серії ISO/IEC 27000. Порівняльний аналіз підходів до оцінювання ризиків показав, що для нотаріальної контори найбільш доцільним є комбінований (напівкількісний) підхід, який забезпечує необхідну точність при простоті реалізації.

В рамках дипломного проекту пропонується адаптувати методологію ДСТУ ISO/IEC 27005 до специфіки нотаріальної контори із застосуванням комбінованого підходу. Основний фокус дослідження зосереджено на етапі оцінювання ризиків.

Таким чином, проведений аналіз створив підґрунтя для подальшого дослідження. У другому розділі буде проведено практичну ідентифікацію активів, загроз та вразливостей, а також здійснено оцінювання ризиків для типової нотаріальної контори.

2. ІДЕНТИФІКАЦІЯ АКТИВІВ, ЗАГРОЗ, ВРАЗЛИВОСТЕЙ ТА ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НОТАРІАЛЬНОЇ КОНТОРИ

2.1. Встановлення контексту оцінювання ризиків

Першим етапом процесу оцінювання ризиків є встановлення контексту. На цьому етапі визначаються межі системи управління інформаційною безпекою (СУІБ), критерії прийнятності ризиків, а також шкали для оцінювання ймовірності та наслідків. Від правильності встановлення контексту залежить об’єктивність усіх подальших результатів, оскільки саме тут задаються правила, за якими оцінюватимуться ризики.

Межі СУІБ для нотаріальної контори охоплюють усі процеси, пов’язані зі збиранням, накопиченням, зберіганням, обробкою, передачею та знищенням інформації, що становить нотаріальну таємницю або є персональними даними клієнтів. До сфери оцінювання ризиків включено всі активи, які будуть ідентифіковані в наступному підрозділі, а також усі співробітники нотаріальної контори: нотаріус, помічники нотаріуса та технічний персонал (системний адміністратор). Зовнішніми системами, які впливають на ризики, є державні електронні реєстри (Єдиний реєстр нотаріальних дій, Державний реєстр речових прав на нерухоме майно, Єдиний державний реєстр юридичних осіб, Спадковий реєстр), мережа Інтернет, кваліфіковані надавачі електронних довірчих послуг, а також постачальники програмного забезпечення.

Критерії прийнятності ризику визначаються виходячи з вимог законодавства, цінності активів та ресурсних обмежень нотаріальної контори. Розголошення нотаріальної таємниці є неприйнятним за будь-яких обставин, оскільки це прямо заборонено статтею 8 Закону України «Про нотаріат» і тягне за собою кримінальну відповідальність. Компрометація кваліфікованого електронного підпису (КЕП) нотаріуса є неприйнятною, оскільки це ставить під сумнів юридичну значущість усіх електронних документів, посвідчених нотаріусом. Блокування доступу до державних реєстрів на термін більше ніж

один робочий день є неприйнятним, оскільки це унеможливлює виконання нотаріальних дій.

Втрата нотаріальних справ (паперових або електронних) є неприйнятною, оскільки термін їх зберігання становить 75 років і відновити такі документи неможливо.

Фінансові втрати загальним обсягом понад 100 000 гривень внаслідок реалізації одного ризику вважаються неприйнятними, оскільки це може призвести до банкрутства малої нотаріальної контори. Усі інші ризики, які не досягають зазначених порогових значень, підлягають обробці (зменшенню, передачі або прийняттю) залежно від їх рівня та пріоритетності.

Для оцінювання ризиків обрано комбінований (напівкількісний) підхід, який передбачає використання п’ятибальних шкал для оцінювання ймовірності реалізації загрози та наслідків (табл. 2.1). Рівень ризику розраховується як добуток ймовірності та наслідків, що дає значення в діапазоні від 1 до 25. На основі отриманого числового значення ризики класифікуються за чотирма категоріями: неприйнятні (рівень ризику 20-25) потребують негайної обробки; високі (рівень ризику 15-19) потребують обробки в пріоритетному порядку; середні (рівень ризику 8-14) потребують обробки в плановому порядку; низькі (рівень ризику 1-7) можуть бути прийняті без додаткової обробки.

Таблиця 2.1 — Шкали оцінювання ймовірності та наслідків

Рівень	Назва	Ймовірність (частота реалізації)	Наслідки (фінансові втрати / репутація / законодавство / припинення діяльності)
1	Дуже низький	Раз на 5 років або рідше	до 1000 грн / незначний вплив / відсутність / до 1 год
2	Низький	Раз на рік або рідше	1000-10000 грн / локальний вплив / незначне порушення / до 4 год
3	Середній	Раз на півроку або рідше	10000-50000 грн / тимчасовий вплив / штраф / до 1 дня

Продовження таблиці 2.1

4	Високий	Раз на місяць або рідше	50000-100000 грн / довготривалий вплив / кримінальна відповідальність / до 1 тижня
5	Дуже високий	Частіше ніж раз на місяць	понад 100000 грн / втрата довіри, закриття бізнесу / кримінальна відповідальність / більше 1 тижня

2.2 Ідентифікація та ранжування активів нотаріальної контори

Ідентифікація активів є першим кроком безпосереднього оцінювання ризиків. Активом вважається все, що має цінність для нотаріальної контори та потребує захисту. У ході дослідження було ідентифіковано шість категорій активів: інформаційні, апаратні, програмні, людські, сервісні та фізичні (табл 2.2).

До інформаційних активів належать нотаріальна таємниця (зміст документів, відомості про клієнтів, відомості про майно), персональні дані клієнтів, нотаріальні справи (паперовий архів), електронний архів нотаріальних документів, ключі кваліфікованого електронного підпису, паролі доступу до державних реєстрів, внутрішні політики та інструкції, фінансові документи, а також інформація про систему захисту.

До апаратних активів належать робочий комп’ютер нотаріуса, робочі комп’ютери помічників, ноутбук, носії ключової інформації (токени, смарт-карти), мережеве обладнання (роутер, комутатор), принтер/сканер/БФП, зовнішні накопичувачі (USB-диски).

До програмних активів належать операційна система, спеціалізоване нотаріальне програмне забезпечення, засоби криптографічного захисту, система електронного документообігу, антивірусне програмне забезпечення, офісний пакет та веб-браузер.

До людських активів належать нотаріус (ключова особа, яка несе повну відповідальність за захист інформації, має доступ до всіх активів, володіє КЕП), помічник нотаріуса (особа, яка має допуск до конфіденційної інформації, готує проекти документів, взаємодіє з клієнтами), системний адміністратор (технічний персонал, який має доступ до всієї інфраструктури), а також клієнти (відвідувачі), які можуть ненавмисно розголосити конфіденційну інформацію.

До сервісних активів належать доступ до державних реєстрів (Єдиного реєстру нотаріальних дій, Державного реєстру речових прав, Єдиного державного реєстру юридичних осіб, Спадкового реєстру), доступ до мережі Інтернет, електропостачання, послуги кваліфікованого надавача електронних довірчих послуг, технічна підтримка ПЗ, а також послуги з фізичної охорони приміщення.

До фізичних активів належать приміщення нотаріальної контори, архівне приміщення, серверна кімната (за наявності), а також сейфи та металеві шафи.

Таблиця 2.2 — Ідентифікація активів

ID	Назва	Опис	Тип активу
1	БФП	Пристрій для друку та сканування нотаріальних документів	Апаратний
2	Робочий ПК нотаріуса	Персональний комп'ютер нотаріуса з доступом до державних реєстрів та нотаріальних документів	Апаратний
3	Робочий ПК помічника	Комп'ютер помічника нотаріуса, які використовуються для підготовки документів	Апаратний
4	Засоби криптографічного захисту (агент підпису)	Програмне забезпечення для роботи з КЕП, шифрування даних	Програмний
5	Антивірусне ПЗ	Програми для захисту від шкідливого програмного забезпечення	Програмний
6	Операційна система (Windows)	Базова операційна система на робочих комп'ютерах та сервері	Програмний

Продовження таблиці 2.2

7	Ноутбук	Ноутбук нотаріуса, для виїзду до клієнта додому	Апаратний
8	Пакети Microsoft Office	ПЗ для створення та редагування текстових документів, таблиць	Програмний
9	Персональні дані клієнтів	Дані, що дозволяють ідентифікувати особу (паспортні дані, РНОКПП, місце проживання	Інформаційний
10	Нотаріальна таємниця	Відомості, що стали відомі нотаріусу у зв'язку з вчиненням нотаріальних дій	Інформаційний
11	Електронний архів	Електронні копії нотаріальних документів, підписані КЕП	Інформаційний
12	Ключі КЕП	Закриті ключі КЕП нотаріуса на захищених носіях (токенах)	Інформаційний
13	Паролі доступу до держ. реєстрів	Облікові дані для входу до Єдиного реєстру нотаріальних дій, Державного реєстру речових прав тощо	Інформаційний
14	Фінансові документи	Договори про оплату послуг, квитанції, звітність	Інформаційний
15	Роутер	Пристрій для забезпечення доступу до мережі Інтернет та локальної мережі	Апаратний
16	Токен	Апаратний засіб захисту, що містить закриті ключі КЕП нотаріуса	Апаратний
17	Веб-браузер	Програма для доступу до веб-інтерфейсів державних реєстрів	Програмний
18	Нотаріус	Ключова особа, яка несе повну відповідальність за захист інформації, має доступ до всіх активів, володіє КЕП	Людський
19	Помічник нотаріуса	Особа, яка має допуск до конфіденційної інформації, готує проекти документів, взаємодіє з клієнтами	Людський

Продовження таблиці 2.2

20	Технічний персонал	Особа, відповідальна за налаштування та обслуговування апаратних та програмних засобів, має доступ до всієї інфраструктури	Людський
21	Клієнти	Особи, які надають конфіденційну інформацію, можуть ненавмисно розголосити дані або стати жертвами соціальної інженерії	Людський
22	Доступ до Єдиного реєстру нотаріальних дій	Можливість реєстрації вчинених нотаріальних дій	Сервісний
23	Доступ до Державного реєстру речових прав на нерухоме майно	Можливість перевірки інформації про нерухоме майно та обтяжень	Сервісний
24	Доступ до Єдиного державного реєстру юридичних осіб	Можливість перевірки відомостей про юридичних осіб та ФОП	Сервісний
25	Доступ до Спадкового реєстру	Можливість перевірки наявності заповітів та спадкових справ	Сервісний
26	Доступ до мережі Інтернет	Забезпечення підключення до державних реєстрів та інших онлайн-сервісів	Сервісний
27	Електропостачання	Безперебійне забезпечення електроенергією апаратних засобів	Сервісний
28	Послуги кваліфікованого надавача електронних довірчих послуг	Обслуговування інфраструктури КЕП, видача сертифікатів, підтримка	Сервісний
29	Послуги з фізичної охорони приміщення	Охоронна сигналізація, пультова охорона, контроль доступу	Сервісний
30	Приміщення нотаріальної контори	Робоче приміщення, де знаходяться робочі місця, обладнання, документи	Фізичний
31	Архівне приміщення	Окреме приміщення для зберігання нотаріальних справ	Фізичний

Продовження таблиці 2.2

32	Сейф	Засіб для зберігання нотаріальних справ, документів, носіїв ключової інформації	Фізичний
33	Зовнішні накопичувачі	Портативні накопичувачі для резервного копіювання або передачі даних	Апаратний

У ході дослідження з загального переліку активів, який налічував 33 позиції, було відібрано вісім найбільш критичних об’єктів, що безпосередньо впливають на виконання нотаріальних дій, зберігання конфіденційної інформації та дотримання вимог законодавства. До відібраних активів належать: критичні бази даних (електронний архів нотаріальних документів), паперовий архів (нотаріальні справи), ключі КЕП та токен (носій кваліфікованого електронного підпису), нотаріальна таємниця, доступ до державних реєстрів, персональні дані клієнтів, робочий персональний комп’ютер нотаріуса, а також антивірусне програмне забезпечення.

Для визначення ступеня цінності кожного активу та встановлення пріоритетів їх захисту було проведено експертне опитування. В якості експертів виступили чотири фахівці у сфері інформаційної безпеки та нотаріальної діяльності. Кожен експерт оцінив активи за шкалою від 1 (найбільш цінний, критичний) до 8 (найменш цінний). Вихідні ранги, нормалізована матриця, а також детальний розрахунок суми рангів, поправки на зв’язні ранги, коефіцієнт конкордації та критерій Пірсона наведені в Додатку А.

Для перевірки узгодженості думок експертів було розраховано коефіцієнт конкордації Кендала W за формулою (2.1).

$$W = \frac{12\sum_{j-1}^{m} d_j^2}{n^2(m^3-m)-12\sum_{i=1}^{n} T_i} \quad (2.1)$$

де n – кількість експертів;

m – кількість активів;

T – середня сума рангів;

d_j^2 – квадрат відхилення;

T_i – поправка на зв’язні ранги.

Розрахунки показали, що сума квадратів відхилень сум рангів від середньої величини становить 636. З урахуванням поправок на зв’язані ранги, значення коефіцієнта конкордації дорівнює 0,92. Оскільки W > 0,5, це свідчить про високий ступінь узгодженості думок експертів. Перевірка значущості отриманого коефіцієнта за критерієм Пірсона X^2 (формула 2.2) показала, що розрахункове значення $X^2_{розр}$ = 26,8 перевищує табличне $X^2_{табл}$ = 14,1 при рівні значущості α = 0,05 та кількості ступенів свободи k = 7. Це підтверджує статистичну значущість отриманих результатів та обґрунтовує можливість їх використання для подальшого аналізу.

$$X^2 = n * (m - 1) * W \quad (2.2)$$

де n – кількість екпертів;

m – кількість активів;

W – коефіцієнт конкордації.

На основі отриманих сум рангів Rj для кожного активу було розраховано узагальнену цінність за формулою нормування в діапазоні від 7 до 10, де вищий бал відповідає більшій цінності активу:

$$\text{Цінність} = 10 - (Rj - Rj\_min)/(Rj\_max - Rj\_min) * 3 \quad (2.3)$$

де Rj – сума рангів;

Rj_min – мінімальна сума рангів;

Rj_max – максимальна сума рангів;

3 – розмах кінцевих значень цінності (7-10).

Результати ранжування за пріоритетом захисту наведені в таблиці 2.3.

Таблиця 2.3 – Ранжування активів нотаріальної контори за пріоритетом захисту

Актив	Rj	Цінність
Критичні бази даних	4	10
Нотаріальна таємниця	9,5	9,377358
Паперовий архів	12	9,09434
Доступ до держ. реєстрів	14,5	8,811321
Токен (носій КЕП)	20	8,188679
Персональні дані клієнтів	25	7,622642
Антивірусне ПЗ	28,5	7,226415
ПК нотаріуса	30,5	7

Відповідно до наведеної таблиці 2.3 найвищий пріоритет (цінність 10,0) мають критичні бази даних (електронний архів нотаріальних документів). Цей актив є найбільш критичним, оскільки містить усі електронні копії нотаріальних документів, втрата або пошкодження яких може призвести до неможливості підтвердження вчинених нотаріальних дій.

Високий пріоритет (цінність від 8,80 до 9,38) мають нотаріальна таємниця (цінність 9,38), паперовий архів нотаріальних справ (цінність 9,09) та доступ до державних реєстрів (цінність 8,81). Нотаріальна таємниця відповідно до статті 8 Закону України «Про нотаріат» є інформацією з найвищим ступенем конфіденційності, її розголошення є злочином та тягне за собою кримінальну відповідальність. Паперовий архів має критичне значення через 75-річний термін зберігання та неможливість відновлення знищених документів. Доступ до державних реєстрів (Єдиного реєстру нотаріальних дій, Державного реєстру речових прав на нерухоме майно, Єдиного державного реєстру юридичних осіб, Спадкового реєстру) є критичним сервісним активом, оскільки його блокування унеможливлює виконання нотаріальних дій.

Середній пріоритет (цінність від 7,23 до 8,19) мають токен (носій КЕП) з цінністю 8,19, персональні дані клієнтів з цінністю 7,62 та антивірусне програмне забезпечення з цінністю 7,23. Токен забезпечує зберігання ключів кваліфікованого електронного підпису та доступ до державних реєстрів, його компрометація може призвести до неправомірних нотаріальних дій. Персональні дані клієнтів захищаються Законом України «Про захист персональних даних», їх витік тягне за собою адміністративну та кримінальну відповідальність. Антивірусне програмне забезпечення є базовим елементом захисту всіх інформаційних активів, його відсутність створює передумови для реалізації загроз, пов'язаних з шкідливим програмним забезпеченням.

Найнижчий пріоритет (цінність 7,0) має робочий персональний комп'ютер нотаріуса. Цей актив є основним інструментом роботи, містить ключі, паролі та забезпечує доступ до державних реєстрів, однак його захист значною мірою опосередковано забезпечується через захист інших активів (зокрема, антивірусного ПЗ та токена з КЕП).

Визначені пріоритети захисту активів є основою для подальшої ідентифікації загроз, виявлення вразливостей та оцінювання ризиків. Найбільш критичні активи, що отримали найвищий та високий пріоритет, потребують першочергового застосування заходів захисту та найбільш ретельного моніторингу.

2.3 Модель загроз та модель порушника

Модель порушника та модель загроз є ключовим етапом оцінювання ризиків, оскільки дозволяє системно описати, хто і яким чином може завдати шкоди активам нотаріальної контори. Згідно з результатами ранжування, наведеними в табл. 2.3, токен (носій КЕП) має середній пріоритет захисту з цінністю 8,19. Незважаючи на середній пріоритет, саме цей актив було обрано для детального моделювання з кількох причин. По-перше, токен є фізичним носієм ключів кваліфікованого електронного підпису, що робить його вразливим як до технічних, так і до фізичних загроз. По-друге, компрометація токена може

призвести до критичних наслідків, зокрема до неправомірного використання КЕП третіми особами. По-трете, побудова моделей для цього активу дозволяє наочно продемонструвати методику, яка надалі може бути застосована для інших активів.

2.3.1 Модель загроз

На основі аналізу можливих послаблюючих факторів та вразливостей в нотаріальній конторі було ідентифіковано основні загрози для токена з КЕП. Для систематизації загроз використано методологію STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of privilege), яка дозволяє комплексно охопити порушення автентифікації, цілісності, неможливості заперечення, конфіденційності, доступності та розмежування доступу.

Таблиця 2.4 – Модель загроз за шістьма категоріями STRIDE

Категорія (STRIDE)	Опис загрози	Приклад сценарію	Заходи захисту
Spoofing (Підміна)	Використання чужого носія з ЕЦП для видачі себе за іншого нотаріуса або керівника контори.	Співробітник знайшов флешку колеги на столі та підписав документ від його імені, поки той вийшов.	Використання носіїв із захистом (токени/смарт-карти замість флешок), блокування сесії при виході з робочого місця, встановлення PIN-коду на сам носій.
Tampering (Втручання)	Модифікація програмного забезпечення на токені або підміна сертифіката.	Вірус на ПК нотаріуса перехоплює звернення до ключа і підписує інший документ	Використання ліцензійного антивірусу, перевірка цілісності ПЗ КриптоПро, застосування

Продовження таблиці 2.4

		(атака на заміну підпису).	захищених носіїв, які унеможливлюють підміну даних всередині.
Repudiation (Відмова)	Нотаріус стверджує, що не підписував документ, хоча підпис було поставлено його ключем.	Ключ використали у неробочий час, але нотаріус каже, що втратив токен і не знав про це.	Впровадження системи логування часу підписання та ідентифікаторів пристроїв, ведення журналів видачі носіїв.
Information Disclosure (Розкриття)	Копіювання закритого ключа (приватного ключа КЕП) з флешки зловмисником.	Хакер отримав віддалений доступ до ПК і скопіював файли ключів з флешки на свій сервер.	Зберігання ключів виключно на захищених токенах з неможливістю зчитування закритого ключа. Шифрування диска ПК та носія (якщо це файловий носій).
Denial of Service (Відмова у сервісі)	Фізичне знищення носія або блокування доступу до нього.	Флешка зламалася (фізичний знос) або була залита кавою, через що нотаріус не може підписати терміновий договір.	Наявність резервного (бекапного) носія, регулярне створення резервних копій ключів (у зашифрованому вигляді), використання хмарного підписання замість локальних флешок.

Продовження таблиці 2.4

Elevation of Privilege (Підвищення привілей)	Отримання доступу до закритих розділів державних реєстрів через підміну ролі.	Технічний працівник, який знайшов флешку нотаріуса, спробував відкрити реєстр речових прав на нерухомість і внести туди зміни.	Технічне обмеження повноважень на стороні реєстрів, геолокаційна прив'язка сеансів підписання, обов'язкове підтвердження операції через SMS на телефон власника.

2.3.2 Модель порушника

Аналіз потенційних порушників дозволяє визначити, хто може становити загрозу для токена з КЕП. На основі експертного опитування та аналізу типових сценаріїв порушень виокремлено п’ять типів порушників:

1. Внутрішній користувач (ненавмисний порушник).

Мотив/причина: помилки, недостатня обізнаність, порушення регламентів “для зручності”, недбалість, втома.

Типові дії: Залишення флешки з КЕП у USB-порті після завершення роботи. Використання простих PIN-кодів (1234, дата народження) або записування їх на папірці поруч із комп'ютером. Копіювання ключів КЕП на незахищені носії або в хмарні сховища "для зручності доступу". Підключення флешки до заражених комп'ютерів (вдома, в інтернет-кафе, у клієнта). Втрата носія під час транспортування (залишив у таксі, ресторані). Передача флешки колезі "на хвилинку" без фіксації передачі.

Ризик: витік приватного ключа, компрометація КЕП, несанкціоноване підписання документів, зараження носія шкідливим ПЗ, блокування роботи через втрату носія.

2. Внутрішній користувач (умисний порушник/інсайдер).

Мотив: особиста вигода (продаж ключа або даних), помста роботодавцю, конкуренція (перехід до іншої контори), тиск ззовні (шантаж, борги).

Типові дії: Цілеспрямоване копіювання ключів КЕП (директора, головного бухгалтера) перед звільненням. Створення дубліката флешки без відома власника. Несанкціоноване підписання документів з метою наживи. Передача доступу до КЕП третім особам (конкурентам, шахраям). Саботаж — навмисне пошкодження носія або видалення ключів напередодні важливої угоди. Використання КЕП для доступу до закритих реєстрів із метою збору інформації.

Ризик: критичний витік конфіденційної інформації, підписання фіктивних угод, фінансові втрати, втрата довіри клієнтів, судові позови, зупинка нотаріальної діяльності.

3. Привілейований порушник (адміністратор, техпідтримка, оператор ІТ).

Особливості: має розширені права та доступ до ключових компонентів АС (сервери, робочі станції, системи логування, антивірусне ПЗ).

Типові дії: Зміна політик доступу для розширення прав на використання КЕП. Створення "тіньових" облікових записів із доступом до криптографічного ПЗ. Відключення антивірусного захисту на робочих станціях нотаріусів. Модифікація системних бібліотек для перехоплення PIN-кодів. Копіювання резервних копій ключів КЕП із серверів. Приховування слідів несанкціонованого доступу шляхом редагування логів. Навмисне блокування носіїв через антивірус.

Ризик: повна компрометація криптографічного захисту, неможливість довести факт злому (відсутність логів), тривале приховане використання ключів, підрив довіри до всієї системи електронного документообігу.

4. Зовнішній порушник (хакер, кіберзлочинець, конкурент).

Мотив: фінансова вигода (крадіжка грошей через підписання платіжок), промислове шпигунство (доступ до реєстрів угод), дискредитація нотаріальної системи.

Типові дії: Віддалений злом ПК нотаріуса (через фішинг, вразливості) з метою копіювання ключів. Встановлення шпигунського ПЗ для перехоплення

PIN-кодів. Атака на канали зв'язку (збір трафіку з КЕП). Фізичне проникнення в офіс (під виглядом клієнта) для встановлення апаратних кейлогерів. Соціальна інженерія — дзвінки нотаріусам від імені "техпідтримки" для отримання паролів. Організація DDoS-атак на інфраструктуру, щоб паралізувати роботу і вимагати викуп.

Ризик: фінансові втрати, викрадення персональних даних клієнтів, репутаційні втрати, зупинка діяльності, втрата ліцензії.

5. Зовнішній порушник (випадковий / ненавмисний).

Мотив: відсутній — дії через незнання, цікавість або випадковість.

Типові дії: Знаходження загубленої флешки сторонньою особою (клієнт, перехожий, прибиральниця). Підключення знайденого носія до свого комп'ютера "подивитися, що там". Випадкове пошкодження носія (механічне, магнітне, хімічне). Передача знахідки третім особам замість повернення власнику.

Ризик: витік даних через сторонніх осіб, втрата ключа без можливості відновлення, потрапляння ключа до зловмисників через "ланцюжок" передач.

Отримані моделі є основою для подальшої ідентифікації вразливостей та оцінювання ризиків.

2.4 Виявлення вразливостей

Вразливість — це слабке місце в системі захисту, яке може бути використане для реалізації ідентифікованих загроз (табл. 2.4). На цьому етапі проведено аналіз існуючого стану захисту інформації в нотаріальній конторі. Виявлені вразливості поділено на три категорії: організаційні, технічні та фізичні.

Організаційні вразливості є найбільш критичними, оскільки вони створюють передумови для реалізації інших загроз. Типовими організаційними вразливостями для нотаріальної контори є відсутність затверджених політик інформаційної безпеки, що призводить до неузгодженості дій персоналу та відсутності єдиних правил роботи з конфіденційною інформацією. Також до організаційних вразливостей належать відсутність плану реагування на

інциденти, внаслідок чого дії персоналу при надзвичайних ситуаціях є хаотичними та неефективними, а також недостатня обізнаність персоналу з питань кібербезпеки, що робить співробітників легкою мішенню для атак соціальної інженерії (фішинг, телефонне шахрайство). Крім того, до цієї категорії належать відсутність регламенту резервного копіювання, відсутність контролю за доступом до приміщення (вільний вхід сторонніх осіб), відсутність підписаних зобов'язань про нерозголошення конфіденційної інформації, а також відсутність процедур періодичної зміни паролів та регулярного навчання персоналу.

Технічні вразливості пов'язані з недоліками апаратного та програмного забезпечення, а також з помилками в його налаштуванні. До них належать використання застарілих версій операційної системи, які мають невиправлені вразливості, що може бути використано зловмисниками для отримання несанкціонованого доступу. Також критичною є відсутність антивірусного захисту або використання застарілих антивірусних баз, що не забезпечує належного захисту від сучасних загроз. До технічних вразливостей належать зберігання ключів кваліфікованого електронного підпису на жорсткому диску замість апаратного захищеного носія (токена), використання слабких або стандартних паролів для доступу до систем, відсутність шифрування даних на зовнішніх носіях, а також відсутність резервного копіювання або його нерегулярність. Крім того, до цієї категорії належать відсутність захисту каналів зв'язку (незашифрований Wi-Fi), відсутність автоматичних оновлень програмного забезпечення, а також відсутність системи виявлення вторгнень та моніторингу підозрілої активності.

Фізичні вразливості пов'язані з неналежним станом приміщень, обладнання та систем фізичного захисту. Типовими фізичними вразливостями для нотаріальної контори є відсутність охоронної сигналізації в приміщенні, що робить можливою крадіжку обладнання або документів у неробочий час. Також до цієї категорії належать зберігання нотаріальних справ у незамиканих шафах

замість металевих сейфів, що дозволяє вільний доступ сторонніх осіб до конфіденційних документів, а також відсутність окремого приміщення для серверного обладнання або його незадовільний стан (немає замка, обмеження доступу). Крім того, до фізичних вразливостей належать відсутність засобів пожежогасіння (вогнегасників) або їх несправність, відсутність резервного джерела живлення (ДБЖ) для критичного обладнання, що може призвести до втрати даних при раптовому відключенні електроенергії, а також вільний доступ сторонніх осіб до приміщення контори (відсутність ресепшн, контролера або системи контролю доступу).

Для кожної виявленої вразливості було визначено, які загрози вона може посилювати або робити можливими. Наприклад, вразливість «зберігання ключів КЕП на жорсткому диску» робить можливою реалізацію загроз «крадіжка ключової інформації» та «несанкціонований доступ до комп'ютера» з критичними наслідками. Вразливість «відсутність регулярного резервного копіювання» підвищує критичність загрози «збій жорсткого диска», оскільки відновити втрачені дані буде неможливо. Вразливість «недостатня обізнаність персоналу» робить можливою реалізацію загроз соціальної інженерії (фішинг, телефонне шахрайство) та ненавмисного розголошення інформації.

Найбільш критичними для нотаріальної контори є наступні вразливості. По-перше, зберігання ключів КЕП на жорсткому диску замість апаратного токена, що створює можливість їх копіювання при віддаленому зламі комп'ютера. По-друге, відсутність резервного копіювання критичних баз даних, що робить їх втрату (внаслідок збою диска, вірусу-вимагача або помилки людини) незворотною. По-третє, відсутність контролю доступу до архівного приміщення, що створює ризик несанкціонованого доступу до паперових нотаріальних справ. По-четверте, відсутність засобів пожежогасіння в архівному приміщенні, що при виникненні пожежі призведе до безповоротного знищення унікальних документів з 75-річним терміном зберігання. По-п'яте, недостатня

обізнаність персоналу з питань безпеки, що робить їх легкою мішенню для соціальної інженерії.

Таким чином, виявлені вразливості охоплюють усі рівні захисту — від організаційного (відсутність політик, навчання) до технічного (антивірус, шифрування, резервне копіювання) та фізичного (охорона, пожежна безпека, контроль доступу). Усунення цих вразливостей є необхідною умовою зниження ризиків інформаційної безпеки нотаріальної контори.

2.5 Аналіз та оцінювання ризиків

На основі ідентифікованих активів (табл 2.1), загроз (табл. 2.4) та вразливостей (п. 2.4) необхідно оцінити рівень кожного ризику за формулою (2.4). Для кожної комбінації «актив — загроза — вразливість» (тобто для кожної ситуації, коли існує актив, є загроза, яка може його вразити, і є вразливість, яка дозволяє цій загрозі реалізуватися) визначаються два параметри: ймовірність реалізації загрози та рівень потенційних наслідків.

$$R = P * A \tag{2.4}$$

де P – ймовірність реалізації ризику;

A – наслідки реалізації ризику.

У ході дослідження було проаналізовано всі можливі комбінації «актив — загроза — вразливість» для активу «Токен (носій КЕП)» та виконано оцінювання ризиків із застосуванням розроблених шкал (п.2.1). Розрахунок рівня ризику здійснювався як добуток ймовірності (від 1 до 5) та наслідків (від 1 до 5), що дає значення в діапазоні від 1 до 25. Нижче наведено результати оцінювання для кожної з ідентифікованих загроз.

Ризик використання чужого носія з КЕП для видачі себе за іншого нотаріуса або керівника контори. Загроза реалізується через вразливість відсутності контролю за доступом до приміщення та відсутності блокування сесії при виході з робочого місця. Ймовірність оцінено як 3 (один раз на півроку або

рідше), оскільки внутрішній порушник має фізичний доступ до приміщення та може скористатися флешкою колеги, залишеною без нагляду. Наслідки — 5 (критичні, оскільки у разі успішної підміни порушник отримує можливість використовувати КЕП нотаріуса для вчинення неправомірних нотаріальних дій, що тягне за собою кримінальну відповідальність). Рівень ризику становить 15, що відноситься до категорії високих.

Ризик модифікації програмного забезпечення на файловому носії або підміни сертифіката. Загроза реалізується через вразливість відсутності контролю цілісності ПЗ та використання незахищених файлових носіїв замість апаратних токенів. Ймовірність оцінено як 2 (один раз на рік або рідше), оскільки модифікація ПЗ потребує високого рівня технічної експертизи та може бути реалізована лише привілейованим порушником (адміністратором) або зовнішнім хакером після зламу ПК. Наслідки — 5 (критичні, оскільки модифікація ПЗ може призвести до того, що підпис буде поставлено під іншим документом, ніж той, який бачив нотаріус). Рівень ризику становить 10, що відноситься до категорії середніх.

Ризик того, що нотаріус стверджує, що не підписував документ, хоча підпис було поставлено його ключем. Загроза реалізується через вразливість відсутності системи логування часу підписання та ідентифікаторів пристроїв, а також відсутності журналів видачі носіїв. Ймовірність оцінено як 4 (один раз на місяць або рідше), оскільки відсутність доказової бази створює сприятливі умови для зловживань. Наслідки — 4 (високі, оскільки відсутність можливості довести факт підписання ускладнює розслідування інцидентів та може призвести до судових спорів). Рівень ризику становить 16, що відноситься до категорії високих.

Ризик копіювання закритого ключа (приватного ключа КЕП) з токену зловмисником. Загроза реалізується через вразливість зберігання ключів на файловому носії (флешці) замість захищеного апаратного токена, а також відсутності шифрування диска ПК. Ймовірність оцінено як 3 (один раз на півроку

або рідше), оскільки зовнішній хакер після віддаленого зламу ПК може скопіювати файли ключів. Наслідки — 5 (критичні, оскільки копіювання ключа дає зловмиснику повний доступ до КЕП нотаріуса поза межами контори). Рівень ризику становить 15, що відноситься до категорії високих.

Ризик фізичного знищення носія або блокування доступу до нього. Загроза реалізується через вразливість відсутності резервного носія, відсутності регулярного створення резервних копій ключів, а також відсутності контролю за фізичним зберіганням токену. Ймовірність оцінено як 3 (один раз на півроку або рідше), оскільки внутрішній ненавмисний порушник може випадково пошкодити або загубити флешку. Наслідки — 5 (критичні, оскільки без токену нотаріус втрачає можливість доступу до державних реєстрів та посвідчення електронних документів, що унеможливлює виконання нотаріальних дій). Рівень ризику становить 15, що відноситься до категорії високих.

Ризик отримання доступу до закритих розділів державних реєстрів через підміну ролі. Загроза реалізується через вразливість відсутності геолокаційної прив’язки сеансів підписання та відсутності додаткового підтвердження операцій. Ймовірність оцінено як 2 (один раз на рік або рідше), оскільки привілейований порушник (системний адміністратор) має фізичний доступ до серверного обладнання, але для успішної реалізації загрози йому потрібно подолати додаткові заходи захисту. Наслідки — 5 (критичні, оскільки підвищення привілеїв дозволяє порушнику вносити зміни до державних реєстрів від імені нотаріуса). Рівень ризику становить 10, що відноситься до категорії середніх.

Результати оцінювання рівнів ризиків для активу «Токен (носій КЕП)» зведено в таблиці 2.5.

Таблиця 2.5 – Оцінювання рівнів ризиків для активу «Токен (носій КЕП)»

ID	Загроза	Вразливість	Ймовірність	Наслідки	Рівень ризику	Категорія
1	Використання чужого носія з КЕП для видачі себе за іншого нотаріуса	Відсутность контролю за доступом до приміщення та відсутность блокування сесії при виході з робочого місця.	3	5	15	Високий
2	Модифікація програмного забезпечення на токені або підміна сертифіката.	Відсутность контролю цілісності ПЗ та використання незахищених файлових носіїв замість апаратних токенів.	2	5	10	Середній
3	Нотаріус стверджує, що не підписував документ, хоча підпис було поставлено його ключем.	Відсутность системи логування часу підписання та ідентифікаторів пристроїв	4	4	16	Високий
4	Копіювання закритого ключа (приватного ключа КЕП) з флешки зловмисником.	Зберігання ключів на файловому носії замість захищеного апаратного токена, відсутності шифрування диска ПК	3	5	15	Високий

Продовження таблиці 2.5

5	Фізичне знищення носія або блокування доступу до нього.	Відсутності резервного носія, відсутність регулярного створення резервних копій ключів, відсутность контролю за фізичним зберіганням токену	3	5	15	Високий

Можна побачити з табл. 2.5, що для активу «Токен (носій КЕП)» найвищі рівні ризику (16 та 15, категорія «високі») мають чотири загрози: використання чужого носія для видачі себе за іншого нотаріуса, відмова нотаріуса від підпису, копіювання закритого ключа зловмисником та фізичне знищення носія. Це означає, що захист токену має бути спрямований насамперед на запобігання цим загрозам. Загрози з середнім рівнем ризику (модифікація ПЗ та отримання доступу до закритих розділів реєстрів) потребують планової обробки.

2.6 Побудова матриці ризиків

Для наочного представлення результатів оцінювання ризиків будується матриця (карта) ризиків. Матриця ризиків є двовимірною таблицею, де по вертикалі відкладається рівень наслідків (від 1 до 5), а по горизонталі — рівень ймовірності (від 1 до 5). Кожна клітина матриці відповідає певному рівню ризику, який визначається як добуток ймовірності та наслідків. Така візуалізація дозволяє швидко ідентифікувати найбільш критичні ризики та визначити пріоритети для їх обробки.

Згідно зі шкалами, визначеними в підрозділі 2.1, кольорове маркування матриці дозволяє ідентифікувати зони ризику. Зона неприйнятних ризиків (рівень 20-25, клітини з ймовірністю 4-5 та наслідками 5, або ймовірністю 5 та наслідками 4) позначається червоним кольором. Зона високих ризиків (рівень 15-

19, клітини з ймовірністю 3 та наслідками 5, або ймовірністю 4 та наслідками 4, або ймовірністю 5 та наслідками 3) позначається помаранчевим кольором. Зона середніх ризиків (рівень 8-14) позначається жовтим кольором. Зона низьких ризиків (рівень 1-7) позначається зеленим кольором.

На основі результатів оцінювання, наведених у табл. 2.5, на матрицю нанесено всі ідентифіковані ризики для активу «Токен (носій КЕП)». Результати побудови матриці наведено в табл. 2.7.

Таблиця 2.7 – Матриця (карта) ризиків для активу «Токен (носій КЕП)»

Наслідки \ Ймовірність	1 (дуже низька)	2 (низька)	3 (середня)	4 (висока)	5 (дуже висока)
5 (критичні)		№2, №6	№1, №4, №5		
4 (високі)				№3	
3 (середні)					
2 (низькі)					
1 (незначні)					

З табл. 2.7, жоден з ідентифікованих ризиків не потрапив до червоної зони (неприйнятні ризики). До помаранчевої зони (високі ризики) потрапили чотири загрози: використання чужого носія з КЕП для видачі себе за іншого нотаріуса (№1), копіювання закритого ключа з токену зловмисником (№4), фізичне знищення носія або блокування доступу до нього (№5), а також відмова нотаріуса від підпису (№3).

До жовтої зони (середні ризики) потрапили дві загрози: модифікація ПЗ на токені або підміна сертифіката (№2) та отримання доступу до закритих розділів державних реєстрів через підміну ролі (№6).

Матриця ризиків дозволяє керівництву нотаріальної контори швидко оцінити загальний стан захищеності активів. Відсутність ризиків у червоній зоні свідчить про те, що критичних загроз, які потребують негайного реагування, не виявлено. Однак наявність чотирьох ризиків у помаранчевій зоні (високий

рівень) вказує на необхідність першочергової розробки та впровадження заходів з обробки цих загроз. Пріоритетами є: посилення контролю за фізичним доступом до носіїв (проти загроз №1 та №5), впровадження системи логування використання КЕП (проти загрози №3) та використанння апаратних токенів замість файлових флешок (проти загрози №4).

Отримана матриця ризиків є основою для подальшого визначення пріоритетних ризиків (підрозділ 2.7).

2.7 Визначення пріоритетних ризиків

На основі проведеного оцінювання рівнів ризиків (табл. 2.5) та побудованої матриці ризиків (табл. 2.7) визначаються пріоритетні ризики, які потребують першочергової обробки. До пріоритетних відносяться ризики, що потрапили до помаранчевої зони (високі ризики з рівнем 15-19). Ризики з жовтої зони (середні ризики з рівнем 8-14) потребують планової обробки в другу чергу. Ризики із зеленої зони (низькі ризики з рівнем 1-7) можуть бути прийняті без додаткової обробки.

Для активу «Токен (носій КЕП)» до пріоритетних (високих) ризиків належать чотири загрози, які отримали рівень 15-16. Кожен з цих ризиків потребує розробки та впровадження відповідних заходів обробки.

Пріоритетний ризик №1 (високий, рівень 16) — відмова нотаріуса від підпису. Цей ризик полягає в тому, що нотаріус стверджує, що не підписував документ, хоча підпис було поставлено його ключем. Загроза реалізується через вразливість відсутності системи логування часу підписання та ідентифікаторів пристроїв, а також відсутності журналів видачі носіїв. Найбільш ймовірним джерелом цієї загрози є внутрішній умисний порушник (інсайдер), який має легітимний доступ до токену та може використати її в неробочий час. Для обробки цього ризику обирається стратегія зменшення шляхом впровадження системи логування часу підписання та ідентифікаторів пристроїв, а також ведення журналів видачі носіїв, що дозволить створити доказову базу для підтвердження або спростування факту підписання.

Пріоритетний ризик №2 (високий, рівень 15) — використання чужого носія з КЕП для видачі себе за іншого нотаріуса. Цей ризик полягає в тому, що порушник використовує чужий носій з КЕП для підписання документів від імені іншого нотаріуса. Загроза реалізується через вразливості відсутності контролю за доступом до приміщення, відсутності блокування сесії при виході з робочого місця та відсутності PIN-коду на самому носії. Найбільш ймовірними джерелами цієї загрози є внутрішній умисний порушник (інсайдер) або внутрішній ненавмисний порушник, який залишив токен без нагляду. Для обробки цього ризику обирається стратегія зменшення шляхом посилення контролю за фізичним доступом до приміщення, впровадження політики обов'язкового блокування сесії при виході з робочого місця, встановлення PIN-коду на сам носій, а також використання апаратних токенів замість файлових флешок.

Пріоритетний ризик №3 (високий, рівень 15) — копіювання закритого ключа з токену зловмисником. Цей ризик полягає в тому, що зловмисник отримує копію закритого ключа КЕП з файлової флешки та використовує її поза межами контори. Загроза реалізується через вразливість зберігання ключів на файловому носії замість захищеного апаратного токена, а також через відсутність шифрування диска ПК. Найбільш ймовірним джерелом цієї загрози є зовнішній порушник (хакер), який отримує віддалений доступ до ПК нотаріуса. Для обробки цього ризику обирається стратегія зменшення шляхом заміни файлових флешок на апаратні токени з неможливістю зчитування закритого ключа, а також впровадження шифрування дисків ПК та підвищення рівня антивірусного захисту.

Пріоритетний ризик №4 (високий, рівень 15) — фізичне знищення носія або блокування доступу до нього. Цей ризик полягає в тому, що токен фізично знищується або блокується, внаслідок чого нотаріус втрачає можливість доступу до державних реєстрів та посвідчення електронних документів. Загроза реалізується через вразливості відсутності резервного носія, відсутності регулярного створення резервних копій ключів, а також відсутності контролю за

фізичним зберіганням. Найбільш ймовірними джерелами є внутрішній ненавмисний порушник (загубив або пошкодив флешку) або внутрішній умисний порушник (навмисне резервного (бекапного) носія, регулярного створення резервних копій ключів у зашифрованому вигляді, а також посилення контролю за фізичним зберіганням носія. Частково ризик може бути переданий шляхом страхування відповідальності нотаріуса на випадок втрати КЕП.

Пріоритетні ризики середнього рівня (рівень 10, жовта зона). Загроза №2 (модифікація ПЗ на токені або підміна сертифіката) та загроза №6 (отримання доступу до закритих розділів державних реєстрів через підміну ролі) мають середній рівень ризику (10). Вони потребують планової обробки після завершення роботи з високими ризиками. Для загрози №2 обирається стратегія зменшення шляхом використання ліцензійного антивірусу, перевірки цілісності ПЗ та застосування захищених носіїв. Для загрози №6 обирається стратегія зменшення шляхом технічного обмеження повноважень на стороні реєстрів, геолокаційної прив’язки сеансів підписання та обов’язкового підтвердження операцій через SMS на телефон власника.

2.8 Висновок до розділу 2

У другому розділі «Ідентифікація активів, загроз, вразливостей та оцінювання ризиків інформаційної безпеки нотаріальної контори» проведено оцінювання ризиків інформаційної безпеки для типової нотаріальної контори. На основі обраної методики виконано всі етапи процесу оцінювання ризиків: встановлення контексту, ідентифікацію активів, загроз та вразливостей, оцінювання ризиків, побудову матриці ризиків та визначення пріоритетів.

Розроблено шкали оцінювання ймовірності та наслідків, визначено критерії прийнятності ризиків. Проведено ідентифікацію та ранжування активів нотаріальної контори. Застосування методу експертного ранжування з розрахунком коефіцієнта конкордації Кендалла підтвердило високий ступінь узгодженості думок експертів та статистичну значущість результатів.

Побудовано модель загроз та модель порушника для активу «Токен (носій КЕП)» як показового прикладу. Ідентифіковано шість категорій загроз підміна носія, модифікація ПЗ, відмова від підпису, копіювання ключа, фізичне знищення носія та підвищення привілеїв. Виявлено організаційні, технічні та фізичні вразливості в існуючій системі захисту інформації.

На основі ідентифікованих загроз та вразливостей проведено оцінювання ризиків. Побудована матриця ризиків наочно продемонструвала розподіл загроз за зонами: чотири загрози потрапили до зони високих ризиків, дві — до зони середніх ризиків. Визначено пріоритетні ризики, що потребують першочергової обробки, та обґрунтовано вибір стратегій їх обробки (зменшення для всіх високих ризиків, а для ризику фізичного знищення носія — додатково передача у вигляді страхування).

В умовах зростання кількості кібератак на державні реєстри та суб'єктів інформаційної діяльності, а також почастішання випадків компрометації кваліфікованих електронних підписів, виникає нагальна потреба у системному оцінюванні ризиків саме для нотаріальних контор, які є ключовими учасниками електронної взаємодії з реєстрами. Таким чином, своєчасне виявлення та кількісна оцінка ризиків є необхідною умовою забезпечення безперервності нотаріальної діяльності. Отримані результати створюють необхідне підґрунтя для третього розділу, де будуть розроблені конкретні організаційно-технічні заходи з обробки ідентифікованих ризиків, а також практичні рекомендації щодо впровадження процесу управління ризиками в систему управління інформаційною безпекою нотаріальної контори.

3. ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НОТАРІАЛЬНОЇ КОНТОРИ

3.1 Мета та завдання програмної реалізації

На основі результатів теоретичного дослідження, проведеного у другому розділі, було встановлено, що оцінка ризиків інформаційної безпеки нотаріальної контори є багатоетапним процесом, який включає ранжування активів за ступенем їх цінності та оцінювання ризиків активу. Виконання цих розрахунків вручну є трудомістким і схильним до помилок, що обумовлює необхідність автоматизації цього процесу.

Метою програмної реалізації є створення інструменту, який дозволяє автоматизувати такі етапи оцінки ризиків, як-от: введення експертних даних для ранжування активів, отримання кінцевих результатів у вигляді таблиць та звітів.

Для досягнення поставленої мети необхідно реалізувати наступні функціональні можливості: введення та обробка матриць рангів для ранжування активів; розрахунок коефіцієнта конкордації Кендалла та перевірка статистичної значущості результатів; визначення цінності активів за формулою нормування; автоматичне визначення найціннішого активу за результатами ранжування; оцінка ризиків для найціннішого активу за параметрами ймовірності та наслідків; розрахунок рівня ризику та визначення категорії ризику; збереження результатів у форматі CSV для подальшого аналізу та зберігання.

3.2 Автоматизація процесів

Розроблена програма автоматизує два етапи оцінки ризиків інформаційної безпеки нотаріальної контори.

На етапі автоматизації ранжування активів програма надає користувачеві попередньо визначений список з 33 активів нотаріальної контори, з якого він може обрати активи для ранжування. Програма автоматично розраховує суми рангів Rj для кожного активу на основі введеної експертами матриці рангів, визначає цінність кожного активу за шкалою від 7 до 10, обчислює коефіцієнт конкордації Кендалла W (формула 2.1), який показує ступінь узгодженості думок

експертів, та критерій Пірсона X^2 для перевірки статистичної значущості результатів (формула 2.2), після чого автоматично визначає найцінніший актив - той, що має максимальне значення цінності.

Після визначення найціннішого активу програма пропонує оцінити ризики саме для цього активу. Користувач вводить параметри кожної загрози: назву, опис, ймовірність P (1-5) та наслідки A (1-5). Програма автоматично розраховує рівень ризику (формула 2.4), визначає категорію ризику згідно з встановленою шкалою (неприйнятний, високий, середній, низький), формує рекомендації щодо обробки кожного ризику, виконує статистичний аналіз (підрахунок кількості ризиків за категоріями, обчислення сумарного та середнього рівнів ризику) та забезпечує збереження результатів у CSV-файл для подальшого аналізу та зберігання.

Таким чином, програма повністю автоматизує цикл оцінки ризиків - від введення вихідних даних до отримання готового структурованого звіту, що значно скорочує час на проведення розрахунків та унеможливлює помилки, пов’язані з людським фактором.

3.3 Структура модулів

Структура модулів системи оцінки ризиків є ключовим аспектом її розробки. Вона визначає, як різні компоненти системи взаємодіють між собою, які завдання вони виконують та як вони організовані для досягнення основної мети - надійного і точного автоматизованого оцінювання ризиків інформаційних активів нотаріальної контори.

Основні модулі системи:

1. Модуль вводу даних (Data Input Module)
Функції:

- забезпечення вводу даних користувачем для ранжування активів вибір активів зі списку, введення кількості експертів, введення матриці рангів);
- забезпечення вводу даних користувачем для оцінки ризиків (введення назви загрози, опису, ймовірності P та наслідків W;

- валідація введених даних для забезпечення їх коректності (перевірка діапазону значень, перевірка формату введення).

Компоненти:

- консольний інтерфейс користувача для введення даних;
- логіка валідації введених значень (перевірка, що ранг знаходиться в межах від 1 до кількості активів, а ймовірність та наслідки - в межах від 1 до 5).

2. Модуль обробки даних (Data Processing Module)
Функції:

- обробка введених даних для подальшого використання у розрахунках;
- зберігання даних у структурованому форматі (списки активів та загроз);
- нормалізація матриці рангів для обробки зв’язаних рангів.

Компоненти:

- алгоритми обробки даних (розрахунок сум рангів Rj, розрахунок відхилень Dj, розрахунок поправок на зв’язані ранги Ti);
- структури даних для зберігання активів (клас Asset) та ризиків (клас Risk);
- списки (List<T>) для динамічного зберігання колекцій активів та ризиків.

3. Модуль розрахунків (Calculation Module)
Функції:

- виконання розрахунків на основі введених користувачем даних;
- розрахунок цінності активів за формулою нормування; розрахунок коефіцієнта конкордації Кендала W;
- розрахунок критерію Пірсона X^2 та порівняння з табличним значенням;
- розрахунок рівня ризику $R = P \times A$;
- визначення категорії ризику (неприйнятний, високий, середній, низький);
- визначення найціннішого активу (з максимальним значенням Value).

Компоненти:

- формули та алгоритми для розрахунків;
- логіка для обчислення загальної оцінки та визначення категорії ризику;

- словник (Dictionary) для зберігання табличних значень X^2 для різних ступенів свободи.

4. Модуль виводу даних (Data Output Module)
Функції:

- відображення результатів розрахунків користувачу;
- форматування результатів у зрозумілий та зручний для користувача вигляд;
- виведення результатів ранжування;
- виведення таблиці оцінювання ризиків (номер, ймовірність P, наслідки A рівень ризику R, категорія);
- виведення рекомендацій щодо обробки кожного ризику;
- виведення статистичного аналізу (кількість ризиків за категоріями, сумарний та середній рівні ризику);
- збереження результатів у CSV-файл для подальшого аналізу.

Компоненти:

- консольний інтерфейс користувача для відображення результатів;
- логіка форматування та виводу даних (форматування таблиць, маркування рекомендацій);
- логіка збереження звіту у файл (StreamWriter, формат CSV).

Модуль вводу даних отримує дані від користувача (вибір активів, кількість експертів, матриця рангів, параметри ризиків) і передає їх до модуля обробки даних. Модуль обробки даних валідує та зберігає введені дані у структурованому форматі (списки активів та ризиків), передаючи їх до модуля розрахунків. Модуль розрахунків виконує необхідні обчислення на основі оброблених даних (розрахунок цінності активів, коефіцієнта конкордації, рівня ризику, категорії) і передає результати до модуля виводу даних. Модуль виводу даних відображає результати користувачу у зрозумілому форматі (таблиці, рекомендації, статистичний аналіз) та за бажанням користувача зберігає їх у CSV- файл.

3.4 Алгоритм функціонування програми

Алгоритм — це формально описана обчислювальна процедура, яка отримує вхідні дані, слідуючи якій можна досягнути поставлену мету. Він відображає логіку та спосіб розв’язання задачі із зазначенням необхідних розрахункових формул, умов, співвідношень для контролю ймовірності вихідних результатів.

На рисунках 3.1, 3.2 представлено блок-схему розрахунку оцінки ризиків, яка демонструє послідовність етапів від введення даних до отримання загальної оцінки. Блок-схема чітко відображає всі кроки алгоритму, включаючи необхідні умови та розрахункові формули, забезпечуючи зручне і зрозуміле представлення процесу розв’язання задачі.

Рисунок 3.1 — Алгоритм функціонування програми

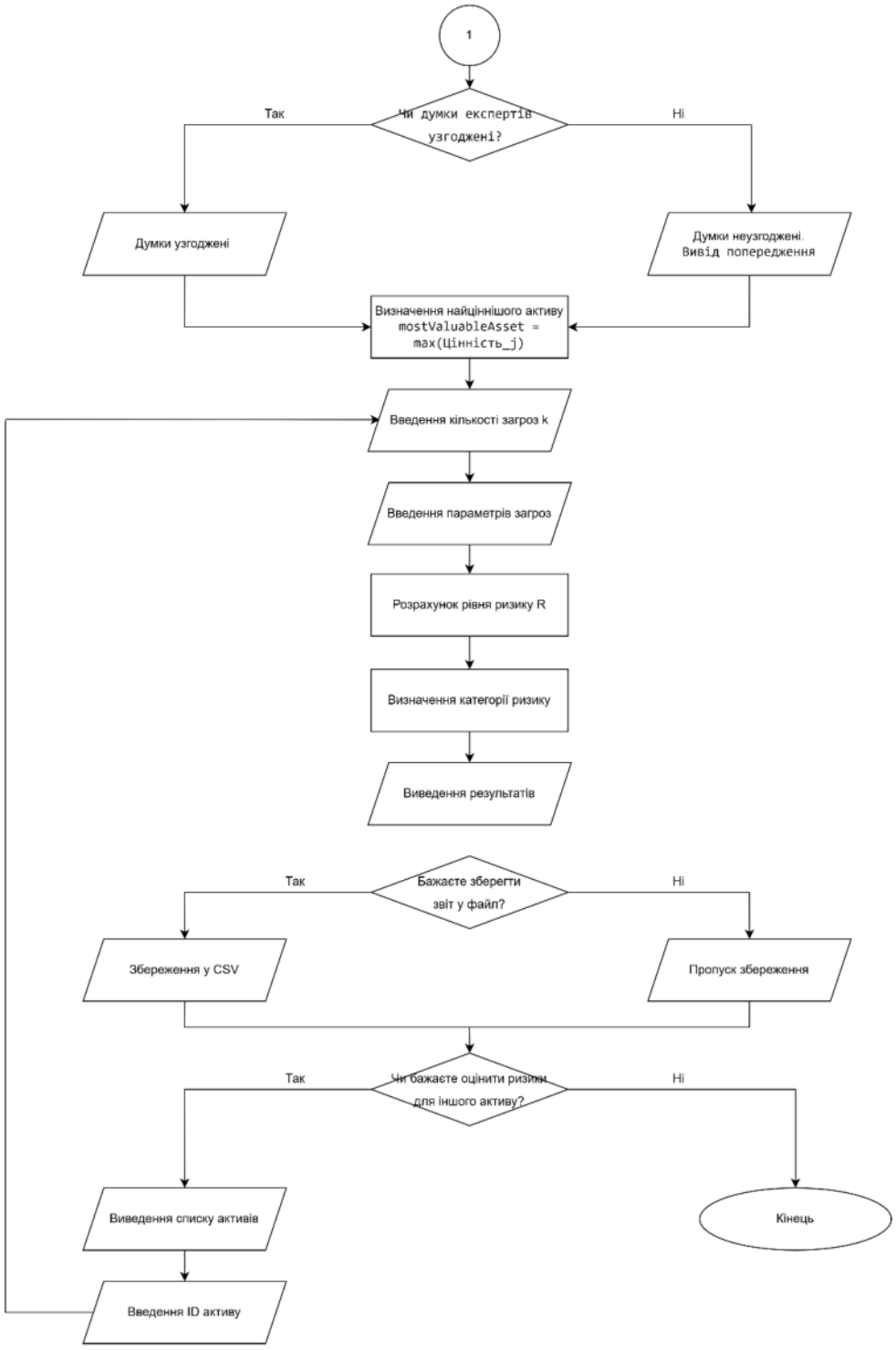


Рисунок 3.2 — Продовження алгоритму функціонування програми

Блок 1. Початок. Цей блок позначає початок процесу оцінки ризиків.

Блок 2. Вибір активів для ранжування. На цьому етапі користувач обирає з попередньо визначеного списку активи, які будуть ранжуватися.

Блок 3. Введення кількості експертів. Користувач вводить кількість експертів, які братимуть участь у ранжуванні.

Блок 4. Введення матриці рангів. Користувач вводить оцінки кожного експерта для кожного активу за шкалою від 1 до m, де m - кількість активів.

Блок 5. Розрахунок сум рангів та цінності активів. Програма обчислює суми рангів для кожного активу та визначає його цінність за формулою.

Блок 6. Розрахунок коефіцієнта конкордації та критерію Пірсона. Програма обчислює коефіцієнт конкордації W за формулою (2.1) та критерій Пірсона X^2 за формулою (2.2).

Блок 7. Перевірка узгодженості думок експертів. Отримане значення X^2 порівнюється з табличним значенням X табл. Якщо $X^2 > X_{табл}$, думки експертів вважаються узгодженими, результати ранжування - статистично значущими.

Блок 8. Визначення найціннішого активу. Програма автоматично визначає актив з максимальним значенням цінності.

Блок 9. Введення кількості загроз. Користувач вводить кількість загроз для найціннішого активу.

Блок 10. Введення загроз. Для кожної загрози користувач вводить назву, опис, ймовірність P (1-5) та наслідки A (1-5).

Блок 11. Розрахунок рівня ризику. Програма обчислює рівень ризику $R = P \times A$ за формулою (2.4).

Блок 12. Визначення категорії ризику. На основі значення R визначається категорія ризику: неприйнятний ($R \geq 20$), високий ($15 \leq R \leq 19$), середній ($8 \leq R \leq 14$) або низький ($R < 8$).

Блок 13. Виведення результатів. Програма виводить таблицю оцінювання ризиків, рекомендації щодо обробки кожного ризику та статистичний аналіз.

Блок 14. Збереження звіту. За бажанням користувача результати зберігаються у CSV-файл.

Блок 15. Запит на оцінку іншого активу. Програма запитує, чи бажає користувач оцінити ризики для іншого активу. Якщо «ні» - перехід до блоку 18 (кінець).

Блок 16. Якщо користувач в попередньому блоці відповів «так», то відбувається виведення повного списку активів.

Блок 17. Вибір ID активу для оцінки. Користувач вводить ID активу, для якого хоче оцінити ризики. І далі відбувається перехід до блоку 9.

Блок 18. Кінець. Цей блок позначає завершення процесу оцінки ризиків.

3.5 Вибір мови програмування

Програмна реалізація даного дипломного проекту була виконана в середовищі програмування Microsoft Visual Studio за допомогою мови C#. Microsoft Visual Studio - це лінійка продуктів компанії Microsoft, яка включає інтегроване середовище розробки програмного забезпечення та інші інструментальні засоби. Ці продукти дозволяють розробляти консольні додатки, додатки з графічним інтерфейсом, веб-сайти, веб-додатки та веб-служби.

Вибір обумовлений тим, що C# є об’єктно-орієнтованою мовою, що дозволило створити чітку структуру програми з чотирьох основних класів: Asset (актив), Risk (ризик), RankingCalculator (розрахунок ранжування) та Program (головний клас). Кожен клас відповідає за свою зону відповідальності, що забезпечує легке супроводження та можливість подальшого розширення функціоналу.

Стандартна бібліотека C# значно спростила реалізацію багатьох компонентів. Для зберігання списків активів та ризиків використовувались колекції List<T>, для роботи з файлами - Streambriter (експорт результатів у CSV), а для математичних обчислень - клас Math та методи LINQ для групування та сортування даних.

Консольний додаток обрано тому, що він не потребує встановлення додаткових бібліотек та працює на будь-якому комп’ютері з Windows. Крім того, всі дії виконуються через текстові команди, що дозволяє зосередитись на логіці розрахунків, а не на графічному інтерфейсі. Такий додаток легко інтегрується в інші системи.

Середовище Visual Studio надало зручні засоби розробки: вбудований відладчик дозволив покроково виконувати код та відстежувати значення змінних, а функція автодоповнення IntelliSense пришвидшила написання коду. Код програми є повністю документованим - кожен клас та метод супроводжується коментарями українською мовою, а назви змінних обрані таким чином, щоб відображати їх призначення (CalculateConcordance, CalculateAssetValues, mostValuableAsset).

Таким чином, обрана мова програмування є оптимальним вибором для реалізації поставленої задачі, забезпечуючи необхідну функціональність, зручність розробки та можливість подальшого супроводження.

3.6 Тестування роботи програми

Розглянемо роботу програми на прикладі. Після запуску програми відкривається консоль зі списком доступних активів на вибір (рисунок 3.2)

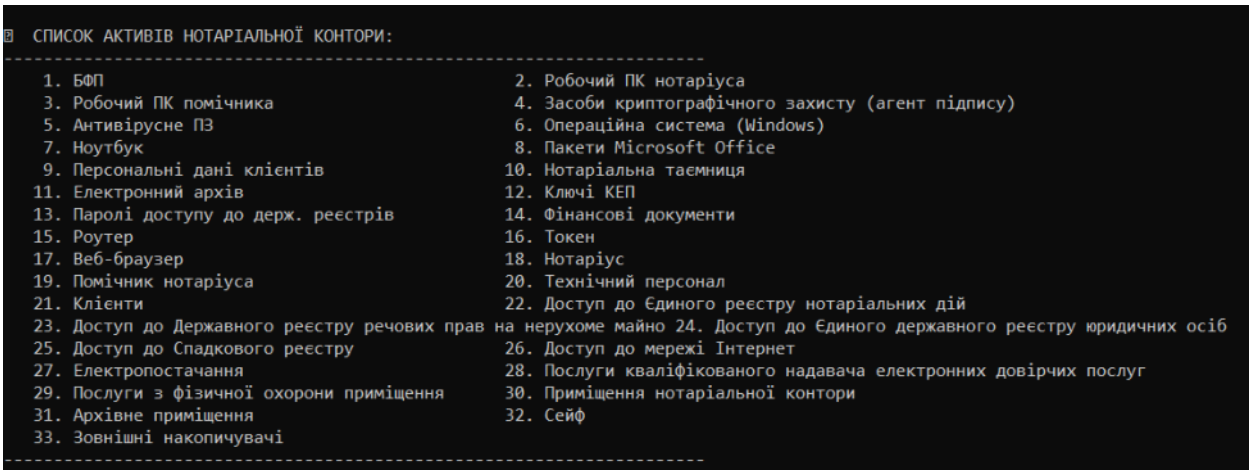


Рисунок 3.2 — Список активів

Далі користувач вводить ID бажаних активів для ранжування через кому, для прикладу оберемо 8: Робочий ПК нотаріуса (ID 2), Антивірусне ПЗ (ID 5), Нотаріальна таємниця (ID 10), Роутер (ID 15), Помічник нотаріуса (ID 19), Доступ до Спадкового реєстру (ID 25), Послуги з фізичної охорони приміщення (ID 29), Зовнішні накопичувачі (ID 33) (рисунок 3.3).

```
Введіть ID активів для ранжування (через кому, наприклад: 11,10,31,22,16,9,5,2): 2,5,10,15,19,25,29,33

 Обрано 8 активів для ранжування:
   - Робочий ПК нотаріуса (ID 2)
   - Антивірусне ПЗ (ID 5)
   - Нотаріальна таємниця (ID 10)
   - Роутер (ID 15)
   - Помічник нотаріуса (ID 19)
   - Доступ до Спадкового реєстру (ID 25)
   - Послуги з фізичної охорони приміщення (ID 29)
   - Зовнішні накопичувачі (ID 33)
```

Рисунок 3.3 — Обрані активи

Наступним кроком користувач вводить кількість експертів для ранжування (рисунок 3.4).

```
Введіть кількість експертів: 4
```

Рисунок 3.4 — Кількість експертів

Далі користувач вводить матрицю рангів. Кожен експерт оцінює активи за шкалою від 1 до 8, де 1 – найцінніший актив, 8 – найменш цінний (рисунки 3.5, 3.6).

```
  ВВЕДЕННЯ МАТРИЦІ РАНГІВ
   (менший ранг = вища цінність, від 1 до 8)
   Увага: при однаковій цінності активів можна ставити однакові ранги!

Експерт 1:
   Робочий ПК нотаріуса: 4
   Антивірусне ПЗ: 7
   Нотаріальна таємниця: 1
   Роутер: 8
   Помічник нотаріуса: 5
   Доступ до Спадкового реєстру: 1
   Послуги з фізичної охорони приміщення: 6
   Зовнішні накопичувачі: 5

Експерт 2:
   Робочий ПК нотаріуса: 5
   Антивірусне ПЗ: 8
   Нотаріальна таємниця: 1
   Роутер: 7
   Помічник нотаріуса: 4
   Доступ до Спадкового реєстру: 2
   Послуги з фізичної охорони приміщення: 7
   Зовнішні накопичувачі: 6

Експерт 3:
   Робочий ПК нотаріуса: 3
   Антивірусне ПЗ: 6
   Нотаріальна таємниця: 2
   Роутер: 6
   Помічник нотаріуса: 5
   Доступ до Спадкового реєстру: 2
   Послуги з фізичної охорони приміщення: 8
   Зовнішні накопичувачі: 5
```

Рисунок 3.5 — Матриця рангів

```
Експерт 4:
   Робочий ПК нотаріуса: 5
   Антивірусне ПЗ: 7
   Нотаріальна таємниця: 1
   Роутер: 8
   Помічник нотаріуса: 4
   Доступ до Спадкового реєстру: 2
   Послуги з фізичної охорони приміщення: 7
   Зовнішні накопичувачі: 5
```

Рисунок 3.6 — Продовження матриці рангів

Після введення матриці рангів програма автоматично виконує розрахунки та виводить результати ранжування (рисунок 3.7).

```
  РЕЗУЛЬТАТИ РАНЖУВАННЯ:
   Кількість активів (m) = 8
   Кількість експертів (n) = 4
   Ступені свободи (k = m-1) = 7
   Коефіцієнт конкордації W = 0,9184
   X²розр = n×(m-1)×W = 4 × 7 × 0,9184 = 25,72
   X²табл (α=0,05; k=7) = 14,07
    Результат статистично значущий (X²розр > X²табл) - думки експертів узгоджені

  ЦІННІСТЬ АКТИВІВ:
   Робочий ПК нотаріуса: Rj = 14,50, Цінність = 8,812
   Антивірусне ПЗ: Rj = 28,00, Цінність = 7,125
   Нотаріальна таємниця: Rj = 5,00, Цінність = 10,000
   Роутер: Rj = 29,00, Цінність = 7,000
   Помічник нотаріуса: Rj = 15,00, Цінність = 8,750
   Доступ до Спадкового реєстру: Rj = 7,00, Цінність = 9,750
   Послуги з фізичної охорони приміщення: Rj = 27,00, Цінність = 7,250
   Зовнішні накопичувачі: Rj = 18,50, Цінність = 8,312

  НАЙЦІННІШИЙ АКТИВ: Нотаріальна таємниця (ID: 10)
   Цінність: 10,000 (за шкалою 7-10)
```

Рисунок 3.7 — Результати ранжування

Як видно з результатів, найціннішим активом є Нотаріальна таємниця з цінністю 10,000. Саме для цього активу на наступному етапі будуть оцінюватися ризики.

Після визначення найціннішого активу програма автоматично переходить до оцінки ризиків. Програма виводить шкалу та категорії ризиків. Користувач вводить кількість загроз для активу. Наприклад, введемо 6 (рисунок 3.8).

```
  ЕТАП 2: ОЦІНКА РИЗИКІВ ДЛЯ АКТИВУ "Нотаріальна таємниця"
------------------------------------------------

  ШКАЛА ОЦІНЮВАННЯ РИЗИКІВ:
   Ймовірність (P) та Наслідки (C) оцінюються за шкалою 1-5:
      1 - дуже низька / незначні
      2 - низька / малі
      3 - середня / помірні
      4 - висока / значні
      5 - дуже висока / критичні

   Рівень ризику R = P × C
   Категорії ризику:
      R ≥ 20  → Неприйнятний (негайна обробка)
      R ≥ 15  → Високий (першочергова обробка)
      R ≥ 8   → Середній (планова обробка)
      R < 8   → Низький (прийнятний ризик)

Введіть кількість загроз: 6
```

Рисунок 3.8 — Оцінка ризиків. Кількість загроз

Далі користувач вводить шість загроз для активу (рисунок 3.9).

```
  ЗАГРОЗА №1 (для активу: Нотаріальна таємниця)
   Назва загрози: Розголошення нотаріальної таємниці через ненавмисні дії персоналу
   Опис загрози: Недостатня обізнаність персоналу щодо правил роботи з конфіденційною інформацією, відсутність регулярного навчання
   Ймовірність P (1-5): 4
   Наслідки C (1-5): 5

  ЗАГРОЗА №2 (для активу: Нотаріальна таємниця)
   Назва загрози: Витік інформації через соціальну інженерію (фішинг, телефонне шахрайство)
   Опис загрози: Відсутність політики безпеки щодо роботи з електронною поштою та телефонними дзвінками
   Ймовірність P (1-5): 3
   Наслідки C (1-5): 5

  ЗАГРОЗА №3 (для активу: Нотаріальна таємниця)
   Назва загрози: Несанкціонований доступ до документів з нотаріальною таємницею
   Опис загрози: Відсутність контролю доступу до приміщення та архіву, незамикані шафи
   Ймовірність P (1-5): 3
   Наслідки C (1-5): 5

  ЗАГРОЗА №4 (для активу: Нотаріальна таємниця)
   Назва загрози: Перехоплення даних при передачі електронною поштою
   Опис загрози: Відсутність шифрування електронних листів, використання незахищених каналів зв'язку
   Ймовірність P (1-5): 2
   Наслідки C (1-5): 5

  ЗАГРОЗА №5 (для активу: Нотаріальна таємниця)
   Назва загрози: Розголошення таємниці під час розмови в присутності сторонніх осіб
   Опис загрози: Відсутність окремого приміщення для конфіденційних розмов, порушення правил етики
   Ймовірність P (1-5): 4
   Наслідки C (1-5): 4

  ЗАГРОЗА №6 (для активу: Нотаріальна таємниця)
   Назва загрози: Втрата паперових документів з нотаріальною таємницею
   Опис загрози: Відсутність системи обліку та контролю за переміщенням документів
   Ймовірність P (1-5): 2
   Наслідки C (1-5): 5
```

Рисунок 3.9 — Введення загроз

Після введення всіх загроз програма виконує розрахунки та виводить результати (рисунки 3.10, 3.11, 3.12).

```
================================================================================================
ТАБЛИЦЯ – ОЦІНЮВАННЯ РИЗИКІВ ДЛЯ АКТИВУ "Нотаріальна таємниця"
================================================================================================
 №  | Ймовірність P | Наслідки C    | Ризик R = P×C    | Категорія
------------------------------------------------------------------
  1 |             4 |             5 |               20 | Неприйнятний
  2 |             3 |             5 |               15 | Високий
  3 |             3 |             5 |               15 | Високий
  4 |             2 |             5 |               10 | Середній
  5 |             4 |             4 |               16 | Високий
  6 |             2 |             5 |               10 | Середній

================================================================================================
  РЕКОМЕНДАЦІЇ ЩОДО ОБРОБКИ РИЗИКІВ
================================================================================================

  Ризик №1: Розголошення нотар?альної таємниц? через ненавмисн? д?ї персоналу
     НЕГАЙНА ОБРОБКА - необхідне негайне впровадження заходів
    Рівень ризику: 20 (Неприйнятний)
    Актив: Нотаріальна таємниця
    Опис: Недостатня об?знан?сть персоналу щодо правил роботи з конф?денц?йною ?нформац?єю, в?дсутн?сть регулярного навчання

  Ризик №2: Вит?к ?нформац?ї через соц?альну ?нженер?ю (ф?шинг, телефонне шахрайство)
     ПЕРШОЧЕРГОВА ОБРОБКА - пріоритетне впровадження заходів
    Рівень ризику: 15 (Високий)
    Актив: Нотаріальна таємниця
    Опис: В?дсутн?сть пол?тики безпеки щодо роботи з електронною поштою та телефонними дзв?нками

  Ризик №3: Несанкц?онований доступ до документ?в з нотар?альною таємницею
     ПЕРШОЧЕРГОВА ОБРОБКА - пріоритетне впровадження заходів
    Рівень ризику: 15 (Високий)
    Актив: Нотаріальна таємниця
    Опис: В?дсутн?сть контролю доступу до прим?щення та арх?ву, незамикан? шафи
```

Рисунок 3.10 — Оцінка ризиків та рекомендації для 1,2,3 ризиків

```
  Ризик №4: Перехоплення даних при передач? електронною поштою
     ПЛАНОВА ОБРОБКА - включити до плану заходів
    Рівень ризику: 10 (Середній)
    Актив: Нотаріальна таємниця
    Опис: В?дсутн?сть шифрування електронних лист?в, використання незахищених канал?в зв'язку

  Ризик №5: Розголошення таємниц? п?д час розмови в присутност? сторонн?х ос?б
     ПЕРШОЧЕРГОВА ОБРОБКА - пріоритетне впровадження заходів
    Рівень ризику: 16 (Високий)
    Актив: Нотаріальна таємниця
    Опис: В?дсутн?сть окремого прим?щення для конф?денц?йних розмов, порушення правил етики

  Ризик №6: Втрата паперових документ?в з нотар?альною таємницею
     ПЛАНОВА ОБРОБКА - включити до плану заходів
    Рівень ризику: 10 (Середній)
    Актив: Нотаріальна таємниця
    Опис: В?дсутн?сть системи обл?ку та контролю за перем?щенням документ?в
```

Рисунок 3.11 — Рекомендації для 4,5,6 активів

```
  СТАТИСТИЧНИЙ АНАЛІЗ РИЗИКІВ
------------------------------------------------------------
Актив: Нотаріальна таємниця
Всього проаналізовано загроз: 6
  - Неприйнятний рівень: 1
  - Високий рівень: 3
  - Середній рівень: 2
  - Низький рівень: 0

Сумарний показник ризику: 86
Середній рівень ризику: 14,33
```

Рисунок 3.12 — Статистичний аналіз ризиків

В результаті бачимо, що для активу Нотаріальна таємниця виявлено один неприйнятний ризик, три високих та два середніх. Програма надала необхідні рекомендації щодо обробки кожного ризику.

Також за бажанням користувач може зберегти звіт у CSV-файл для подальшого аналізу (рисунок 3.13).

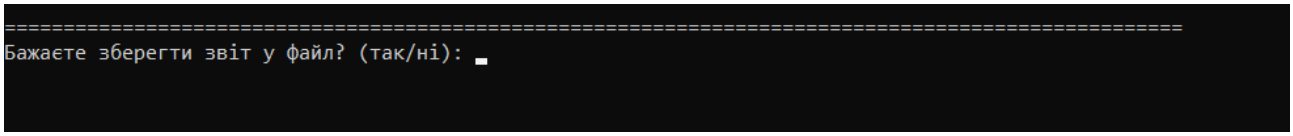


Рисунок 3.13 — Питання про збереження звіту

Введемо «так» і переглянемо сформований звіт (рисунки. 3.14, 3.15, 3.16, 3.17).

Рисунок 3.14 — Повідомлення про успішне збереження звіту у файл

1	РЕЗУЛЬТАТИ ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ		
2	Дата: 22.05.2026 0:56:01		
3	Найцінніший актив: Нотаріальна таємниця (ID: 10, Цінність: 10,000)		
4			
5	ЕТАП 1: РАНЖУВАННЯ АКТИВІВ		
6	Актив	Rj	Цінність
7	Робочий ПК нотаріуса	17	8,5
8	Антивірусне ПЗ	28	7,125
9	Нотаріальна таємниця	5	10
10	Роутер	29	7
11	Помічник нотаріуса	18	8,375
12	Доступ до Спадкового реєстру	7	9,75
13	Послуги з фізичної охорони приміщення	28	7,125
14	Зовнішні накопичувачі	21	8
15	Кількість активів (m)	8	
16	Кількість експертів (n)	4	
17	Ступені свободи (k=m-1)	7	
18	Коефіцієнт конкордації W	0,9296	
19	X^2розр	26,03	
20	X^2табл (α=0,05;k=7)		14,07
21	Статистична значущість	Так (думки узгоджені)	

Рисунок 3.15 — Звіт. Ранжування активів

23	ЕТАП 2: ОЦІНКА РИЗИКІВ		
24	ID	Назва загрози	Актив
25	1	Розголошення нотар?альної таємниц? через ненавмисн? д?ї персоналу	Нотаріальна таємниця
26	2	Вит?к ?нформац?ї через соц?альну ?нженер?ю (ф?шинг, телефонне шахрайство)	Нотаріальна таємниця
27	3	Несанкц?онований доступ до документ?в з нотар?альною таємницею	Нотаріальна таємниця
28	4	Перехоплення даних при передач? електронною поштою	Нотаріальна таємниця
29	5	Розголошення таємниц? п?д час розмови в присутност? сторонн?х ос?б	Нотаріальна таємниця
30	6	Втрата паперових документ?в з нотар?альною таємницею	Нотаріальна таємниця

Рисунок 3.16 — Звіт. Оцінка ризиків (1)

Ймовірність P	Наслідки C	Ризик R=P	Категорія	Опис
4	5	20	Неприйнятний	Недостатня об?знан?сть персоналу щодо правил роботи з конф?денц?йною ?нформац?єю, в?дсутн?сть регулярного навчання
3	5	15	Високий	В?дсутн?сть пол?тики безпеки щодо роботи з електронною поштою та телефонними дзв?нками
3	5	15	Високий	В?дсутн?сть контролю доступу до прим?щення та арх?ву, незамикан? шафи
2	5	10	Середній	В?дсутн?сть шифрування електронних лист?в, використання незахищених канал?в зв'язку
4	4	16	Високий	В?дсутн?сть окремого прим?щення для конф?денц?йних розмов, порушення правил етики
2	5	10	Середній	В?дсутн?сть системи обл?ку та контролю за перем?щенням документ?в

Рисунок 3.17 — Звіт. Оцінка ризиків (2)

Після завершення оцінки ризиків для найціннішого активу програма запитує, чи бажає користувач оцінити ризики інших активів.

```
Чи бажаєте оцінити ризики для іншого активу? (так/ні): так
```

Рисунок 3.18 — Питання про оцінку ризиків інших активів

Програма повторно дублює список активів (рисунок 3.2). Користувач вводить ID активу.

```
Введіть ID активу для оцінки ризиків: 32
```

Рисунок 3.19 — Вибір активу

Далі так само як для активу «Нотаріальна таємниця» виводиться шкала та категорії ризику (рисунок 3.7). Вводимо кількість загроз та їх характеристики.

```
Введіть кількість загроз для цього активу: 3

 ЗАГРОЗА №1 (для активу: Сейф)
   Назва загрози: Фізичне зламування сейфа
   Опис загрози: Ненадійна конструкція, відсутність сигналізації
   Ймовірність P (1-5): 2
   Наслідки C (1-5): 5

 ЗАГРОЗА №2 (для активу: Сейф)
   Назва загрози: Втрата ключа або коду доступу
   Опис загрози: Відсутність резервного зберігання ключа
   Ймовірність P (1-5): 3
   Наслідки C (1-5): 4

 ЗАГРОЗА №3 (для активу: Сейф)
   Назва загрози: Пошкодження сейфа при пожежі
   Опис загрози: Відсутність протипожежного захисту
   Ймовірність P (1-5): 2
   Наслідки C (1-5): 5
```

Рисунок 3.20 — Загрози для активу «Сейф»

Отримуємо таблицю оцінювання ризиків, рекомендації та статистичний аналіз (рисунки 3.21, 3.22).

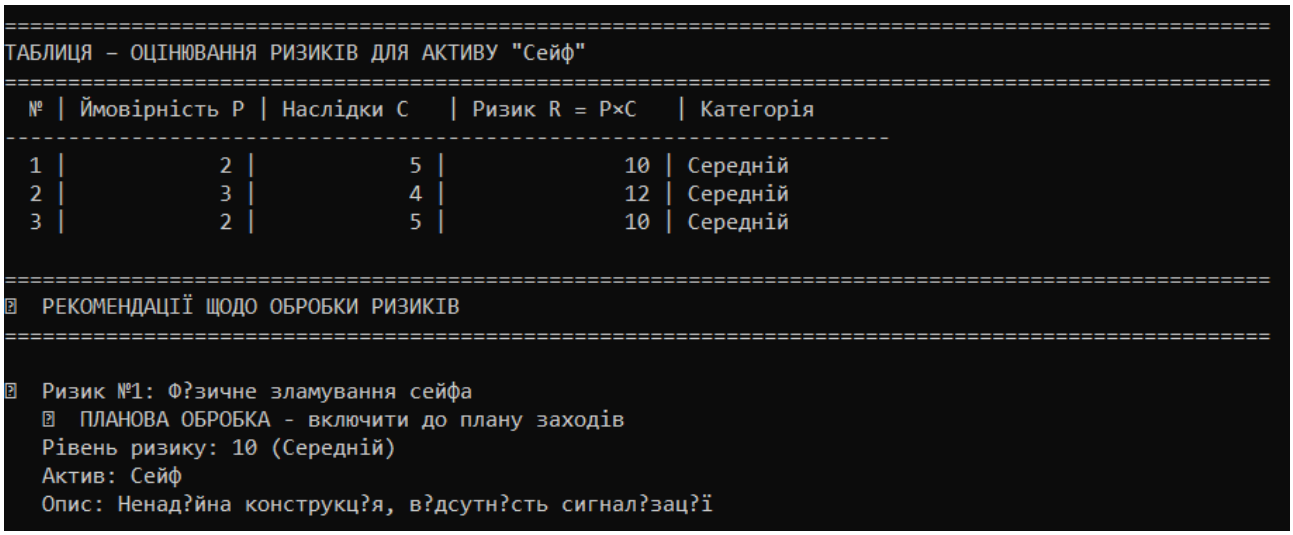


Рисунок 3.21 — Таблиця оцінювання ризиків для активу «Сейф»

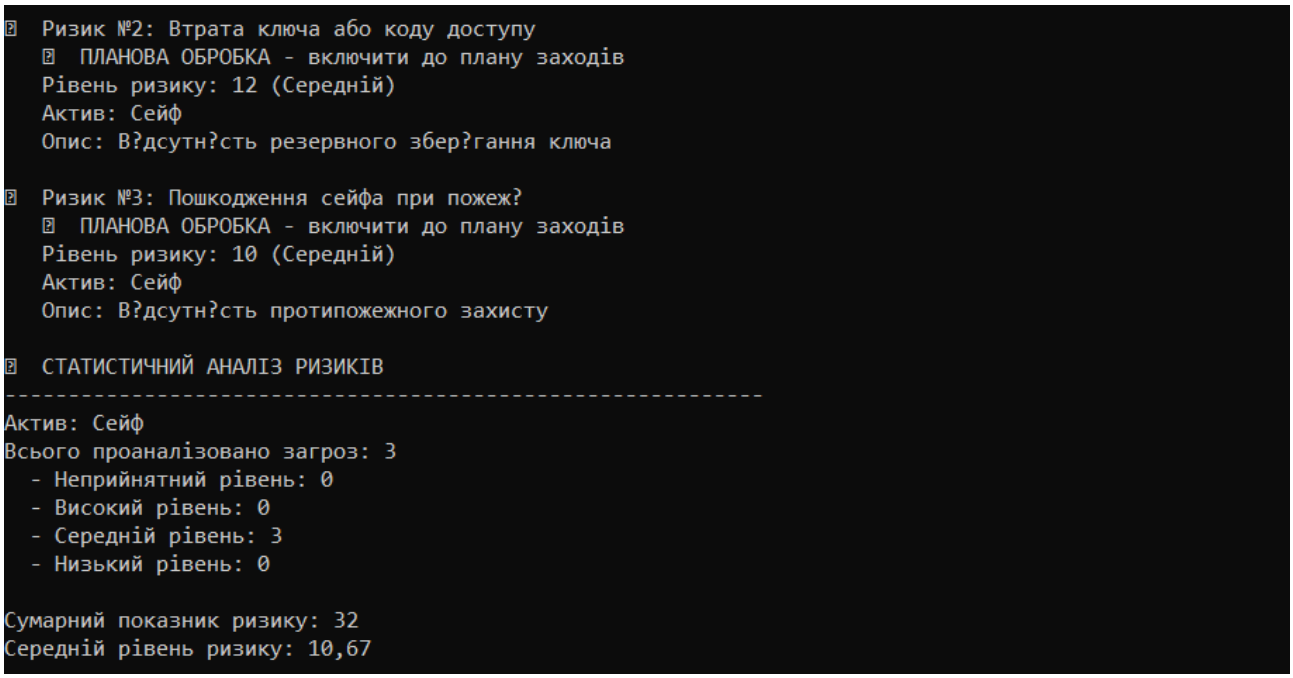


Рисунок 3.22 — Рекомендації та статистичний аналіз

Програма знову пропонує зберегти звіт (рисунок 3.12). Та запитує чи бажаємо оцінити ризики для інших активів. Вводимо ні — програма завершує роботу (рисунок 3.23).

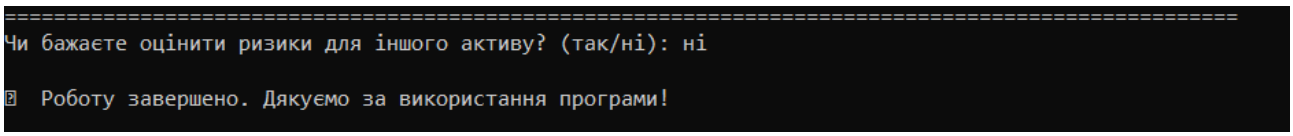


Рисунок 3.23 — Роботу завершено

3.7 Перевірка програми на достовірність розрахунків

Для підтвердження коректності роботи розробленої системи оцінки ризиків інформаційної безпеки було виконано перевірку розрахунків. Цей важливий етап передбачає проведення серії тестових обчислень з різними вхідними даними. Метою перевірки є впевненість у точності та правильності результатів, які формує програма.

1. Ранжування активів.

Кількість активів (m) = 8

Кількість експертів (n) = 4

Таблиця 3.1 — Вхідна матриця рангів

Експерт	Робочий ПК нотаріуса	Антивірусне ПЗ	Нотаріальна таємниця	Роутер	Помічник нотаріуса	Доступ до Спадкового	Послуги з фіз. охорони	Зовнішні накопичувачі
1	4	7	1	8	5	1	6	5
2	5	8	1	7	4	2	7	6
3	3	6	2	6	5	2	8	5
4	5	7	1	8	4	2	7	5

Таблиця 3.2 — Нормалізована матриця (середні ранги при зв'язаних рангах)

Експерт	Робочий ПК нотаріуса	Антивірусне ПЗ	Нотаріальна таємниця	Роутер	Помічник нотаріуса	Доступ до Спадкового	Послуги з фіз. охорони	Зовнішні накопичувачі	Ri
1	3	7	1,5	8	4,5	1,5	6	4,5	36
2	4	8	1	6,5	3	2	6,5	5	36
3	3	6,5	1,5	6,5	4,5	1,5	8	4,5	36
4	4,5	6,5	1	8	3	2	6,5	4,5	36

Таблиця 3.3 — Суми рангів Rj, середнє T*, відхилення Dj та Dj^2

Rj	14,5	28	5	29	15	7	27	18,5	ΣDj^2
T* = n*(m+1)/2	18								
Dj = Rj - T*	-3,5	10	-13	11	-3	-11	9	0,5	
Dj^2	12,25	100	169	121	9	121	81	0,25	613,5

Таблиця 3.4 — Поправка на зв’язні ранги Ti=Σ(t^3-t)/12

Групи зв'язаних рангів	[2,2]	[2]	[2,2,2]	[2,2]	ΣTi
Ti=Σ(t^3-t)/12	1	0,5	1,5	1	4

Коефіцієнт конкордації W за формулою 2.1:

$$W = \frac{12*613,5}{4^2*(8^3-8)-4*4} = \frac{7362}{16*504-16} = 0,918 \quad (3.1)$$

Перевірка значущості W - Критерій Пірсона X^2 за формулою 2.2:

$$X^2\text{розр} = 4 * (8-1) * 0,918 = 25,716 \quad (3.2)$$

Цінність активів в діапазоні оцінювання від 7 до 10 за формулою 2.3:

Таблиця 3.5 — Цінність активів

Актив	Rj	Цінність
Робочий ПК нотаріуса	14,5	8,8125
Антивірусне ПЗ	28	7,125
Нотаріальна таємниця	5	10
Роутер	29	7
Помічник нотаріуса	15	8,75
Доступ до Спадкового реєстру	7	9,75
Послуги з фіз. охорони приміщення	27	7,25
Зовнішні накопичувачі	18,5	8,3125

2. Оцінка ризиків за формулою 2.4.

Таблиця 3.6 — Оцінка ризиків

№	Назва загрози	Опис загрози	P	C	R
1	Розголошення нотаріальної таємниці через	Недостатня обізнаність персоналу щодо правил роботи з конфіденційною інформацією,	4	5	20

Продовження таблиці 3.6

		відсутність регулярного навчання			
2	Витік інформації через соціальну інженерію (фішинг, телефонне шахрайство)	Відсутність політики безпеки щодо роботи з електронною поштою та телефонними дзвінками	3	5	15
3	Несанкціонований доступ до документів з нотаріальною таємницею	Відсутність контролю доступу до приміщення та архіву, незамикані шафи	3	5	15
4	Перехоплення даних при передачі електронною поштою	Відсутність шифрування електронних листів, використання незахищених каналів зв'язку	2	5	10
5	Розголошення таємниці під час розмови в присутності сторонніх осіб	Відсутність окремого приміщення для конфіденційних розмов, порушення правил етики	4	4	16
6	Втрата паперових документів з нотаріальною таємницею	Відсутність системи обліку та контролю за переміщенням документів	2	5	10

Сумарний показник ризику = 20+15+15+10+16+10=86 (3.3)

Середній рівень ризику = $\frac{86}{6} = 14{,}33$ (3.4)

Таким чином, перевіривши всі розрахунки можна зробити висновок, що програма розраховує правильно.

3.8 Висновок до розділу 3

У третьому розділі «Програмна реалізація системи оцінювання ризиків інформаційної безпеки нотаріальної контори» дипломної роботи було реалізовано програмну систему компонентів оцінки ризиків інформаційної безпеки нотаріальної контори. Відповідно до міжнародного стандарту ДСТУ ISO/IEC 27005, процес управління ризиками складається з кількох етапів: встановлення контексту, оцінювання ризиків, обробка ризиків, прийняття ризиків, моніторинг та аналіз, комунікація та консультування. Розроблена програма автоматизує один із етапів цього процесу - оцінювання ризиків.

У рамках програмної реалізації було створено інструмент, який дозволяє виконати наступні завдання в межах етапу оцінювання ризиків:

1) Ідентифікація активів - користувач обирає активи з попередньо визначеного списку для подальшого ранжування.
2) Аналіз ризиків - на основі експертних оцінок (матриці рангів) програма розраховує суми рангів Rj, цінність активів, коефіцієнт конкордації Кендалла W та критерій Пірсона X^2, що дозволяє оцінити узгодженість думок експертів та статистичну значущість результатів.
3) Оцінка ризиків - після визначення найціннішого активу програма дозволяє оцінити ризики для цього активу за параметрами ймовірності P та наслідків A, розраховує рівень ризику та визначає категорію ризику згідно з встановленою шкалою.
4) Додатково можна провести оцінку ризиків для інших активів за бажанням користувача.

Таким чином, розроблена програма повністю реалізує етап оцінювання ризиків згідно з ДСТУ ISO/IEC 27005, що є фундаментом для подальших етапів управління ризиками. Отримані результати оцінювання є вхідними даними для

наступних етапів управління ризиками, які можуть бути реалізовані в подальших дослідженнях.

Розроблена система автоматизує процес оцінювання ризиків, що значно підвищує ефективність та точність розрахунків, зменшує вплив людського фактору та забезпечує можливість швидкого перерахунку при зміні вхідних даних. Це сприяє своєчасному виявленню загроз та оцінці ризиків, що є необхідною умовою для прийняття обґрунтованих рішень щодо захисту інформаційних активів нотаріальної контори в рамках загальної системи управління інформаційною безпекою.

ВИСНОВКИ

У результаті виконання дипломної роботи було проведено дослідження процесу управління ризиками в системі управління інформаційною безпекою нотаріальної контори. Цифровізація нотаріальної діяльності, інтеграція з державними електронними реєстрами та використання кваліфікованого електронного підпису суттєво підвищили ефективність роботи нотаріусів, але водночас створили нові загрози інформаційній безпеці, які раніше не були характерними для нотаріату.

Українські нотаріальні контори часто нехтують системним підходом до захисту інформації, впроваджуючи заходи безпеки без попереднього аналізу ризиків та обґрунтування їх доцільності. Це призводить або до надмірних витрат на захист, або до недостатнього рівня безпеки, що може мати критичні наслідки, включаючи розголошення нотаріальної таємниці, компрометацію кваліфікованого електронного підпису або блокування доступу до державних реєстрів. Це обґрунтовує актуальність подальших досліджень по удосконаленню системи управління ризиками в нотаріальній діяльності.

Для вирішення цих проблем у роботі запропоновано використовувати методологію управління ризиками згідно з міжнародним стандартом ДСТУ ISO/IEC 27005. На відміну від фрагментарного підходу, управління ризиками дозволяє обґрунтовано визначати пріоритетні напрями захисту та пропорційно розподіляти ресурси. Як показало дослідження, найбільш доцільним для нотаріальної контори є комбінований (напівкількісний) підхід до оцінювання ризиків, який поєднує простоту якісного аналізу з об’єктивністю кількісних методів.

Для автоматизації процесу оцінювання ризиків розроблено програмну систему мовою C# у середовищі Microsoft Visual Studio. Обрано модульну архітектуру, яка включає модуль вводу даних, модуль обробки даних, модуль розрахунків та модуль виводу результатів. Розроблена програма дозволяє виконати ранжування активів на основі експертних оцінок, розрахувати коефіцієнт конкордації Кендала та критерій Пірсона, автоматично визначити

найцінніший актив, оцінити ризики для нього за параметрами ймовірності та наслідків, розрахувати рівень ризику, визначити категорію ризику, сформувати рекомендації щодо обробки ризиків, зберегти результати у CSV-файл для подальшого аналізу, а також оцінити ризики для інших активів зі списку.

Розроблена система реалізує ключовий етап управління ризиками згідно з ДСТУ ISO/IEC 27005 - етап оцінювання ризиків, що є фундаментом для подальших етапів обробки та моніторингу ризиків. Впровадження результатів дослідження дозволить нотаріальним конторам обґрунтовано розподіляти ресурси на захист інформації, документально підтвердити виконання вимог законодавства та підвищити загальний рівень інформаційної безпеки.

Перспективними напрямами подальшого розвитку є доповнення програми функцією автоматичного формування плану заходів з обробки виявлених ризиків, підключення до баз даних для накопичення історії оцінювань, а також створення графічного інтерфейсу для більш зручної взаємодії з користувачем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про нотаріат [Електронний ресурс]: Закон України від 2 вересня 1993 р. № 3425-XII (зі змінами). —URL: https://zakon.rada.gov.ua/laws/show/3425-12#Text (дата звернення: 01.04.2026).
2. Про інформацію [Електронний ресурс]: Закон України від 2 жовтня 1992 р. № 2657-XII (зі змінами). – URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 01.04.2026).
3. Про захист персональних даних [Електронний ресурс]: Закон України від 1 грудня 2022 р. № 2849-IX. – URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 01.04.2026).
4. Про основні засади забезпечення кібербезпеки України [Електронний ресурс]: Закон України від 5 жовтня 2017 р. № 2163-VIII. – URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 01.04.2026).
5. Про електронну ідентифікацію та електронні довірчі послуги [Електронний ресурс] : Закон України від 5 жовтня 2017 р. № 2155-VIII. – URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 01.04.2026).
6. Про затвердження Положення про вимоги до робочого місця (контори) приватного нотаріуса та здійснення контролю за організацією нотаріальної діяльності [Електронний ресурс]: Наказ Міністерства юстиції України від 23 грудня 2010 р. № 3306/5. – URL: https://zakon.rada.gov.ua/laws/show/z0406-11#Text (дата звернення: 01.04.2026).
7. Про затвердження Порядку вчинення нотаріальних дій нотаріусами України [Електронний ресурс]: Наказ Міністерства юстиції України від 22 лютого 2012 р. № 296/5. – URL: https://zakon.rada.gov.ua/laws/show/z0282-12#Text (дата звернення: 01.04.2026).
8. Про затвердження Правил ведення нотаріального діловодства [Електронний ресурс]: Наказ Міністерства юстиції України від 22 грудня 2010 р. № 3253/5. – URL: https://zakon.rada.gov.ua/laws/show/z1318-10#Text

9. ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013, IDT). Чинний від 2016-07-01. Вид. офіц. Київ : ДП «УкрНДНЦ», 2016. 28 с.
10. ДСТУ ISO/IEC 27002:2015. Інформаційні технології. Методи захисту. Кодекс практики для управління інформаційною безпекою (ISO/IEC 27002:2013, IDT). Чинний від 2016-07-01. Вид. офіц. Київ : ДП «УкрНДНЦ», 2016. 102 с.
11. ДСТУ ISO/IEC 27005:2015. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2011, IDT). Чинний від 2016-07-01. Вид. офіц. Київ : ДП «УкрНДНЦ», 2016. 72 с.
12. NIST SP 800-30 Rev. 1. Guide for Conducting Risk Assessments. – Gaithersburg : National Institute of Standards and Technology, 2012. – 95 p.
13. NIST SP 800-39. Managing Information Security Risk: Organization, Mission, and Information System View. – Gaithersburg : National Institute of Standards and Technology, 2011. – 121 p.
14. IEC 31010:2019. Risk management – Risk assessment techniques. – Geneva : International Electrotechnical Commission, 2019. – 216 p.
15. Ізмайлова О.В. Теорія прийняття рішень : метод. вказівки. – Київ : КНУБА, 2024. – 39 с.
16. Microsoft. STRIDE Threat Modeling [Електронний ресурс]. – URL: https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats (дата звернення: 10.04.2026).
17. В.Л. Бурячок, С.В.Толюпа, А.О. Аносов, В.А.Козачок, Н.В. Лукова-Чуйко Системний аналіз інформаційної безпеки : підручник. – Київ : ДУТ, 2015. – 345 с.
18. Гайворонський М.В., Новиков О.М. Безпека інформаційно-комунікаційних систем. – Київ : Вид. група BHV, 2009. – 608 с.
19. Литвинов В.В., Петренко С.А. Управління ризиками інформаційної безпеки : методологія та практика. – Київ : Центр учбової літератури, 2019. – 312 с.

20. Saaty T.L. The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation. – Pittsburgh : RWS Publications, 1990. – 287 p.
21. Паспорт кваліфікаційної роботи бакалавра спеціальності 125 «Кібербезпека та захист інформації». – Київ : КНУБА, [б. р.]. – 8 с.
22. Загурський О.А. Управління ризиками. - К.: Університет Україна, 2016. - 244 с.
23. Корченко О.Г., Казмірчук С.В., Ахметов Б.Б., Прикладні системи оцінювання ризиків інформаційної безпеки. Монографія, Київ, ЦП «Компринт», 2017 – 435 с.
24. Kusumah R.N., Hanim L. Legal Protection of Notaries in Executing Their Office in the Digital Era // SANLaR. – 2025. – Vol. 7, No. 4. – P. 351–358.
25. Secura. Risk Assessment Standards for ICS Environments [Електронний ресурс]. – URL: https://cybersecurity.bureauveritas.com/uploads/whitepapers/Risk-Assessment-Standards-for-ICS-Environments.pdf (дата звернення: 05.05.2026).

Додаток А Ранжування активів

Вихідні ранги								
Експерт	Критичні бази даних	Нотаріальна	Паперовий архів	Доступ до держ.	Токен (носій ЕЦП)	Персональні дані	Антивірусне ПЗ	ПК нотаріуса
1	1	3	2	3	4	5	6	7
2	1	2	3	3	4	5	5	5
3	2	1	3	5	4	6	7	7
4	1	7	7	3	5	6	4	2

Нормалізована матриця (середні ранги при зв'язаних рангах)									
Експерт	Критичні бази даних	Нотаріальна таємниця	Паперовий архів	Доступ до держ. реєстрів	Токен (носій ЕЦП)	Персональні дані клієнтів	Антивірусне ПЗ	ПК нотаріуса	Ri
1	1	3	3	3	5	6	7	8	36
2	1	2	3,5	3,5	5	7	7	7	36
3	1	2	3	4	5	6	7,5	7,5	36
4	1	2,5	2,5	4	5	6	7	8	36

Суми рангів Rj, середнє T*, відхилення Dj та Dj^2									
Rj	4	9,5	12	14,5	20	25	28,5	30,5	ΣDj^2
T* = n*(m+1)/2	18								

Dj = Rj - T*	-14	-8,5	-6	-3,5	2	7	10,5	12,5	
Dj^2	196	72,25	36	12,25	4	49	110,25	156,25	636

Поправка на зв'язані ранги Ti=Σ(t^3-t)/12					
Групи зв'язаних рангів	[2,2]	[2]	[2,2,2]	[2,2]	ΣTi
Ti=Σ(t^3-t)/12	1	0,5	1,5	1	4

Коефіцієнт конкордації W	
n (кількість експертів)	4
m (кількість активів)	8
ΣDj^2	636
ΣTi	4
W =	0,948310139

Перевірка значущості W - Критерій Пірсона X^2	
X^2розр = n*(m-1)*W	25,71611
Ступені свободи k=m-1	7
X^2табл (α=0,05; k=7)	14,1

Додаток Б Код програми

```
using System;
using System.Collections.Generic;
using System.IO;
using System.Linq;

namespace RiskAssessmentTool
{
    public class Asset
    {
        public int Id { get; set; }
        public string Name { get; set; }
        public double Rj { get; set; }
        public double Value { get; set; }

        public Asset(int id, string name)
        {
            Id = id;
            Name = name;
            Rj = 0;
            Value = 0;
        }
    }
    public class Risk
    {
```

```
public int Id { get; set; }
public string Name { get; set; }
public string Description { get; set; }
public int AssetId { get; set; }
public string AssetName { get; set; }
public int Probability { get; set; }
public int Consequences { get; set; }
public int RiskLevel { get; set; }
public string Category { get; set; }

public void CalculateRiskLevel()
{
    RiskLevel = Probability * Consequences;
    DetermineCategory();
}
private void DetermineCategory()
{
    if (RiskLevel >= 20)
        Category = "Неприйнятний";
    else if (RiskLevel >= 15)
        Category = "Високий";
    else if (RiskLevel >= 8)
        Category = "Середній";
    else
        Category = "Низький";
```

```
        }
        public string GetRecommendation()
        {
            switch (Category)
            {
                case "Неприйнятний":
                    return "НЕГАЙНА ОБРОБКА - необхідне
негайне впровадження заходів";
                case "Високий":
                    return "ПЕРШОЧЕРГОВА ОБРОБКА - пріоритетне
впровадження заходів";
                case "Середній":
                    return "ПЛАНОВА ОБРОБКА - включити до
плану заходів";
                default:
                    return "ПРИЙНЯТНИЙ РИЗИК - додаткові
заходи не потрібні";
            }
        }
    }
    public class RankingCalculator
    {
        private int nExperts;
        private List<Asset> assets;
        private double[,] ranks;
```

```
        public RankingCalculator(int experts, List<Asset>
assetList)
        {
            nExperts = experts;
            assets = assetList;
            ranks = new double[experts, assets.Count];
        }
        public void InputRanks()
        {
            Console.WriteLine("\n ВВЕДЕННЯ МАТРИЦІ РАНГІВ");
            Console.WriteLine("   (менший ранг = вища
цінність, від 1 до {0})", assets.Count);
            Console.WriteLine("   Увага: при однаковій
цінності активів можна ставити однакові ранги!\n");
            for (int i = 0; i < nExperts; i++)
            {
                Console.WriteLine($"Експерт {i + 1}:");
                for (int j = 0; j < assets.Count; j++)
                {
                    Console.Write($"   {assets[j].Name}: ");
                    ranks[i, j] =
double.Parse(Console.ReadLine());
                }
                Console.WriteLine();
            }
        }
```

```
        public void CalculateSumRanks()
        {
            for (int j = 0; j < assets.Count; j++)
            {
                assets[j].Rj = 0;
                for (int i = 0; i < nExperts; i++)
                    assets[j].Rj += ranks[i, j];
            }
        }
        public void CalculateAssetValues()
        {
            double minRj = assets.Min(a => a.Rj);
            double maxRj = assets.Max(a => a.Rj);
            for (int j = 0; j < assets.Count; j++)
            {
                assets[j].Value = 10.0 - (assets[j].Rj -
minRj) / (maxRj - minRj) * 3.0;
            }
        }
        public double CalculateConcordance(out double
chiSquared)
        {
            int m = assets.Count;
            double T = nExperts * (m + 1.0) / 2.0;
            double sumD2 = 0;
```

```
            foreach (var asset in assets)
            {
                double d = asset.Rj - T;
                sumD2 += d * d;
            }
            double sumTi = 0;
            for (int i = 0; i < nExperts; i++)
            {
                var grouped = new List<double>();
                for (int j = 0; j < m; j++)
                    grouped.Add(ranks[i, j]);

                var groups = grouped.GroupBy(r => r).Where(g
=> g.Count() > 1);
                foreach (var g in groups)
                {
                    int t = g.Count();
                    sumTi += (t * t * t - t) / 12.0;
                }
            }
            double numerator = 12 * sumD2;
            double denominator = nExperts * nExperts * (m * m
* m - m) - 12 * sumTi;
            double W = numerator / denominator;
            chiSquared = nExperts * (m - 1) * W;
```

```
            return W;
        }
        public List<Asset> GetAssets() => assets;
    }
    class Program
    {
        static double GetChiSquaredTableValue(int
degreesOfFreedom)
        {
            Dictionary<int, double> chiSquaredTable = new
Dictionary<int, double>
            {
                { 1, 3.84 }, { 2, 5.99 }, { 3, 7.81 }, { 4,
9.49 },
                { 5, 11.07 }, { 6, 12.59 }, { 7, 14.07 }, { 8,
15.51 },
                { 9, 16.92 }, { 10, 18.31 }, { 12, 21.03 }, {
15, 25.00 },
                { 20, 31.41 }
            };
            if (chiSquaredTable.ContainsKey(degreesOfFreedom))
                return chiSquaredTable[degreesOfFreedom];
            return 14.07;
        }
        static List<Asset> GetPredefinedAssets()
        {
```

```
            return new List<Asset>
            {
                new Asset(1, "БФП"),
                new Asset(2, "Робочий ПК нотаріуса"),
                new Asset(3, "Робочий ПК помічника"),
                new Asset(4, "Засоби криптографічного захисту
(агент підпису)"),
                new Asset(5, "Антивірусне ПЗ"),
                new Asset(6, "Операційна система (Windows)"),
                new Asset(7, "Ноутбук"),
                new Asset(8, "Пакети Microsoft Office"),
                new Asset(9, "Персональні дані клієнтів"),
                new Asset(10, "Нотаріальна таємниця"),
                new Asset(11, "Електронний архів (Критичні
бази даних)"),
                new Asset(12, "Ключі КЕП"),
                new Asset(13, "Паролі доступу до держ.
реєстрів"),
                new Asset(14, "Фінансові документи"),
                new Asset(15, "Роутер"),
                new Asset(16, "Токен"),
                new Asset(17, "Веб-браузер"),
                new Asset(18, "Нотаріус"),
                new Asset(19, "Помічник нотаріуса"),
                new Asset(20, "Технічний персонал"),
                new Asset(21, "Клієнти"),
```

```
                new Asset(22, "Доступ до Єдиного реєстру
нотаріальних дій"),
                new Asset(23, "Доступ до Державного реєстру
речових прав на нерухоме майно"),
                new Asset(24, "Доступ до Єдиного державного
реєстру юридичних осіб"),
                new Asset(25, "Доступ до Спадкового реєстру"),
                new Asset(26, "Доступ до мережі Інтернет"),
                new Asset(27, "Електропостачання"),
                new Asset(28, "Послуги кваліфікованого
надавача електронних довірчих послуг"),
                new Asset(29, "Послуги з фізичної охорони
приміщення"),
                new Asset(30, "Приміщення нотаріальної
контори"),
                new Asset(31, "Архівне приміщення (Паперовий
архів)"),
                new Asset(32, "Сейф"),
                new Asset(33, "Зовнішні накопичувачі")
            };
        }
        static void DisplayFullAssetList(List<Asset> assets)
        {
            Console.WriteLine("\n СПИСОК АКТИВІВ НОТАРІАЛЬНОЇ
КОНТОРИ (33 активи):");
            Console.WriteLine(new string('-', 80));
            for (int i = 0; i < assets.Count; i += 2)
            {
```

```
                if (i + 1 < assets.Count)
                    Console.WriteLine($"   {assets[i].Id,2}. 
{assets[i].Name,-42} {assets[i + 1].Id,2}. {assets[i + 
1].Name}");
                else
                    Console.WriteLine($"   {assets[i].Id,2}. 
{assets[i].Name}");
            }
            Console.WriteLine(new string('-', 80));
        }
        static List<Asset> SelectAssetsForRanking(List<Asset> 
allAssets)
        {
            DisplayFullAssetList(allAssets);
            Console.Write("\nВведіть ID активів для ранжування 
(через кому, наприклад: 11,10,31,22,16,9,5,2): ");
            string input = Console.ReadLine();
            var selectedIds = 
input.Split(',').Select(int.Parse).ToList();
            var selectedAssets = allAssets.Where(a => 
selectedIds.Contains(a.Id)).ToList();
            if (selectedAssets.Count == 0)
            {
                Console.WriteLine("Активів не вибрано. 
Використовуються всі активи.");
                return allAssets;
            }
```

```
            Console.WriteLine($"\n Обрано
{selectedAssets.Count} активів для ранжування:");

            foreach (var asset in selectedAssets)

            {

                Console.WriteLine($"   - {asset.Name} (ID
{asset.Id})");

            }

            return selectedAssets;

        }

        static void AssessRisksForAsset(Asset asset, double W,
double chiSquared,

                                        int degreesOfFreedom,
double chiSquaredTable, int nExperts,

                                        List<Asset>
rankingAssets, bool isFirstAsset = false)

        {

            if (!isFirstAsset)

            {

                Console.Clear();

                Console.WriteLine(new string('=', 100));

                Console.WriteLine($"ОЦІНКА РИЗИКІВ ДЛЯ АКТИВУ
\"{asset.Name}\" (ID: {asset.Id})");

                Console.WriteLine(new string('=', 100));

            }

            var rankedAsset = rankingAssets.FirstOrDefault(a
=> a.Id == asset.Id);

            if (rankedAsset != null)
```

```
            {
                Console.WriteLine($"   Цінність активу: 
{rankedAsset.Value:F3} (за шкалою 7-10)");
                Console.WriteLine($"   Сума рангів (Rj): 
{rankedAsset.Rj:F2}");
            }
            else
            {
                Console.WriteLine($"   (Актив не брав участі в 
ранжуванні)");
            }
            Console.WriteLine();


            Console.WriteLine("\n ШКАЛА ОЦІНЮВАННЯ РИЗИКІВ:");
            Console.WriteLine("   Ймовірність (P) та Наслідки 
(C) оцінюються за шкалою 1-5:");
            Console.WriteLine("      1 - дуже низька / 
незначні");
            Console.WriteLine("      2 - низька / малі");
            Console.WriteLine("      3 - середня / помірні");
            Console.WriteLine("      4 - висока / значні");
            Console.WriteLine("      5 - дуже висока / 
критичні");
            Console.WriteLine("\n   Рівень ризику R = P × C");
            Console.WriteLine("   Категорії ризику:");
            Console.WriteLine("      R ≥ 20  → Неприйнятний 
(негайна обробка)");
```

```
            Console.WriteLine("      R ≥ 15  → Високий
(першочергова обробка)");

            Console.WriteLine("      R ≥ 8   → Середній
(планова обробка)");

            Console.WriteLine("      R < 8   → Низький
(прийнятний ризик)");


            Console.Write("\nВведіть кількість загроз для
цього активу: ");

            int nRisks = int.Parse(Console.ReadLine());

            List<Risk> risks = new List<Risk>();

            for (int r = 0; r < nRisks; r++)

            {

                Console.WriteLine($"\n ЗАГРОЗА №{r + 1} (для
активу: {asset.Name})");

                Console.Write("   Назва загрози: ");

                string name = Console.ReadLine();

                Console.Write("   Опис загрози: ");

                string description = Console.ReadLine();

                Console.Write("   Ймовірність P (1-5): ");

                int prob = int.Parse(Console.ReadLine());

                Console.Write("   Наслідки C (1-5): ");

                int cons = int.Parse(Console.ReadLine());

                Risk risk = new Risk

                {

                    Id = r + 1,
```

```
                    Name = name,
                    Description = description,
                    AssetId = asset.Id,
                    AssetName = asset.Name,
                    Probability = prob,
                    Consequences = cons
                };

                risk.CalculateRiskLevel();
                risks.Add(risk);
            }
            Console.WriteLine("\n" + new string('=', 100));
            Console.WriteLine($"ТАБЛИЦЯ – ОЦІНЮВАННЯ РИЗИКІВ
ДЛЯ АКТИВУ \"{asset.Name}\"");
            Console.WriteLine(new string('=', 100));
            Console.WriteLine($"{"№",3} | {"Ймовірність P",-
12} | {"Наслідки C",-12} | {"Ризик R = P×C",-15} |
{"Категорія",-14}");
            Console.WriteLine(new string('-', 70));
            foreach (var risk in risks)
            {
                Console.WriteLine($"{risk.Id,3} |
{risk.Probability,12} | {risk.Consequences,12} |
{risk.RiskLevel,15} | {risk.Category,-14}");
            }
            Console.WriteLine("\n" + new string('=', 100));
```

```
            Console.WriteLine("РЕКОМЕНДАЦІЇ ЩОДО ОБРОБКИ
РИЗИКІВ");
            Console.WriteLine(new string('=', 100));


            foreach (var risk in risks)
            {
                string emoji = risk.Category == "Неприйнятний"
? "🚨" :
                                    risk.Category == "Високий" ?
"⚠️" :
                                    risk.Category == "Середній" ?
"📋" : "✅";
                Console.WriteLine($"\n{emoji} Ризик
№{risk.Id}: {risk.Name}");
                Console.WriteLine($"
{risk.GetRecommendation()}");
                Console.WriteLine($"   Рівень ризику:
{risk.RiskLevel} ({risk.Category})");
                Console.WriteLine($"   Актив:
{risk.AssetName}");
                Console.WriteLine($"   Опис:
{risk.Description}");
            }
            Console.WriteLine("\n СТАТИСТИЧНИЙ АНАЛІЗ
РИЗИКІВ");
            Console.WriteLine(new string('-', 60));
            int highCount = risks.Count(r => r.Category ==
"Високий");
```

```
            int mediumCount = risks.Count(r => r.Category ==
"Середній");

            int lowCount = risks.Count(r => r.Category ==
"Низький");

            int unacceptableCount = risks.Count(r =>
r.Category == "Неприйнятний");



            Console.WriteLine($"Актив: {asset.Name}");

            Console.WriteLine($"Всього проаналізовано загроз:
{risks.Count}");

            Console.WriteLine($"  - Неприйнятний рівень:
{unacceptableCount}");

            Console.WriteLine($"  - Високий рівень:
{highCount}");

            Console.WriteLine($"  - Середній рівень:
{mediumCount}");

            Console.WriteLine($"  - Низький рівень:
{lowCount}");

            int totalRisk = risks.Sum(r => r.RiskLevel);

            double avgRisk = risks.Average(r => r.RiskLevel);

            Console.WriteLine($"\nСумарний показник ризику:
{totalRisk}");

            Console.WriteLine($"Середній рівень ризику:
{avgRisk:F2}");

            Console.WriteLine("\n" + new string('=', 100));

            Console.Write("Бажаєте зберегти звіт для цього
активу у файл? (так/ні): ");

            string saveChoice = Console.ReadLine();
```

```
            if (saveChoice?.ToLower() == "так" ||
saveChoice?.ToLower() == "yes")

            {

                SaveReport(risks, asset, rankingAssets, W,
chiSquared, degreesOfFreedom, chiSquaredTable, nExperts);

            }

        }

        static void SaveReport(List<Risk> risks, Asset
selectedAsset, List<Asset> rankingAssets,

                               double W, double chiSquared, int
degreesOfFreedom, double chiSquaredTable, int nExperts)

        {

            string fileName =
$"RiskReport_{selectedAsset.Name}_{DateTime.Now:yyyyMMdd_HHmms
s}.csv";

            string filePath =
Path.Combine(Directory.GetCurrentDirectory(), fileName);



            using (StreamWriter writer = new
StreamWriter(filePath, false, System.Text.Encoding.UTF8))

            {

                writer.WriteLine("РЕЗУЛЬТАТИ ОЦІНКИ РИЗИКІВ
ІНФОРМАЦІЙНОЇ БЕЗПЕКИ");

                writer.WriteLine($"Дата: {DateTime.Now}");

                writer.WriteLine($"Актив: {selectedAsset.Name}
(ID: {selectedAsset.Id})");



                var rankedAsset =
rankingAssets.FirstOrDefault(a => a.Id == selectedAsset.Id);
```

```
                if (rankedAsset != null)
                {
                    writer.WriteLine($"Цінність активу: 
{rankedAsset.Value:F3}");
                    writer.WriteLine($"Сума рангів (Rj): 
{rankedAsset.Rj:F2}");
                }
                writer.WriteLine();
                writer.WriteLine("РАНЖУВАННЯ АКТИВІВ");
                writer.WriteLine("Актив;Rj;Цінність");
                foreach (var asset in rankingAssets)
                {

writer.WriteLine($"{asset.Name};{asset.Rj:F2};{asset.Value:F3}
");
                }
                writer.WriteLine($"Кількість активів 
(m);{rankingAssets.Count}");
                writer.WriteLine($"Кількість експертів 
(n);{nExperts}");
                writer.WriteLine($"Ступені свободи (k=m-
1);{degreesOfFreedom}");
                writer.WriteLine($"Коефіцієнт конкордації 
W;{W:F4}");
                writer.WriteLine($"X²розр;{chiSquared:F2}");
                writer.WriteLine($"X²табл (α=0,05; 
k={degreesOfFreedom});{chiSquaredTable:F2}");
```

```
                string significance = (chiSquared > 
chiSquaredTable) ? "Так (думки узгоджені)" : "Ні (думки 
розрізняються)";

                writer.WriteLine($"Статистична 
значущість;{significance}");

                writer.WriteLine();

                writer.WriteLine("ОЦІНКА РИЗИКІВ");

                writer.WriteLine("ID;Назва 
загрози;Актив;Ймовірність P;Наслідки C;Ризик 
R=P×C;Категорія;Опис");

                foreach (var risk in risks)

                {


writer.WriteLine($"{risk.Id};{risk.Name};{risk.AssetName};{ris
k.Probability};{risk.Consequences};{risk.RiskLevel};{risk.Cate
gory};{risk.Description}");

                }

            }

            Console.WriteLine($"\n Звіт збережено у файл: 
{filePath}");

        }

        static void Main(string[] args)

        {

            Console.OutputEncoding = 
System.Text.Encoding.UTF8;

            Console.Title = "RiskAssessmentTool - Оцінка 
ризиків ІБ нотаріальної контори";

            Console.Clear();

            Console.WriteLine(new string('=', 100));
```

```
            Console.WriteLine("ПРОГРАМНА РЕАЛІЗАЦІЯ ОЦІНКИ
РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ");

            Console.WriteLine("Нотаріальна контора - Оцінка
ризиків для активів");

            Console.WriteLine(new string('=', 100));


            List<Asset> allAssets = GetPredefinedAssets();

            Console.WriteLine("\n ЕТАП 1: РАНЖУВАННЯ
АКТИВІВ");

            Console.WriteLine(new string('-', 50));

            List<Asset> rankingAssets =
SelectAssetsForRanking(allAssets);

            int m = rankingAssets.Count;

            Console.Write("\nВведіть кількість експертів: ");

            int nExperts = int.Parse(Console.ReadLine());

            RankingCalculator ranking = new
RankingCalculator(nExperts, rankingAssets);

            ranking.InputRanks();

            ranking.CalculateSumRanks();

            ranking.CalculateAssetValues();

            double chiSquared;

            double W = ranking.CalculateConcordance(out
chiSquared);

            int degreesOfFreedom = m - 1;

            double chiSquaredTable =
GetChiSquaredTableValue(degreesOfFreedom);

            Console.WriteLine("\n РЕЗУЛЬТАТИ РАНЖУВАННЯ:");
```

```
            Console.WriteLine($"   Кількість активів (m) =
{m}");

            Console.WriteLine($"   Кількість експертів (n) =
{nExperts}");

            Console.WriteLine($"   Ступені свободи (k = m-1) =
{degreesOfFreedom}");

            Console.WriteLine($"   Коефіцієнт конкордації W =
{W:F4}");

            Console.WriteLine($"   X²розр = n×(m-1)×W =
{nExperts} × {degreesOfFreedom} × {W:F4} = {chiSquared:F2}");

            Console.WriteLine($"   X²табл (α=0,05;
k={degreesOfFreedom}) = {chiSquaredTable:F2}");


            if (chiSquared > chiSquaredTable)

                Console.WriteLine("Результат статистично
значущий (X²розр > X²табл) - думки експертів узгоджені");

            else

                Console.WriteLine("Результат статистично не
значущий (X²розр ≤ X²табл) - думки експертів розрізняються")

            Console.WriteLine("\nЦІННІСТЬ АКТИВІВ
(відсортовано за спаданням):");

            foreach (var asset in
rankingAssets.OrderByDescending(a => a.Value))

            {

                Console.WriteLine($"   {asset.Name}: Rj =
{asset.Rj:F2}, Цінність = {asset.Value:F3}");

            }
```

```
            Asset mostValuableAsset =
rankingAssets.OrderByDescending(a =>
a.Value).FirstOrDefault();

            Console.WriteLine($"\n НАЙЦІННІШИЙ АКТИВ:
{mostValuableAsset.Name} (ID: {mostValuableAsset.Id})");

            Console.WriteLine($"   Цінність:
{mostValuableAsset.Value:F3} (за шкалою 7-10)");

            AssessRisksForAsset(mostValuableAsset, W,
chiSquared, degreesOfFreedom, chiSquaredTable, nExperts,
rankingAssets, true);

            while (true)

            {

                Console.WriteLine("\n" + new string('=',
100));

                Console.Write("Чи бажаєте оцінити ризики для
іншого активу? (так/ні): ");

                string answer = Console.ReadLine()?.ToLower();


                if (answer != "так" && answer != "yes" &&
answer != "y" && answer != "т")

                {

                    Console.WriteLine("\n Роботу завершено.
Дякуємо за використання програми!");

                    break;

                }

                DisplayFullAssetList(allAssets);

                Console.Write("\nВведіть ID активу для оцінки
ризиків: ");
```

```
                int selectedId =
int.Parse(Console.ReadLine());

                var selectedAsset = allAssets.FirstOrDefault(a
=> a.Id == selectedId);

                if (selectedAsset == null)

                {

                    Console.WriteLine("Актив з таким ID не
знайдено. Спробуйте ще раз.");

                    continue;

                }

                AssessRisksForAsset(selectedAsset, W,
chiSquared, degreesOfFreedom, chiSquaredTable, nExperts,
rankingAssets, false);

            }

            Console.WriteLine("\n" + new string('=', 100));

            Console.WriteLine("Розрахунок завершено. Натисніть
будь-яку клавішу для виходу...");

            Console.ReadKey();

        }

    }

}
```

Додаток В Графічний матеріал

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

КАФЕДРА КІБЕРБЕЗПЕКИ ТА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

Графічний матеріал до
Бакалаврської кваліфікаційної роботи
Охріменко Єлизавети Валентинівни

На тему:
«Система управління ризиками інформаційної безпеки нотаріальної контори»

Науковий керівник:
к.т.н. доц. Ізмайлова О.В.

Київ 2026

АКТУАЛЬНІСТЬ НАПРЯМУ

Сучасний етап розвитку суспільства характеризується стрімкою цифровізацією всіх сфер діяльності, включаючи нотаріат.

1) По-перше, спостерігається зростання кіберзагроз та атак на державні реєстри.
2) По-друге, відбувається посилення законодавчих вимог до захисту персональних даних та нотаріальної таємниці.
3) По-третє, відсутність системного підходу в багатьох нотаріальних конторах, де заходи захисту інформації впроваджуються фрагментарно, без системного аналізу ризиків та об ґрунтування необхідності тих чи інших захисних механізмів.
4) По-четверте, існує нагальна необхідність забезпечення безперервності діяльності, оскільки блокування доступу до державних реєстрів, компрометація ключів електронного підпису або знищення архівних даних можуть паралізувати роботу нотаріальної контори, що матиме серйозні наслідки як для самого нотаріуса, так і для клієнтів.

МЕТА, ОБ'ЄКТ ТА ПРЕДМЕТ ДОСЛІДЖЕННЯ

- **Метою роботи**є розробка програмної системи оцінювання ризиківяка дозволить підвищити ефективність та об'єктивність прийняття рішень щодо захисту інформаційних активів.
- **Об'єктомдослідження**є система управління інформаційною безпекою нотаріальної контори.
- **Предметом**є методи та засоби оцінювання та управління ризиками інформаційної безпеки в діяльності нотаріальної контори.

НОРМАТИВНО-ПРАВОВА БАЗА

- Проведено аналіз предметної області, нормативно -правової бази та існуючих підходів до управління ризиками інформаційної безпеки нотаріальної контори. Вона характеризується високою цінністю інформації, що обробляється (нотаріальна таємниця, персональні дані), інтеграцією з державними електронними реєстрами та тривалими термінами зберігання даних.
- Аналіз нормативно -правової бази показав, що діяльність нотаріуса регулюється комплексом актів: загальним законодавством, галузевим законодавством та підзаконними актами. Визначено зацікавлені сторони СУІБ нотаріальної контори.

Загальне законодавство	Закони «Про інформацію», «Про захист персональних даних», «Про кібербезпеку», «Про електронну ідентифікацію»
Галузеве законодавство	Закон України «Про нотаріат» (ст. 8 – нотаріальна таємниця)
Підзаконні акти	Положення про вимоги до робочого місця нотаріуса

ПІДХІД ДО УПРАВЛІННЯ РИЗИКАМИ

Методологічну основу управління ризиками складають стандарти серії ISO/IEC 27000. Порівняльний аналіз підходів до оцінювання ризиків показав,що для нотаріальної контори найбільш доцільним є комбінований(напівкількісний) підхід, який забезпечує необхідну точність при простоті реалізації.

В рамках дипломного проекту пропонується адаптувати методологію ДСТУ ISO/IEC 27005 до специфіки нотаріальної контори із застосуванням комбінованого підходуОсновний фокус дослідження зосереджено на етапі оцінювання ризиків

Якісний	Простий, але суб'єктивний
Кількісний	Об'єктивний, але складний
Комбінований (обраний)	Поєднує простоту та об'єктивність

ІДЕНТИФІКАЦІЯ АКТИВІВ

Ідентифікація активів є першим кроком безпосереднього оцінювання ризиків. У ході дослідження було ідентифіковано шість категорій активів інформаційні, апаратні, програмні, людські, сервісні та фізичні. З загального переліку активів, який налічував 33 позиції, було відібрано вісім найбільш критичних об’єктів.

Актив	Rj	Цінність
Критичні бази даних	4	10
Нотаріальна таємниця	9,5	9,377358
Паперовий архів	12	9,09434
Доступ до держ. реєстрів	14,5	8,811321
Токен (носій КЕП)	20	8,188679
Персональні дані клієнтів	25	7,622642
Антивірусне ПЗ	28,5	7,226415
ПК нотаріуса	30,5	7

МОДЕЛЬ ЗАГРОЗ

Ідентифіковано основні загрози для токена з ЕЦП. Для систематизації загроз використано методологію STRIDE.

КатегоріяSTRIDE	Опис загрози
Spoofing(підміна)	Використання чужого носія з ЕЦП
Tampering(втручання)	Модифікація ПЗ на токені
Repudiation(відмова)	Нотаріусстверджує, що не підписувавдокумент
Information Disclosure(розкриття)	Копіювання закритого ключа
Denial of Service(відмова)	Фізичне знищення носія
Elevation of Privilege(підвищення привілеїв)	Доступ дозакритихрозділів реєстрів

МОДЕЛЬ ПОРУШНИКА

Аналіз потенційних порушників дозволяє визначитихто може становити загрозу для токена з КЕП. На основі експертного опитування та аналізу типових сценаріїв порушень виокремлено’ять типів порушників

№	Тип порушника	Мотив	Типові дії
1	Внутрішній ненавмисний	Помилка, недбалість	Втрата токена, ненавмисне розголошення
2	Внутрішній умисний (інсайдер)	Фінансова вигода, помста	Крадіжка токена, копіювання ключа
3	Привілейований (адмін, техпідтримка)	Розширений доступ	Відключення захисту, копіювання ключів
4	Зовнішній хакер	Фінансова вигода	Злам ПК, перехоплення даних, фішинг
5	Зовнішній випадковий	Відсутня (випадковість)	Використання знайденого токена

ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ

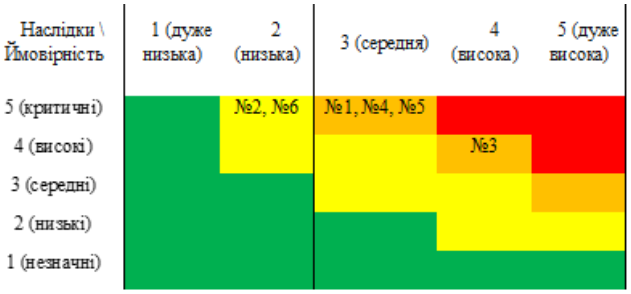
Вразливість — це слабке місце в системі захисту, яке може бути використане для реалізації ідентифікованих загроз. Виявлені вразливості поділено на три категорії: організаційні, технічні та фізичні.

Категорія	Вразливості
Організаційні	Відсутність політик безпеки, недостатня обізнаність персоналу
Технічні	Зберігання ключів на HDD, відсутність антивірусу, резервного копіювання
Фізичні	Відсутність контролю доступу, засобів пожежогасіння

ID	Загроза	Вразливість	Ймовірність	Наслідки	Рівень ризику	Категорія
1	Використання чужого носія з ЕЦП для видачі себе за іншого нотаріуса	Відсутность контролю за доступом до приміщення та відсутность блокування сесії при виході з робочого місця.	3	5	15	Високий
2	Модифікація програмного забезпечення на токені або підміна сертифіката.	Відсутность контролю цілісності ПЗ та використання незахищених файлових носіїв замість апаратних токенів.	2	5	10	Середній
3	Нотаріус стверджує, що не підписував документ, хоча підпис було поставлено його ключем.	Відсутность системи логування час підписання та ідентифікаторів пристроїв	4	4	16	Високий
4	Копіювання закритого ключа (приватного ключа ЕЦП) з флешки зловмисником.	Зберігання ключів на файловому носії замість захищеного апаратного токена, відсутності шифрування диска ПК	3	5	15	Високий
5	Фізичне знищення носія або блокування доступу до нього.	Відсутності резервного носія, відсутність регулярного створення резервних копій ключів, відсутность контролю за фізичним зберіганням токену	3	5	15	Високий
6	Отримання доступу до закритих розділів державних реєстрів через підміну ролі	Відсутность геолокаційної прив'язки сеансів підписання та відсутность додаткового підтвердження операцій	2	5	10	Середній

МАТРИЦЯ РИЗИКІВ

Для наочного представлення результатів оцінювання ризиків будується матриця (карта) ризиків.

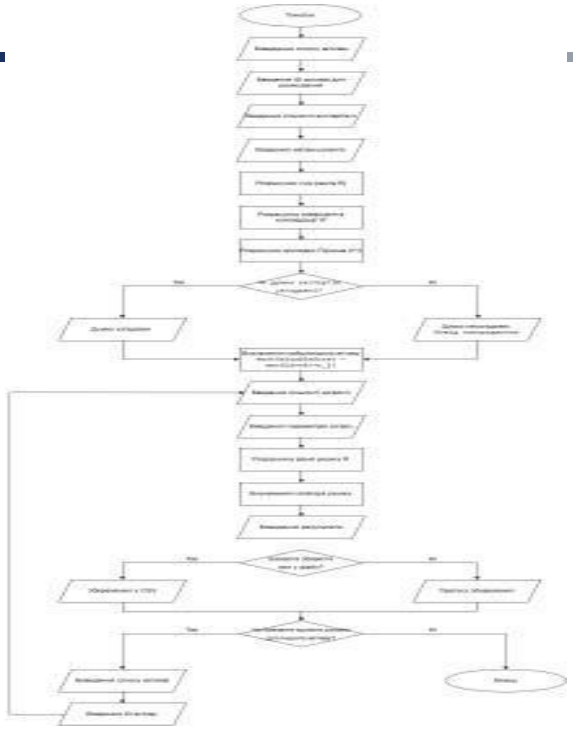


ПРОГРАМНА РЕАЛІЗАЦІЯ

Метою програмної реалізації є створення інструменту, який дозволяє автоматизувати такі етапи оцінки ризиків, як -от: введення експертних даних для ранжування активів, отримання кінцевих результатів у вигляді таблиць та звітів.

Програмна реалізація була виконана в середовищі програмування Microsoft Visual Studio за допомогою мови C#, обрано модульну архітектуру.

Модуль	Функції
Data Input Module	Введення даних, валідація
Data Processing Module	Обробка та зберігання даних
Calculation Module	Розрахунки (W, X^2, R = P×A)
Data Output Module	Виведення результатів, збереження у CSV



```
📋 СПИСОК АКТИВІВ НОТАРІАЛЬНОЇ КОНТОРИ:
------------------------------------------------------------
   1. БФП                                  2. Робочий ПК нотаріуса
   3. Робочий ПК помічника                 4. Засоби криптографічного захисту (агент підпису)
   5. Антивірусне ПЗ                       6. Операційна система (Windows)
   7. Ноутбук                              8. Пакети Microsoft Office
   9. Персональні дані клієнтів            10. Нотаріальна таємниця
  11. Електронний архів                    12. Ключі КЕП
  13. Паролі доступу до держ. реєстрів     14. Фінансові документи
  15. Роутер                               16. Токен
  17. Веб-браузер                          18. Нотаріус
  19. Помічник нотаріуса                   20. Технічний персонал
  21. Клієнти                              22. Доступ до Єдиного реєстру нотаріальних дій
  23. Доступ до Державного реєстру речових прав на нерухоме майно 24. Доступ до Єдиного державного реєстру юридичних осіб
  25. Доступ до Спадкового реєстру        26. Доступ до мережі Інтернет
  27. Електропостачання                   28. Послуги кваліфікованого надавача електронних довірчих послуг
  29. Послуги з фізичної охорони приміщення  30. Приміщення нотаріальної контори
  31. Архівне приміщення                   32. Сейф
  33. Зовнішні накопичувачі
------------------------------------------------------------
```

```
Введіть ID активів для ранжування (через кому, наприклад: 11,10,31,22,16,9,5,2): 2,5,10,15,19,25,29,33

✅ Обрано 8 активів для ранжування:
   - Робочий ПК нотаріуса (ID 2)
   - Антивірусне ПЗ (ID 5)
   - Нотаріальна таємниця (ID 10)
   - Роутер (ID 15)
   - Помічник нотаріуса (ID 19)
   - Доступ до Спадкового реєстру (ID 25)
   - Послуги з фізичної охорони приміщення (ID 29)
   - Зовнішні накопичувачі (ID 33)
```

```
Введіть кількість експертів: 4
```

```
📊 РЕЗУЛЬТАТИ РАНЖУВАННЯ:
   Кількість активів (m) = 8
   Кількість експертів (n) = 4
   Ступені свободи (k = m-1) = 7
   Коефіцієнт конкордації W = 0,9184
   X²розр = n×(m-1)×W = 4 × 7 × 0,9184 = 25,72
   X²табл (α=0,05; k=7) = 14,07
   ✅ Результат статистично значущий (X²розр > X²табл) - думки експертів узгоджені

📊 ЦІННІСТЬ АКТИВІВ:
   Робочий ПК нотаріуса: Rj = 14,50, Цінність = 8,812
   Антивірусне ПЗ: Rj = 28,00, Цінність = 7,125
   Нотаріальна таємниця: Rj = 5,00, Цінність = 10,000
   Роутер: Rj = 29,00, Цінність = 7,000
   Помічник нотаріуса: Rj = 15,00, Цінність = 8,750
   Доступ до Спадкового реєстру: Rj = 7,00, Цінність = 9,750
   Послуги з фізичної охорони приміщення: Rj = 27,00, Цінність = 7,250
   Зовнішні накопичувачі: Rj = 18,50, Цінність = 8,312

🏆 НАЙЦІННІШИЙ АКТИВ: Нотаріальна таємниця (ID: 10)
   Цінність: 10,000 (за шкалою 7-10)
```

```
📝 ВВЕДЕННЯ МАТРИЦІ РАНГІВ
   (менший ранг = вища цінність, від 1 до 8)
   Увага: при однаковій цінності активів можна ставити однакові ранги!

Експерт 1:
   Робочий ПК нотаріуса: 4
   Антивірусне ПЗ: 7
   Нотаріальна таємниця: 1
   Роутер: 8
   Помічник нотаріуса: 5
   Доступ до Спадкового реєстру: 1
   Послуги з фізичної охорони приміщення: 6
   Зовнішні накопичувачі: 5

Експерт 2:
   Робочий ПК нотаріуса: 5
   Антивірусне ПЗ: 8
   Нотаріальна таємниця: 1
   Роутер: 7
   Помічник нотаріуса: 4
   Доступ до Спадкового реєстру: 2
   Послуги з фізичної охорони приміщення: 7
   Зовнішні накопичувачі: 6

Експерт 3:
   Робочий ПК нотаріуса: 3
   Антивірусне ПЗ: 6
   Нотаріальна таємниця: 2
   Роутер: 6
   Помічник нотаріуса: 5
   Доступ до Спадкового реєстру: 2
   Послуги з фізичної охорони приміщення: 8
   Зовнішні накопичувачі: 5

Експерт 4:
   Робочий ПК нотаріуса: 5
   Антивірусне ПЗ: 7
   Нотаріальна таємниця: 1
   Роутер: 8
   Помічник нотаріуса: 4
   Доступ до Спадкового реєстру: 2
   Послуги з фізичної охорони приміщення: 7
   Зовнішні накопичувачі: 5
```

```
ЕТАП 2: ОЦІНКА РИЗИКІВ ДЛЯ АКТИВУ "Нотаріальна таємниця"
--------------------------------------------------

ШКАЛА ОЦІНЮВАННЯ РИЗИКІВ:
  Ймовірність (P) та Наслідки (C) оцінюються за шкалою 1-5:
    1 - дуже низька / незначні
    2 - низька / малі
    3 - середня / помірні
    4 - висока / значні
    5 - дуже висока / критичні

  Рівень ризику R = P × C
  Категорії ризику:
    R ≥ 20  → Неприйнятний (негайна обробка)
    R ≥ 15  → Високий (первочергова обробка)
    R ≥ 8   → Середній (планова обробка)
    R < 8   → Низький (прийнятний ризик)

Введіть кількість загроз: 6

ЗАГРОЗА #1 (для активу: Нотаріальна таємниця)
  Назва загрози: Розголошення нотаріальної таємниці через ненавмисні дії персоналу
  Опис загрози: Недостатня обізнаність персоналу щодо правил роботи з конфіденційною інформацією, відсутність регулярного навчання
  Ймовірність P (1-5): 4
  Наслідки C (1-5): 5

ЗАГРОЗА #2 (для активу: Нотаріальна таємниця)
  Назва загрози: Витік інформації через соціальну інженерію (фішинг, телефонне шахрайство)
  Опис загрози: Відсутність політики безпеки щодо роботи з електронною поштою та телефонними дзвінками
  Ймовірність P (1-5): 3
  Наслідки C (1-5): 5

ЗАГРОЗА #3 (для активу: Нотаріальна таємниця)
  Назва загрози: Несанкціонований доступ до документів з нотаріальною таємницею
  Опис загрози: Відсутність контролю доступу до приміщення та архіву, незамкнені шафи
  Ймовірність P (1-5): 3
  Наслідки C (1-5): 5

ЗАГРОЗА #4 (для активу: Нотаріальна таємниця)
  Назва загрози: Перехоплення даних при передачі електронною поштою
  Опис загрози: Відсутність шифрування електронних листів, використання незахищених каналів зв'язку
  Ймовірність P (1-5): 2
  Наслідки C (1-5): 5

ЗАГРОЗА #5 (для активу: Нотаріальна таємниця)
  Назва загрози: Розголошення таємниці під час розмови в присутності сторонніх осіб
  Опис загрози: Відсутність окремого приміщення для конфіденційних розмов, порушення правил етики
  Ймовірність P (1-5): 4
  Наслідки C (1-5): 4

ЗАГРОЗА #6 (для активу: Нотаріальна таємниця)
  Назва загрози: Втрата паперових документів з нотаріальною таємницею
  Опис загрози: Відсутність системи обліку та контролю за переміщенням документів
  Ймовірність P (1-5): 2
  Наслідки C (1-5): 5
```

```
ТАБЛИЦЯ - ОЦІНЮВАННЯ РИЗИКІВ ДЛЯ АКТИВУ "Нотаріальна таємниця"

 № | Ймовірність P | Наслідки C  | Ризик R = P×C  | Категорія
---------------------------------------------------------------
 1 |             4 |           5 |             20 | Неприйнятний
 2 |             3 |           5 |             15 | Високий
 3 |             3 |           5 |             15 | Високий
 4 |             2 |           5 |             10 | Середній
 5 |             4 |           4 |             16 | Високий
 6 |             2 |           5 |             10 | Середній

РЕКОМЕНДАЦІЇ ЩОДО ОБРОБКИ РИЗИКІВ

Ризик №1: Розголошення нотар?альної таємниці? через ненавмисн? д?Ї персоналу
  НЕГАЙНА ОБРОБКА - необх?дне негайне впровадження заход?в
  Р?вень ризику: 20 (Неприйнятний)
  Актив: Нотар?альна таємниця
  Опис: Недостатня об?зн?сть персоналу щодо правил роботи з конф?денц?йною ?нформац?ою, в?дсутн?сть регулярного навчання

Ризик №2: Вит?к ?нформац?Ї через соц?альну ?нженер?ю (ф?шинг, телефонне шахрайство)
  ПЕРШОЧЕРГОВА ОБРОБКА - пр?оритетне впровадження заход?в
  Р?вень ризику: 15 (Високий)
  Актив: Нотар?альна таємниця
  Опис: В?дсутн?сть пол?тики безпеки щодо роботи з електронною поштою та телефонними дзв?нками

Ризик №3: Несанкц?онований доступ до документ?в з нотар?альною таємницею
  ПЕРШОЧЕРГОВА ОБРОБКА - пр?оритетне впровадження заход?в
  Р?вень ризику: 15 (Високий)
  Актив: Нотар?альна таємниця
  Опис: В?дсутн?сть контролю доступу до прим?щення та арх?ву, незамкнен? шафи

Ризик №4: Перехоплення даних при передач? електронною поштою
  ПЛАНОВА ОБРОБКА - включити до плану заход?в
  Р?вень ризику: 10 (Середній)
  Актив: Нотар?альна таємниця
  Опис: В?дсутн?сть шифрування електронних лист?в, використання незахищених канал?в зв'язку

Ризик №5: Розголошення таємниці? п?д час розмови в присутност? сторонн?х ос?б
  ПЕРШОЧЕРГОВА ОБРОБКА - пр?оритетне впровадження заход?в
  Р?вень ризику: 16 (Високий)
  Актив: Нотар?альна таємниця
  Опис: В?дсутн?сть окремого прим?щення для конф?денц?йних розмов, порушення правил етики

Ризик №6: Втрата паперових документ?в з нотар?альною таємницею
  ПЛАНОВА ОБРОБКА - включити до плану заход?в
  Р?вень ризику: 10 (Середній)
  Актив: Нотар?альна таємниця
  Опис: В?дсутн?сть системи обл?ку та контролю за перем?щенням документ?в
```

```
СТАТИСТИЧНИЙ АНАЛІЗ РИЗИКІВ
------------------------------------------------------------
Актив: Нотаріальна таємниця
Всього проаналізовано загроз: 6
  - Неприйнятний рівень: 1
  - Високий рівень: 3
  - Середній рівень: 2
  - Низький рівень: 0

Сумарний показник ризику: 86
Середній рівень ризику: 14,33
```

```
Бажаєте зберегти звіт у файл? (так/ні): т

Звіт збережено у файл: C:\Users\User\Desktop\Нова папка (2)\ConsoleApp1\ConsoleApp1\bin\Debug\net8.0\RiskReport_Нотаріальна таємниця_20260522_005601.csv
```

1	РЕЗУЛЬТАТИ ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ		
2	Дата: 22.05.2026 0:56:01		
3	Найцінніший актив: Нотаріальна таємниця (ID: 10, Цінність: 10,000)		
4			
5	ЕТАП 1: РАНЖУВАННЯ АКТИВІВ		
6	Актив	Rj	Цінність
7	Робочий ПК нотаріуса	17	8,5
8	Антивірусне ПЗ	28	7,125
9	Нотаріальна таємниця	5	10
10	Роутер	29	7
11	Помічник нотаріуса	18	8,375
12	Доступ до Спадкового реєстру	7	9,75
13	Послуги з фізичної охорони приміщення	28	7,125
14	Зовнішні накопичувачі	21	8
15	Кількість активів (m)	8	
16	Кількість експертів (n)	4	
17	Ступені свободи (k=m-1)	7	
18	Конфіцієнт конкордації W	0,9296	
19	X^2розр	26,03	
20	X^2табл (α=0,05;k=7)		14,07
21	Статистична значущість	Так (думки узгоджені)	

23	ЕТАП 2: ОЦІНКА РИЗИКІВ		
24	ID	Назва загрози	Актив
25	1	Розголошення нотар?альної таємниці? через ненавмисн? д?Ї персоналу	Нотаріальна таємниця
26	2	Вит?к ?нформац?Ї через соц?альну ?нженер?ю (ф?шинг, телефонне шахрайство)	Нотаріальна таємниця
27	3	Несанкц?онований доступ до документ?в з нотар?альною таємницею	Нотаріальна таємниця
28	4	Перехоплення даних при передач? електронною поштою	Нотаріальна таємниця
29	5	Розголошення таємниці? п?д час розмови в присутност? сторонн?х ос?б	Нотаріальна таємниця
30	6	Втрата паперових документ?в з нотар?альною таємницею	Нотаріальна таємниця

Ймовірність P	Наслідки C	Ризик R=P	Категорія	Опис
4	5	20	Неприйнятний	Недостатня об?зн?сть персоналу щодо правил роботи з конф?денц?йною ?нформац?ою, в?дсутн?сть регулярного навчання
3	5	15	Високий	В?дсутн?сть пол?тики безпеки щодо роботи з електронною поштою та телефонними дзв?нками
3	5	15	Високий	В?дсутн?сть контролю доступу до прим?щення та арх?ву, незамкнен? шафи
2	5	10	Середній	В?дсутн?сть шифрування електронних лист?в, використання незахищених канал?в зв'язку
4	4	16	Високий	В?дсутн?сть окремого прим?щення для конф?денц?йних розмов, порушення правил етики
2	5	10	Середній	В?дсутн?сть системи обл?ку та контролю за перем?щенням документ?в

```
Чи бажаєте оцінити ризики для іншого активу? (так/ні): ні

Роботу завершено. Дякуємо за використання програми!
```

ВИСНОВКИ

Дипломна робота була спрямована для вирішення проблем пов’язани х із цифровізацією нотаріальної діяльності. У роботі запропоновано використовувати методологію управління ризиками згідно з міжнародним стандартом ДСТУ ISO/IEC 27005. Як показало дослідження, найбільш доцільним для нотаріальної контори є комбінований підхід до оцінювання ризиків

Для автоматизації процесу оцінювання ризиків розроблено програмну систему мовою C#, обрано модульну архітектуру. Система реалізує ключовий етап управління ризиками - етап оцінювання ризиків, що є фундаментом для подальших етапів обробки та моніторингу ризиків.Впровадження результатів дослідження дозволить нотаріальним конторам обґрунтовано розподіляти ресурси на захист інформації,документально підтвердити виконання вимог законодавства та підвищити загальний рівень інформаційної безпеки

Перспективними напрямами подальшого розвитку є доповнення програми функцією автоматичного формування плану заходів з обробки виявлених ризиків,підключення до баз даних для накопичення історії оцінювань, а також створення графічного інтерфейсу для більш зручної взаємодії з користувачем.

Дякую за увагу!