Міністерство освіти і науки України
Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«МЕТОД РИЗИК-ОРІЄНТОВАНОГО АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ФІНАНСОВО-КРЕДИТНИХ УСТАНОВАХ»

Виконав: студент 2 курсу групи 1БС-24 м
спеціальності 125 Кібербезпека та захист інформації
_____ Максим КРИВОВ'ЯЗЮК

Керівник: к. т. н., доц., доцент каф. ЗІ
_____ Олеся ВОЙТОВИЧ
«19» грудня 2025 р.

Опонент: к. т. н., доц. доцент каф. ПЗ
_____ Володимир МАЙДАНЮК
«19» грудня 2025 р.

Допущено до захисту
В. о. завідувача кафедри ЗІ
д. т. н., проф.
_____ Володимир ЛУЖЕЦЬКИЙ
«16» грудня 2025 р.

Вінниця ВНТУ – 2025 року

Міністерство освіти і науки України
Вінницький національний технічний університет

Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації
Рівень вищої освіти II (магістерський)
Галузь знань – 12 Інформаційні технології
Спеціальність – 125 Кібербезпека та захист інформації
Освітньо-професійна програма – Безпека інформаційних і комунікаційних систем

ЗАТВЕРДЖУЮ
В. о. зав. каф. ЗІ
д. т. н., проф.
Володимир ЛУЖЕЦЬКИЙ
«24» 09 2025 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Максиму КРИВОВ'ЯЗЮКУ

1. Тема роботи: «Метод ризик-орієнтованого аудиту інформаційної безпеки у фінансово-кредитних установах»
   керівник роботи: Олеся ВОЙТОВИЧ, к. т. н., доцент, доцент кафедри ЗІ, затверджені наказом ректора ВНТУ від 24 вересня 2025 року №313.
2. Строк подання студентом роботи 19 грудня 2025 р.
3. Вихідні дані до роботи:
   - Постонови НБУ та стандарти ISO/IEC 27001, ISO/IEC 27005, COBIT, NIST SP 800-30;
   - Дані журналів інцидентів для оцінки ризиків;
   - Автоматизовані інструменти аудиту;
   - Взаємодія аудитора з персоналом.
4. Зміст текстової частини: Вступ. 1. Аналіз джерел за напрямком дослідження. 2. Розробка методу ризик-орієнтованого аудиту інформаційної безпеки. 3. Практичне впровадження ризик-орієнтованого аудиту інформаційної безпеки. 4. Економічна частина. Висновки. Список використаних джерел. Додатки.
5. Перелік ілюстративного матеріалу: порівняльний аналіз нормативно-правових актів, схема проведення аудиту відповіднно до чиного законодавства, схема проведення аудиту відповіднно до міжнародних стандартів, схема взаємодії аудиторів та ризик-координаторів, схема автоматизації аудиту, схема методу ризик-орієнтованого аудиту, показники економічної ефективності.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		Завдання видав	Завдання прийняв
1	О. ВОЙТОВИЧ, к.т.н., доц., доц. каф. ЗІ	25.09.25	06.10.25
2	О. ВОЙТОВИЧ, к.т.н., доц., доц. каф. ЗІ	25.09.25	03.11.25
3	О. ВОЙТОВИЧ, к.т.н., доц., доц. каф. ЗІ	25.09.25	17.11.25
4	О. ЛЕСЬКО, зав. каф. ЕПВМ, к.е.н., доц	29.09.25	18.11.25

7. Дата видачі завдання. 24.09.2025

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз завдання. Вступ	01.09.2025 – 05.09.2025	
2	Аналіз інформаційних джерел за напрямком магістерської кваліфікаційної роботи	08.09.2025 – 12.09.2025	
3	Науково-технічне обґрунтування	15.09.2025 – 19.09.2025	
4	Розробка технічного завдання	22.09.2025 – 26.09.2025	
5	Аналіз нормативних актів України та світу щодо аудити фінансово-кредитних установ	29.09.2025 – 03.10.2025	
6	Розробка організаційної моделі взаємодії між аудитом і службою інформаційної безпеки	06.10.2025 – 10.10.2025	
7	Розробка методу методу ризик-орієнтованого аудиту	13.10.2025 – 17.10.2025	
8	Практичне впровадження методу ризик-орієнтованого аудиту	20.10.2025 – 24.10.2025	
9	Розробка розділу економічного обґрунтування доцільності розробки	27.10.2025 – 14.11.2025	
10	Аналіз виконання ТЗ, висновки	15.11.2025 – 17.11.2025	
11	Оформлення пояснювальної записки	18.11.2025 – 21.11.2025	
12	Перевірка магістерської роботи на наявність текстових запозичень	22.11.2025 – 24.11.2025	
13	Попередній захист та доопрацювання МКР	25.11.2025 – 29.11.2025	
14	Представлення МКР до захисту, рецензування	17.12.2025 – 18.12.2025	
15	Захист МКР	19.12.2025 – 23.12.2025	

Студент _____ Максим КРИВОВ'ЯЗЮК

Керівник роботи _____ Олеся ВОЙТОВИЧ

АНОТАЦІЯ

УДК 004.056

Кривов’язюк М. Метод ризик-орієнтованого аудиту інформаційної безпеки у фінансово-кредитних установах. Магістерська кваліфікаційна робота зі спеціальності 125 Кібербезпека та захист інформації, освітня програма – Безпека інформаційних і комунікаційних систем. Вінниця: ВНТУ, 2025. 88 с.

Укр. мовою. Бібліогр.: 33 назв; рис. 9; табл.: 24.

Магістерська кваліфікаційна робота присвячена розробці методу ризик-орієнтованого аудиту інформаційної безпеки у фінансово-кредитних установах. Здійснено аналіз нормативно-правової бази Національного банку України та міжнародних стандартів у контексті проведення аудиту інформаційної безпеки. Удосконалено метод ризик-орієнтованого аудиту шляхом впровадження ролі ризик-координатора, формування динамічної карти ризиків на основі фактичних даних про інциденти та тестування контролів. Проведено практичну апробацію запропонованого методу, результати якої підтвердили підвищення об’єктивності оцінки ризиків і ефективності аудиторських процедур.

Ілюстративна частина складається з 7 плакатів з демонстрацією результатів проведеного тестування.

Ключові слова: ризик-орієнтований аудит, інформаційна безпека, банківський сектор, міжнародні стандарти, управління ризиками, кібербезпека.

ABSTRACT

UDC 004.056

Kryvoviaziuk M. Risk-Oriented Information Security Audit Method in Financial and Credit Institutions. Master's qualification work in specialty 125 – Cybersecurity and Information Protection, educational program Information and Communication Systems Security. Vinnytsia: VNTU, 2025. 88 p.

In Ukrainian language. References: 33 titles; figures: 9; tables: 24.

The master's qualification thesis is devoted to the development of a risk-oriented method for conducting information security audits in financial and credit institutions. An analysis of the regulatory framework of the National Bank of Ukraine and international standards out in the context of information security auditing. The risk-oriented audit method was improved through the introduction of the risk coordinator role, the development of a dynamic risk map based on actual incident data, and control testing. Practical implementation of the proposed method was performed, and the results confirmed an increase in the objectivity of risk assessment and the effectiveness of audit procedures.

The illustrative part consists of 7 posters demonstrating the results of the conducted testing.

Keywords: risk-oriented audit, information security, banking sector, international standards, risk management, cybersecurity.

ЗМІСТ

ВСТУП 6
1 АНАЛІЗ ДЖЕРЕЛ ЗА НАПРЯМКОМ ДОСЛІДЖЕННЯ 9
1.1 Аналіз постанов та вимог Національного банку України 9
1.2. Огляд міжнародних стандартів 14
1.3 Методологічні принципи проведення аудиту інформаційної безпеки 21
1.4. Процес взаємодії аудиту з інформаційною безпекою. 24
1.5 Аналіз інструментів для автоматизації аудиту 26
1.6 Дослідження застосування штучного інтелекту для аудиту інформаційної безпеки 28
1.7 Постановка завдання 30
2. РОЗРОБКА МЕТОДУ РИЗИК-ОРІЄНТОВАНОГО АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ 32
2.1 Аналіз журналу інцидентів, ідентифікація ризиків та загальний процес аудиту 32
2.2 Процеси та організація аудиту інформаційної безпеки відповідно до вимог НБУ та міжнародних стандартів 36
2.3 Формування карти ризиків 42
2.4 Формування програми аудиту 45
2.5 Розробка організаційної моделі взаємодії між аудитом і службою інформаційної безпеки 47
2.6 Формування звіту та рекомендацій аудиту 50
2.7 Розробка методу ризик-орієнтованого аудиту інформаційної безпеки 53
2.8 Висновки до другого розділу 56
3 ПРАКТИЧНЕ ВПРОВАДЖЕННЯ РИЗИК-ОРІЄНТОВАНОГО АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ 57
3.1 Інтеграція та автоматизація аудиту 57
3.2 Використання технологій штучного інтелекту у аудиті 60
3.3 Організаційна взаємодія та ризик-координатора 63
3.4 Підсумкові висновки щодо практичного етапу оцінки ризиків та формування карти аудиту 66
3.5 Вплив впровадження ризик-орієнтованого аудиту на процеси контролю інформаційної безпеки 71
3.6 Висновки до третього розділу 73
4 ЕКОНОМІЧНА ЧАСТИНА 74

4.1 Проведення комерційного та технологічного аудиту науково-технічної розробки 74
4.2 Розрахунок витрат на здійснення науково-дослідної роботи 79
4.3 Розрахунок економічної ефективності науково-технічної розробки від її впровадження безспосередньо замовником 88
4.4 Висновки до четвертого розділу 91
ВИСНОВКИ 92
СПИСОВ ВИКОРИСТАНИХ ДЖЕРЕЛ 94

ВСТУП

Аудит інформаційної безпеки - це системний процес одержання об'єктивних якісних і кількісних оцінок поточного стану безпеки інформаційної системи, комплексна оцінка рівня інформаційної безпеки клієнта з урахуванням трьох основних факторів: персоналу, процесів і технологій. Порівняльний аналіз поточного стану інформаційної системи, що визначається за підсумками анкетування, з тестовою моделлю вимог стандарту ISO 27001.

Фінансово-кредитні установи залишаються однією з головних мішеней для кіберзлочинців, що зумовлено високою вартістю активів, конфіденційністю оброблюваної інформації та складною розгалуженою IT-інфраструктурою. За даними звіту IBM X-Force Threat Intelligence Index за 2024 рік, саме фінансовий сектор займає перше місце за кількістю цільових кіберінцидентів - на нього припадає близько 19% усіх атак, що підтверджує високий рівень ризиків, з якими стикаються банки у цифровому середовищі.

У таких умовах аудит інформаційної безпеки (ІБ) набуває надзвичайно важливого значення. Він вже не може обмежуватись суто формальною перевіркою дотримання стандартів чи наявності документації. Натомість аудит ІБ повинен розглядатися як системний процес, спрямований на виявлення вразливих місць в інформаційній інфраструктурі, аналіз ефективності заходів безпеки, а також оцінку зрілості системи управління ІБ в фінансових установах. Практика засвідчує, що хоча багато фінансових установ декларують відповідність міжнародним стандартам, зокрема ISO/IEC 27001 або PCI DSS, у реальності аудит часто перетворюється на формальність, орієнтовану лише на підтвердження наявності політик і регламентів. Такий підхід не дозволяє ідентифікувати критичні вразливості, що можуть ховатися у логіці бізнес-процесів, некоректних конфігураціях систем чи в особливостях взаємодії персоналу [1, 2].

Крім того, існує низка викликів, які ускладнюють проведення якісного аудиту інформаційної безпеки у банківському секторі. Серед них - обмежений

або фрагментарний доступ аудиторів до технічних систем і журналів подій, що суттєво знижує об’єктивність висновків. Аудитори часто не мають повного доступу до критичних компонентів інформаційної інфраструктури, таких як системи управління доступом, лог-файли безпеки, SIEM-платформи, що унеможливлює всебічний аналіз подій безпеки та виявлення потенційних інцидентів.

Нерідко аудиторський процес ускладнюється недостатньо формалізованою комунікацією між аудиторами та представниками служби інформаційної безпеки, що призводить до нерозуміння ролей і відповідальності сторін. Відсутність чітко визначених процедур взаємодії, регламентів обміну інформацією та узгоджених форматів звітності створює бар’єри для ефективного співробітництва. Це, своєю чергою, може призвести до втрати важливої інформації, затримок у процесі аудиту та зниження його якості [3].

Також часто відсутні чітко визначені критерії оцінки ефективності саме процесів, а не лише відповідності формальним вимогам, що унеможливлює комплексну перевірку стану інформаційної безпеки. У багатьох випадках аудит обмежується перевіркою наявності політик, процедур та технічних засобів, без глибокого аналізу їх фактичної реалізації, інтеграції в бізнес-процеси та здатності реагувати на реальні загрози.

Тому постає **актуальна** задача розробки методу ризик орієнтованого аудиту у фінансовій сфері

Об’єктом дослідження є процес аудиту інформаційної безпеки у фінансово-кредитних установах.

Предметом дослідження є метод ризик-орієнтованого аудиту інформаційної безпеки у фінансово-кредитних установах.

Метою магістерської кваліфікаційної роботи є підвищення об’єктивності оцінки ризиків інформаційної безпеки у фінансово-кредитних установах за рахунок впровадження ролі ризик-координатора та формування динамічної карти ризиків.

Для досягнення мети необхідно виконати такі завдання:

– провести огляд джерела із забезпечення інформаційної безпеки у фінансових установах;

– розробити та обгрунтувати метод ризик орієнтованого аудиту інформаційної безпеки у фінансово-кредитних установах;

– провести практичне вроваждення та оцінити запропоновані рішення ризик орієнтованого аудиту інформаційної безпеки у фінансово-кредитних установах;

– виконати економінче обгрунтування розробленого підходу ризик орієнтованого аудиту інформаційної безпеки у фінансово-кредитних установах.

Наукова новизна. Удосконалено метод ризик-орієнтованого аудиту інформаційної безпеки, що полягає у використанні ризик-координаторів аудиту та формуванні динамічної карти ризиків на основі фактичних даних про інциденти, тестування контролів.

Практична цінність. Розроблено алгоритми оновлення оцінки ризиків на основі журналів інцидентів, методику взаємодії аудиторів із представниками ІТ та ІБ (ризик-координаторами), а також застосування інструментів автоматизації для тестування інфраструктури.

Публікації результатів магістерської кваліфікаційної роботи.

За результатами магістерської кваліфікаційної роботи виконана апробацію та опубліковані тези доповідей на тему «Особливості банківської інфраструктури в україні та стандарти аудиту» [1] та «Підхід ризик-орієнованого аудиту інформаційної безпеки» [2].

1 АНАЛІЗ ДЖЕРЕЛ ЗА НАПРЯМКОМ ДОСЛІДЖЕННЯ

1.1 Аналіз постанов та вимог Національного банку України

У ході кваліфікаційної роботи здійснено комплексний аналіз нормативних, наукових та методичних джерел, що стосуються аудиту інформаційної безпеки у фінансово-кредитних установах. До проаналізованих джерел увійшли внутрішні політики та процедури банку, нормативно-правові акти Національного банку України, а також міжнародні стандарти та рекомендації провідних організацій (ISO/IEC 27001, ISO/IEC 27005, NIST, COBIT).

Аналіз літератури та нормативних документів дав змогу визначити основні принципи, на яких ґрунтується сучасний підхід до аудиту: системність, безперервність контролю, орієнтація на найбільш критичні активи та процеси, а також інтеграція аудиту в загальну систему управління ризиками організації.

Аналіз нормативно-правового поля, що регулює інформаційну безпеку у банківському секторі України, засвідчує наявність чітко структурованої методологічної бази, яку сформував Національний банк України через низку ключових регуляторних актів. Однією з найважливіших є постанова НБУ №95 від 28 вересня 2017 року, яка затверджує Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі. Банки зобов’язані розробити та впровадити заходи, що забезпечують конфіденційність, цілісність і доступність інформації в банківській системі [2]. Цей документ став першим системним регламентом, який заклав підґрунтя для побудови Систем управління інформаційною безпекою (СУІБ) у вітчизняних банках відповідно до міжнародного стандарту ISO/IEC 27001.

Постанова [6] закріпила обов’язковість створення СУІБ, що передбачає не лише впровадження формалізованих політик, але й систематичне управління ризиками та безпековими інцидентами. Вона також визначає необхідність призначення відповідальної особи на рівні топ-менеджменту, що підвищує управлінську відповідальність за ІБ. Одним із ключових положень є вимога до регулярного аудиту інформаційної безпеки, як засобу оцінки ефективності вже

впроваджених заходів захисту, а також впровадження чітких механізмів управління інцидентами, що включають як виявлення, так і реагування на події у сфері ІБ.

Подальший розвиток методологічної бази було закріплено постановою НБУ №4 від 16 січня 2021 року [4] року, яка суттєво розширила контрольні повноваження регулятора. Цей документ не лише створив нормативну основу для проведення інспекцій НБУ у сфері кібербезпеки, але й запровадив санкції за порушення відповідних вимог, що є ключовим елементом у зміцненні відповідальності банків за стан їхньої кіберзахищеності. Інспектори НБУ отримують право прямого доступу до ІТ-систем фінансових установ з метою оцінки їх роботи та зобов'язання повідомляти про інциденти у встановлені терміни.

Паралельно з цим, нормативне поле було доповнене постановою [5], яка спрямована на регулювання захисту інформації та кіберзахисту у сфері платіжних систем. Забезпечення відповідності платіжної інфраструктури міжнародним стандартам PCI DSS і управління каскадними ризиками. Особливе значення цього документа полягає в охопленні критично важливої платіжної інфраструктури, яка, через свою високу ліквідність, є пріоритетною мішенню для кіберзлочинців. Постанова узгоджується з міжнародними стандартами PCI DSS, які регламентують безпеку даних платіжних карток, і забезпечує адаптацію українських систем до глобальних вимог безпеки.

У ході аналізу нормативно-правових актів Національного банку України було встановлено, що система регулювання у сфері інформаційної безпеки банків поступово формувалася на основі поетапного розширення вимог та контролю. Постанова №95 заклала фундамент для створення Систем управління інформаційною безпекою (СУІБ) у банках, визначивши базові принципи, структуру та вимоги до аудиту. Подальше посилення контролю та відповідальності було реалізовано постановою №4, яка надала НБУ інспекційні повноваження у сфері кібербезпеки та запровадила механізми санкцій [6]. Завершальним етапом розвитку стала постанова №43, спрямована на

забезпечення кіберзахисту у платіжних системах і гармонізацію національних вимог із міжнародними стандартами, зокрема PCI DSS. Таким чином, кожна з постанов послідовно розширює та поглиблює нормативну базу у сфері інформаційної безпеки банківського сектору України. Порівняння постанов НБУ зображено у таблиці 1.1.

Таблиця 1.1 – Результати порівняння постанов НБУ

Номер	Ключові вимоги та положення	Мета документа	Відповідність міжнародним стандартам
№95	Обов'язковість створення Системи управління інформаційною безпекою (СУІБ). Призначення відповідальної особи за ІБ на рівні керівництва. -Регулярне проведення аудиту ІБ. -Управління ризиками та інцидентами безпеки. - Розроблення політик і процедур ІБ.	Створення єдиної методологічної бази для побудови систем ІБ у банках України.	Відповідає ISO/IEC 27001, ISO/IEC 27005 (управління ризиками).
№4	- Розширення повноважень НБУ щодо контролю кібербезпеки. - Право інспекторів НБУ на доступ до ІТ-систем банку. - Встановлення обов'язку повідомляти про кіберінциденти у визначені терміни. - Запровадження санкцій за невиконання вимог.	Посилення відповідальності банків за стан кіберзахищеності; підвищення ефективності державного нагляду.	Узгоджується з принципами NIST Cybersecurity Framework та практиками COBIT (контроль і управління ІТ).
№43	- Регулювання ІБ та кіберзахисту платіжної інфраструктури. - Вимога відповідності стандартам PCI DSS. - Управління каскадними ризиками у платіжних системах. - Контроль за безпекою даних платіжних карток.	Захист критично важливої платіжної інфраструктури від кіберзагроз; інтеграція у глобальну систему безпеки.	Відповідає PCI DSS, частково - ISO/IEC 27032 (кібербезпека).

Після ухвалення постанов [4,5,6] Національний банк України продовжує вдосконалювати підходи до регулювання інформаційної безпеки, поступово наближаючи національну систему вимог до європейських і міжнародних стандартів. Зокрема, останні зміни у сфері регулювання діяльності банків і небанківських фінансових установ свідчать про перехід від формального виконання вимог до ризик-орієнтованого підходу в управлінні інформаційною

безпекою. Такий підхід відповідає сучасним тенденціям управління кіберризиками, закріпленим у стандартах ISO/IEC 27005 та NIST Cybersecurity Framework.

Особлива увага приділяється створенню єдиної системи обміну інформацією про кіберінциденти між банками, Національним банком України та Державною службою спеціального зв'язку та захисту інформації. Це сприяє оперативному реагуванню на інциденти, обміну технічними індикаторами компрометації та запобіганню повторним атакам. Такі ініціативи узгоджуються з практиками EU NIS Directive, яка передбачає обов'язкове інформування регуляторів про значні кіберінциденти.

Крім того, у межах оновленої політики НБУ щодо управління IT-ризиками наголошується на необхідності регулярного проведення незалежного аудиту ІБ із залученням зовнішніх експертів, сертифікованих за міжнародними стандартами (наприклад, CISA, CISSP, ISO 27001 Lead Auditor). Це дає змогу забезпечити об'єктивність оцінки стану захищеності, а також гармонізувати внутрішні процеси фінансових установ з вимогами європейського регуляторного поля. Важливим кроком є також розвиток вимог до кіберстійкості фінансової інфраструктури, зокрема тестування за сценарієм Threat-Led Penetration Testing (TLPT), яке активно впроваджується у країнах ЄС відповідно до ініціативи TIBER-EU. НБУ поступово адаптує цей підхід для вітчизняного ринку, що дозволить банкам підвищити готовність до реальних кібератак шляхом моделювання загроз у контрольованих умовах. У перспективі очікується подальше оновлення нормативної бази НБУ з урахуванням вимог Регламенту ЄС DORA (Digital Operational Resilience Act), який визначає стандарти цифрової операційної стійкості для фінансового сектору. Впровадження аналогічних положень в Україні сприятиме не лише підвищенню рівня кіберзахисту, а й інтеграції національної фінансової системи у спільний європейський простір кібербезпеки.

Отже, сучасна нормативна політика НБУ у сфері інформаційної безпеки демонструє еволюцію від створення базових вимог [6] до формування цілісної

системи управління кіберризиками, що базується на принципах міжнародних стандартів і спрямована на забезпечення сталого функціонування банківського сектору в умовах зростаючих кіберзагроз.

У процесі забезпечення інформаційної безпеки у банківських установах важливу роль відіграє системний підхід до проведення аудиту. На основі вимог Національного банку України [4, 5 ,6], сформовано послідовний алгоритм дій, спрямований на оцінку ефективності впроваджених заходів, виявлення ризиків, управління інцидентами та забезпечення відповідності міжнародним стандартам інформаційної безпеки. Такий підхід дає змогу підвищити рівень контролю, мінімізувати можливі загрози та забезпечити безперервність функціонування критичних інформаційних процесів банківської системи.

Далі здійснюється ідентифікація активів та ризиків, під час якої проводиться аналіз інформаційних ресурсів установи, визначаються критичні елементи інфраструктури та потенційні загрози їх функціонуванню. Отримані результати стають основою для планування аудиту, де встановлюються об’єкти перевірки, методи збору даних, критерії оцінювання та строки проведення робіт.

Наступний етап передбачає безпосереднє проведення аудиту інформаційної безпеки відповідно до вимог постанов [5, 6]. Під час перевірки здійснюється виявлення інцидентів, пов’язаних із порушеннями політик безпеки або неправомірними діями користувачів. Для кожного інциденту фіксуються обставини, рівень впливу та відповідність встановленим вимогам.

Після цього проводиться оцінка відповідності систем інформаційної безпеки міжнародним стандартам, зокрема ISO/IEC, PCI DSS, а також вимогам постанови [5]. Оцінка дозволяє визначити рівень зрілості системи безпеки та ступінь дотримання нормативних положень.

На основі отриманих даних формується звіт про аудит, який містить узагальнені результати перевірки, виявлені порушення, аналітичні висновки та рекомендації щодо усунення недоліків. Після затвердження звіту розпочинається етап реагування - розроблення та впровадження коригувальних дій для усунення виявлених проблем і підвищення рівня захищеності інформаційних систем.

Завершальним етапом процесу є повторна перевірка або моніторинг, який проводиться відповідно до постанови [6]. Його мета - перевірити ефективність виконаних коригувальних заходів, оцінити залишкові ризики та забезпечити безперервність удосконалення системи управління інформаційною безпекою. Після завершення моніторингу процес аудиту вважається завершеним, а результати використовуються для планування наступного циклу перевірок.

Таким чином, нормативна база, сформована Національним банком України, створює комплексне підґрунтя для ефективного управління ризиками, підвищення рівня кіберзахищеності фінансових установ і забезпечення стабільності банківської системи в умовах сучасних інформаційних загроз.

1.2. Огляд міжнародних стандартів

Аудит інформаційної безпеки в банківській сфері неможливо реалізувати ефективно без урахування міжнародного досвіду та загальновизнаних стандартів, що забезпечують методологічну послідовність та контрольну сумісність. Одним із ключових документів є стандарт ISO/IEC 27001, який визначає загальні вимоги до системи управління інформаційною безпекою (СУІБ). Організація повинна запровадити, впроваджувати, підтримувати та постійно покращувати систему управління інформаційною безпекою» [7].

Захист інфраструктури бізнесу – це одна з найкращих і найбільш виправданих інвестицій для будь-якого керівника. Тому що кожні 39 секунд у світі відбувається нове кібервторгнення. У 2022 році кібератаки стали не лише поширенішими, а й значно складнішими. За останні роки постерігали, як зловмисники використовували вразливості великих корпорацій, таких як Colonial Pipeline, JBS USA, а також ключових медичних закладів. У міру того як торгівля особистими даними, медичною інформацією та фінансовими записами на Даркнеті набуває масового характеру, стає зрозуміло, що кібератаки не зникнуть у найближчому майбутньому. Навпаки - із розвитком квантових обчислень наступне десятиліття обіцяє бути ще складнішим і непередбачуванішим [8].

Фреймворк NIST (National Institute of Standards and Technology) - це затверджений урядом США набір рекомендацій, описаний у публікації Special Publication 800-53. Він узгоджується зі стандартом Federal Information Processing Standard (FIP) 200 і широко використовується федеральними агентствами для забезпечення відповідності вимогам безпеки та впровадження систем управління інформаційною безпекою (ISMS), за винятком тих, що безпосередньо займаються національною безпекою [9].

Хоча стандарт NIST містить велику кількість вимог і є досить ґрунтовним, він більше підходить для організацій, які не хочуть витрачати багато часу на адаптацію під власну галузеву специфіку. Через це фреймворк вважається дещо загальним. NIST забезпечує міцну основу саме в напрямку інформаційної безпеки, але може бути недостатньо комплексним для управління всією системою кіберзахисту - людьми, процесами та технологіями. Водночас NIST CSF залишається відмінним інструментом кіберуправління, і навіть панель ORNA Risk & Compliance базується саме на ньому. Панель керування GRC ORNA на основі NIST зображено на рисунку 1.2.

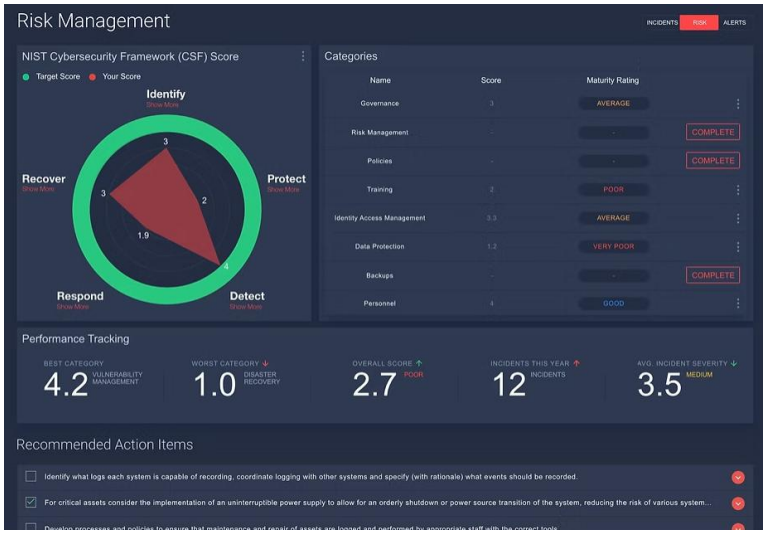


Рисунок 1.1 - Панель керування GRC ORNA на основі NIST

NIST Cybersecurity Framework (CSF) - це універсальний фреймворк для управління кіберризиками, який встановлює структурований підхід до виявлення, захисту, виявлення, реагування та відновлення IT-систем. Він

корисний для аудиту інформаційної безпеки тим, що дає чітку модель оцінювання поточного рівня захисту, дозволяє визначати прогалини в контролях та порівнювати стан системи з рекомендованими практиками. CSF підтримує ризик-орієнтований підхід, оскільки передбачає класифікацію активів, аналіз загроз і визначення пріоритетів перевірок. Завдяки модульності та сумісності з іншими стандартами (ISO 27001, NIST SP 800-53, COBIT), фреймворк допомагає аудиторам проводити комплексну оцінку системи ІБ та формувати обґрунтовані рекомендації щодо посилення безпеки. [10]. Однак, як і у випадку з NIST, їхня основна слабкість полягає в тому, що реальна кібербезпека є всеосяжною проблемою, яку неможливо вирішити лише зусиллями IT-відділу.

Додатково, у міжнародній практиці часто використовується спеціалізований документ NIST SP 800-53, який містить вичерпний перелік контрольних засобів захисту для інформаційних систем, починаючи від фізичної безпеки і закінчуючи криптографією, моніторингом подій та управлінням ідентичністю. Він широко адаптований у регуляторних документах не лише США, але й країн Європейського Союзу, а також у рекомендаціях українських органів кібербезпеки. Ефективне управління журналами подій є необхідним для точного аналізу інцидентів безпеки та судових розслідувань [10]. У межах ризик-орієнтованого аудиту цей документ може слугувати базовим орієнтиром для побудови системи контролів і перевірок відповідності. Його вимоги дозволяють структурувати процес оцінки кіберризиків та узгодити внутрішні політики з міжнародними практиками. Використання підходів NIST SP 800-53 підвищує рівень зрілості системи управління інформаційною безпекою та забезпечує доказову базу для аудиту. [11].

COBIT (Control Objectives for Information and Related Technology) - це потужний фреймворк, який допомагає керівникам будувати ефективні процеси управління у сферах стратегії, інновацій, ризик-менеджменту, управління активами тощо. Його остання версія - COBIT 2019, а вперше він був представлений ще у 1996 році та досі підтримується Information Systems Audit and Control Association (ISACA). COBIT регулярно оновлюється відповідно до

нових технологічних реалій і широко використовується як великими корпораціями, так і малими бізнесами [10].

COBIT має високу прикладну цінність у сфері аудиту завдяки чітким контрольним цілям, механізмам оцінки зрілості процесів, а також метрикам, що дозволяють кількісно визначати рівень управління IT-активами. COBIT дає змогу підприємствам створювати оптимальну цінність від IT, підтримуючи баланс між отриманням переваг та оптимізацією ризиків і ресурсів [11]. COBIT орієнтований не лише на IT-підрозділи, але й на керівництво, що дозволяє формувати міжрівневу відповідальність за ІБ.

ITIL (Information Technology Infrastructure Library) - це набір найкращих практик, спрямованих на узгодження бізнес-цілей із ресурсами IT. Розроблений британським урядовим агентством Central Computer and Telecommunications Agency (CCTA) у 1980-х роках, ITIL спочатку складався із 30 великих томів і був орієнтований на державний сектор. Згодом його значення значно розширилося, і нині ITIL активно використовується у приватних компаніях. Для зручності структура фреймворку скорочена до п’яти томів [11].

Сучасна версія ITIL приділяє велику увагу корпоративній культурі, інтеграції IT у загальну бізнес-структуру та сприяє тіснішій співпраці між IT та іншими підрозділами. Вона наголошує на важливості зворотного зв’язку з клієнтами, адже сучасні компанії мають більше можливостей аналізувати думку споживачів і рівень задоволеності завдяки розумній аналітиці даних.

Останні оновлення цих фреймворків лише посилили їхню взаємодоповнюваність. Хоча ISO та NIST також мають важливе значення, для максимальної ефективності та комплексного підходу до управління кіберризиками найкращим вибором буде поєднання COBIT 2019 і ITIL 4 для GRC (Governance, Risk & Compliance), а також NIST CSF - для безпосереднього управління кібербезпекою, зображено на рисунку 1.3. Такий комбінований підхід дозволяє одночасно охопити стратегічний, операційний та технічний рівні управління ІБ. Він забезпечує узгодженість процесів, підвищує прозорість прийняття рішень і сприяє формуванню єдиного центру відповідальності за

кіберризики. Крім того, інтеграція цих фреймворків спрощує аудит, уніфіковує процеси контролю та дозволяє ефективніше відстежувати динаміку рівня безпеки в організації.

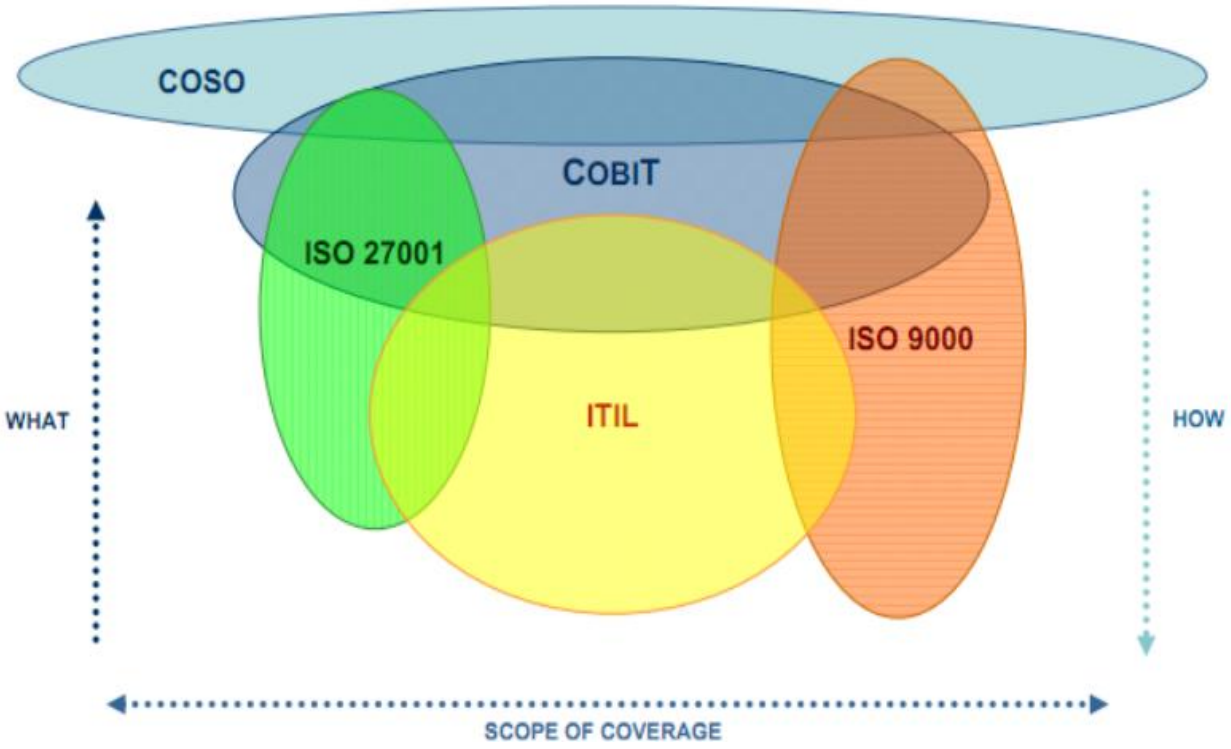


Рисунок 1.2 – Взаємодія стандартів аудиту [15]

PCI DSS (Payment Card Industry Data Security Standard) - це міжнародний стандарт безпеки даних платіжних карт, розроблений для захисту інформації власників карток під час її зберігання, обробки та передавання. Він встановлює чіткі технічні та організаційні вимоги, такі як сегментація мережі, шифрування, контроль доступу, моніторинг подій та регулярне тестування безпеки [14].

Усі компоненти, що зберігають, передають чи обробляють дані платіжних карток, мають відповідати суворим вимогам захисту та моніторингу. Порівняння міжнародних стандартів зображено у таблиці 1.2.

Таблиця 1.2 – Результати порівняння міжнародних стандартів у сфері аудиту інформаційної безпеки

Номер	Ключові вимоги та положення	Мета документа	Відповідність міжнародним стандартам
ISO/IEC 27001:2013	- Визначає вимоги до створення, впровадження та підтримки Системи управління інформаційною безпекою (СУІБ).- Базується на циклі PDCA (Plan-Do-Check-Act).- Передбачає управління ризиками, політиками, процедурами та безперервне вдосконалення системи.	Забезпечення системного підходу до управління інформаційною безпекою організації, підвищення рівня захищеності інформаційних активів.	Є базовим міжнародним стандартом; сумісний із вимогами НБУ №95 щодо впровадження СУІБ.
COBIT 5	- Визначає контрольні цілі, процеси управління IT та оцінку зрілості.- Містить механізми аудиту, метрики ефективності та відповідальності керівництва.- Охоплює стратегічний, операційний і технічний рівні управління IT.	Забезпечення ефективного управління IT та контролю за інформаційними процесами; підтримка балансу між ризиками, ресурсами та вигодами.	Узгоджується з вимогами НБУ №4 (контроль кібербезпеки, управління ризиками); відповідає принципам ISO/IEC 38500.
NIST SP 800-53	- Містить перелік контрольних заходів безпеки (контролів) для IT-систем.- Визначає вимоги до управління доступом, журналювання, криптографії, реагування на інциденти.- Застосовується у державному та фінансовому секторі.	Формування комплексної системи технічних та організаційних заходів для забезпечення кіберзахисту інформаційних систем.	Узгоджується з вимогами ISO/IEC 27001 та ISO/IEC 27002; частково - з НБУ №95 і №43 (контроль подій, реагування на інциденти).
NIST Cybersecurity Framework (CSF)	- Визначає п’ять основних функцій: Identify, Protect, Detect, Respond, Recover.- Забезпечує управління кіберризиками через оцінку поточного і цільового стану безпеки.- Підтримує адаптацію до специфіки організації.	Надання універсальної моделі для побудови системи управління кібербезпекою та вдосконалення процесів реагування на інциденти.	Відповідає ISO/IEC 27005 (управління ризиками) та вимогам НБУ №4, №43 (кіберзахист і моніторинг ризиків).
PCI DSS (Payment Card Industry Data Security Standard)	- Регламентує захист даних платіжних карток.- Містить 12 базових вимог: шифрування, контроль доступу, тестування, моніторинг, політики безпеки.- Встановлює вимоги до мережевої безпеки та зберігання даних.	Захист платіжної інфраструктури від несанкціонованого доступу та шахрайства; забезпечення довіри користувачів до платіжних систем.	Узгоджується з вимогами НБУ №43 (захист платіжної інфраструктури); сумісний із ISO/IEC 27032 (кіберзахист).

У сучасних умовах цифровізації банківських послуг аудит інформаційної безпеки потребує комплексного та системного підходу, який поєднує організаційні, технічні та процесні аспекти захисту інформаційних активів.

Використання міжнародних стандартів, таких як ISO/IEC 27001, COBIT, NIST та PCI DSS, дозволяє забезпечити методологічну послідовність, вимірюваність ефективності заходів та безперервне вдосконалення системи управління інформаційною безпекою.

Наступним кроком є оцінка поточного стану інформаційної безпеки та встановлення цілей. На цьому етапі за допомогою принципів COBIT і NIST Cybersecurity Framework (CSF) проводиться аналіз рівня зрілості процесів безпеки, визначаються пріоритети та цілі вдосконалення системи захисту.

На основі результатів моніторингу проводиться виявлення інцидентів і виконання коригувальних дій, що відповідає етапу «Act» у моделі PDCA. У разі виникнення інцидентів застосовуються методики NIST та ISO/IEC 27001 для усунення порушень і попередження їх повторення.

Після стабілізації системи здійснюється етап відновлення та підвищення рівня безпеки, що відповідає фазі “Recover” у NIST CSF. Його мета - забезпечити безперервність бізнес-процесів і відновити повноцінну роботу інформаційних систем після інцидентів [18].

Проаналізувавши як постанови Національного банку України, так і міжнародні стандарти у сфері аудиту інформаційної безпеки, було розроблено комплексний алгоритм проведення перевірок, що враховує специфіку фінансового сектору та кращі світові практики.

Міжнародні стандарти, такі як ISO/IEC 27001, ISO/IEC 27005, COBIT, NIST та PCI DSS, забезпечують гнучкий і процесно-орієнтований підхід до аудиту. Вони дозволяють використовувати універсальні методи оцінки ризиків, визначення ключових контрольних точок, застосування метрик ефективності та впровадження циклу PDCA (Plan-Do-Check-Act). Крім того, стандарти передбачають інтеграцію управління інформаційною безпекою в загальну систему корпоративного управління, що дає змогу забезпечити взаємозв’язок між бізнес-цілями та IT-цілями, посилюючи стратегічну роль інформаційної безпеки у фінансових установах. Вони орієнтовані на різні типи організацій і можуть адаптуватися до будь-якої інформаційної інфраструктури, забезпечуючи

повторюваність, об’єктивність і безперервне вдосконалення заходів безпеки [19].

1.3 Методологічні принципи проведення аудиту інформаційної безпеки

На практичному рівні ефективність аудиту інформаційної безпеки значною мірою залежить від внутрішньої нормативної документації організації, зокрема політик, процедур та регламентів. Рамкова модель NIST спрямована на безперервне вдосконалення кіберзахисту через управління ризиками.

Для забезпечення системності, об’єктивності та відтворюваності аудиту інформаційної безпеки критично важливим є наявність формалізованої внутрішньої методики, затвердженої на рівні керівництва установи. Така методика повинна враховувати регуляторні вимоги, зокрема Постанову НБУ №95, бути узгодженою з юридичним відділом та службою інформаційної безпеки, а також включати детальну структуру проведення перевірок.

Методологічне забезпечення аудиту ІТ передбачає розробку чітких процедур і стандартів перевірки з урахуванням специфіки інформаційної інфраструктури організації. Типова методика повинна містити визначення цілей та сфери охоплення аудиту, опис нормативної бази, джерела доказів (інтерв’ю, сканування, аналіз логів), контрольні точки, ризик-орієнтовану шкалу оцінювання, формат звіту та архівування результатів. Такий підхід дозволяє забезпечити системність, повторюваність і об’єктивність аудиторських перевірок, а також узгодженість з міжнародними стандартами, такими як ISO/IEC 27001, COBIT або NIST.

Види аудиту інформаційної безпеки

У практиці банківських установ застосовуються такі види аудиту:

– внутрішній аудит проводиться силами підрозділів або служб безпеки та оцінює відповідність внутрішнім політикам і стандартам; саме на ньому зосереджуються всі подальші дослідження;

– зовнішній аудит здійснюють незалежні експерти або сертифіковані

аудитори для об’єктивної оцінки відповідності міжнародним стандартам;

– цільовий аудит концентрується на окремих процесах або системах, наприклад, платіжній інфраструктурі, веб-додатках чи управлінні криптографічними ключами;

– регулярний (плановий) аудит передбачає періодичну перевірку всіх компонентів системи інформаційної безпеки для підтримки постійної готовності до інцидентів, тоді як позаплановий виконується у разі критичних подій або змін у нормативно-правовому полі.

Проведення аудиту базується на ключових принципах: системність (охоплення всіх критичних активів і процесів), об’єктивність (оцінка на основі фактів та перевірених даних), повторюваність (можливість відтворення результатів), пріоритетність ризиків (фокус на найбільш критичних загрозах), інтеграція в загальну систему управління ризиками та безперервність і вдосконалення (використання результатів для поліпшення політик і процедур).

Для реалізації цих принципів застосовуються різні методи: документальна перевірка політик, процедур і журналів; інтерв’ю та опитування персоналу для оцінки обізнаності та практичного виконання політик; технічне сканування та тестування вразливостей для виявлення слабких місць; аналіз журналів і логів для перевірки активності користувачів та IT-систем; а також тестування процедур реагування на інциденти через симуляції атак або інших подій.

Таке комплексне поєднання видів аудиту, принципів та методів забезпечує системний, об’єктивний і відтворюваний процес оцінки інформаційної безпеки, що відповідає вимогам НБУ та міжнародним стандартам, і дозволяє формувати ефективні рекомендації для усунення вразливостей та підвищення рівня кіберстійкості організації.

На практичному рівні ефективність аудиту інформаційної безпеки значною мірою залежить від внутрішньої нормативної документації організації, зокрема політик, процедур та регламентів. Процедури деталізують конкретні кроки для реалізації політик - наприклад, алгоритми реагування на інциденти, регламент резервного копіювання, порядок внесення змін до конфігурацій

систем.

Методологічне забезпечення аудиту інформаційної безпеки передбачає розробку чітких процедур, критеріїв та стандартів оцінювання, що враховують архітектуру, технологічні особливості та ризики IT-середовища організації. Типова методика аудиту ІБ повинна містити визначення цілей і меж перевірки, опис нормативних вимог, перелік джерел доказів (політики, журнали подій, конфігурації систем, результати сканувань, інтерв'ю з персоналом), структуру контрольних точок, ризик-орієнтовану модель оцінки контролів, правила формування висновків, порядок ведення робочої документації та збереження результатів. Такий підхід забезпечує системність, повторюваність і незалежність перевірок, а також уніфікованість аудиторських процедур у межах всієї СУІБ.

Проведений аналіз методологічних аспектів аудиту інформаційної безпеки свідчить, що ефективність перевірок безпосередньо залежить від наявності формалізованої внутрішньої методики, затвердженої керівництвом та узгодженої з регуляторними вимогами, зокрема: Положенням про організацію заходів із забезпечення інформаційної безпеки в банківській системі України (Постанова Правління Національного банку України від 28.09.2017 № 95), Положенням про застосування Національним банком України заходів впливу за порушення законодавства з питань інформаційної безпеки та кіберзахисту (Постанова Правління Національного банку України від 19.05.2021 № 43) та Положенням про планування, організацію та здійснення нагляду за платіжною інфраструктурою (Постанова Правління Національного банку України від 16.01.2021 № 4).

Окрім цього, методика повинна враховувати рекомендації міжнародних стандартів, таких як ISO/IEC 27001 та ISO/IEC 27002 щодо контролів, COBIT щодо управління IT-процесами, NIST SP 800-53 та NIST CSF щодо управління кіберризиками, а також практичні галузеві керівництва на кшталт OWASP для оцінки рівня безпеки застосунків.

Це дозволяє забезпечити комплексність аудиту, підвищити його точність та узгодити внутрішні підходи організації з міжнародно визнаними практиками

кіберзахисту.

Системний підхід до аудиту передбачає визначення цілей і сфери охоплення перевірок, структурування контрольних точок, формування джерел доказів і методів оцінювання ризиків, а також узгодження процедур з іншими функціями організації, зокрема юридичним відділом та службою інформаційної безпеки. Така методика забезпечує повторюваність, об’єктивність та інтеграцію аудиту в загальну систему управління ризиками.

Використання різних видів аудиту - внутрішнього, зовнішнього, цільового, планового та позапланового - у поєднанні з принципами системності, об’єктивності, пріоритетності ризиків та безперервного вдосконалення дозволяє охопити всі критично важливі активи і процеси. Методи проведення аудиту, включно з документальним аналізом, інтерв’ю, технічним скануванням, аналізом логів та тестуванням процедур реагування на інциденти, забезпечують всебічну оцінку стану інформаційної безпеки та дозволяють своєчасно виявляти вразливості.

Таким чином, поєднання внутрішньої методики, різних видів аудиту, принципів та методів перевірок створює системний, структурований і відтворюваний процес оцінки інформаційної безпеки, який відповідає вимогам національного регулятора та міжнародних стандартів. Це дозволяє підвищити ефективність контролю, зменшити ризики суб’єктивної оцінки та забезпечити централізоване управління інформаційною безпекою у фінансово-кредитних установах.

1.4. Процес взаємодії аудиту з інформаційною безпекою.

Під час процесу аудиту інформаційної безпеки у фінансових установах часто виникають проблеми з інтерпретацією технічних деталей, затримками у наданні інформації та непорозуміннями щодо обсягу перевірки. Для подолання цих бар’єрів доцільно впровадити роль технічного координатора з боку служби ІБ – фахівця, який забезпечує технічний супровід аудиту в межах своєї компетенції, пояснює архітектуру, політики, журнали подій, механізми

контролю, виступає єдиною контактною особою між службою ІБ та аудиторами у технічному контексті, а також фіксує, узгоджує і верифікує надані дані. Така роль вже застосовується у ряді фінансових установ як best practice під час перевірок критичних ІТ-систем і дозволяє зменшити кількість хибних висновків аудитів. ІТ-аудит відіграє ключову роль у цифровій трансформації, забезпечуючи прозорість процесів і мінімізуючи ризики через автоматизовані засоби контролю.

Впровадження координатора дає низку переваг: спрощує комунікацію між сторонами, зменшуючи навантаження на працівників ІБ, які не беруть безпосередньої участі в аудиті; прискорює процес перевірки завдяки централізованому доступу до інформації та глибокому розумінню систем; знижує кількість непорозумінь, оскільки технічні нюанси оперативно роз’яснюються аудитору, що формує точнішу картину реального стану інформаційної безпеки. Практика показує, що більшість затримок під час аудитів пов’язані саме з технічними складнощами у комунікації або з потребою погоджень між кількома рівнями ІБ-структури. Крім того, координатор виступає посередником між аудиторами та технічними фахівцями, забезпечуючи узгодженість дій і своєчасне надання необхідних даних.

По-перше, слід забезпечити логування всіх взаємодій координатора з аудиторами – запити, відповіді, доступи мають фіксуватись у спеціалізованих журналах.

По-друге, критичні дії (наприклад, надання логів або доступу до систем) мають виконуватись лише за участі іншого співробітника ІБ або за погодженням з аудиторами.

По-третє, необхідна формалізація процесу у вигляді окремої політики, де буде чітко прописано функціонал координатора, межі його відповідальності, процедури контролю та санкції за порушення. І, нарешті, дії координатора повинні бути максимально прозорими: аудитор має знати, які саме джерела, методи та інструменти були використані для підготовки відповідей. Рекомендується, щоб роль координатора, а також звіти про його дії, регулярно

переглядалися аудиторським комітетом банку для недопущення зловживань і втрати об’єктивності.

1.5 Аналіз інструментів для автоматизації аудиту

У сучасних умовах цифрової трансформації фінансових установ автоматизація аудиторських процесів стає критично важливою для підвищення ефективності, точності та оперативності перевірок. Використання спеціалізованих інструментів дозволяє аудиторам швидко обробляти великі обсяги даних, виявляти аномалії, контролювати дотримання внутрішніх політик та зовнішніх стандартів, а також формувати наочні та інтерактивні звіти для керівництва. Розділ присвячений аналізу сучасних програмних рішень, які застосовуються для автоматизації IT-аудиту та аудиту даних у банківському та корпоративному середовищі, а також їх перевагам і обмеженням у контексті великих організацій.

Power BI – це інструмент від Microsoft, призначений для завантаження, обробки, аналізу та візуалізації даних. Його головна перевага полягає у здатності перетворювати “сирі” дані з різних джерел (Excel, CSV, SQL-бази, журнали подій) у зрозумілі графіки, таблиці та інтерактивні дашборди. Таким чином, Power BI не є вузькоспеціалізованим аудиторським інструментом на зразок IDEA чи ACL, але він ідеально підходить для швидкої аналітики та візуалізації, особливо коли дані надаються у вигляді CSV, Excel чи SQL dump [20].

CaseWare IDEA – це спеціалізований програмний продукт для аудиту та аналітики даних, який широко використовується у фінансових установах, аудиторських компаніях та підрозділах внутрішнього контролю. Основним недоліком цього рішення є те, що CaseWare IDEA є платним програмним продуктом, і для його використання потрібна комерційна ліцензія, що може бути вагомим обмеженням для організацій із обмеженим бюджетом [21].

ACL Robotics (нині входить до платформи Diligent, раніше відома як Galvanize) – це потужний інструмент для автоматизації аудиту, контролю та управління ризиками. Продукт спеціалізується на роботі з великими обсягами

даних і надає аудиторам можливість швидко витягувати інформацію з різних джерел, перевіряти її на відповідність правилам та створювати автоматизовані процедури контролю Основним недоліком ACL Robotics є те, що це комерційне рішення з платною ліцензією, тому його впровадження може вимагати суттєвих фінансових витрат, особливо для організацій, які не мають великого бюджету на IT-аудит та автоматизацію [22].

Tableau – це сучасний інструмент бізнес-аналітики та візуалізації даних, який дозволяє швидко перетворювати великі масиви інформації у зрозумілі графіки, діаграми та інтерактивні дашборди. Продукт особливо ефективний у випадках, коли необхідно виявити закономірності та аномалії у складних наборах даних. [23]. Порівняння забражене у таблиці 1.3.

Таблиця 1.3 – Результати порівняння інструментів автоматизації

Інструмент	Основне призначення	Переваги	Недоліки	Доцільність використання у банках
Power BI (Microsoft)	Аналітика та візуалізація даних	Простота інтеграції з Microsoft-середовищем, гнучка візуалізація, підтримка великих даних	Не є вузькоспеціалізованим аудиторським продуктом; обмежена автоматизація перевірок	Ідеальний для візуалізації аудиторських даних, аналізу активності користувачів і контролю доступів
CaseWare IDEA	Спеціалізований аудит даних і контролів	Професійний інструмент для аудиторів, підтримує скрипти, глибокий аналіз	Платна ліцензія; складніша інтеграція з IT-системами	Підходить для внутрішнього аудиту банків і контролю транзакцій
ACL Robotics (Diligent)	Автоматизація аудиту, контролю та управління ризиками	Високий рівень автоматизації, масштабованість, інтеграція з системами управління ризиками	Висока вартість, потребує навчання персоналу	Найбільш ефективний для великих фінансових установ із розгалуженою IT-інфраструктурою
Tableau	Бізнес-аналітика та візуалізація даних	Висока наочність, інтерактивність, швидкий аналіз даних	Платна ліцензія; безкоштовна версія не підходить для конфіденційних даних	Доцільно використовувати для аналітики результатів аудиту та презентацій керівництву

Існує безкоштовна версія Tableau Public, проте вона має суттєве обмеження: усі створені дашборди зберігаються у відкритому доступі в інтернеті, що робить її непридатною для роботи з конфіденційними банківськими чи корпоративними даними [23].

Основним обмеженням більшості спеціалізованих рішень є висока вартість ліцензій, що може бути фактором при впровадженні в організаціях із обмеженим бюджетом. Загалом, використання цих інструментів дозволяє підвищити прозорість аудиторських процесів, оптимізувати роботу внутрішніх і зовнішніх аудиторів та забезпечити оперативне виявлення ризиків у великих банківських і корпоративних системах.

1.6 Дослідження застосування штучного інтелекту для аудиту інформаційної безпеки

Останні роки характеризуються стрімким впровадженням технологій штучного інтелекту (ШІ) у найрізноманітніші сфери діяльності - від фінансів і медицини до державного управління та освіти. ШІ дедалі частіше використовується для автоматизації рутинних завдань, оптимізації бізнес-процесів, роботи з великими масивами даних і навіть для підтримки прийняття рішень. Такий тренд не оминув і сферу аудиту, зокрема IT-аудит та інформаційну безпеку, де швидкість обробки даних, точність виявлення аномалій і контроль за відповідністю нормативним вимогам мають вирішальне значення [24].

Проте, поряд із новими можливостями, впровадження ШІ породжує і низку викликів: від ризиків витоку конфіденційної інформації та появи «галюцинацій» у висновках моделей - до невизначеності у питаннях нормативного регулювання. Це робить тему застосування ШІ в IT-аудиті надзвичайно актуальною та потребує ґрунтовного аналізу як технічних, так і правових аспектів.

Використання універсальних мовних моделей загального призначення, таких як ChatGPT, Gemini, Claude, Copilot та інші, у сфері аудиту інформаційної безпеки наразі є обмеженим і не відповідає вимогам професійної аудиторської діяльності. Основна причина полягає у відсутності галузевої адаптації таких

систем. Вони не мають доступу до закритих корпоративних даних, не враховують специфіку нормативних документів Національного банку України, стандартів ISO/IEC 27001, ISO/IEC 27005, NIST SP 800-53, COBIT та внутрішніх політик фінансових установ.

Мовні моделі типу Gemini чи ChatGPT мають загальний алгоритм навчання, який базується на масових інтернет-даних. Це означає, що вони не здатні точно відтворювати структуру аудиторського звіту, аналізувати фінансові та технічні показники у специфічному контексті, а також надавати висновки, які можна використати у нормативно значущих документах. Їхні відповіді часто не мають доказової бази, що створює ризики помилкових висновків, некоректного оцінювання ризиків та викривлення аналітичної інформації. У практиці IT-аудиту така похибка може призвести до невірного трактування рівня інформаційної безпеки або помилкової оцінки відповідності стандартам [25].

Крім того, універсальні ШІ-моделі часто використовують хмарні середовища з відкритим доступом, що несумісно з вимогами банківського сектору до захисту конфіденційної інформації. Дані, передані для аналізу, можуть потенційно бути використані у подальшому навчанні моделей або потрапити у зовнішні бази. Це створює прямий ризик витоку чутливої інформації про клієнтів, системи чи аудиторські результати, що є порушенням політик НБУ та вимог ISO 27001 щодо контролю доступу і захисту даних.

Оптимальним напрямом розвитку в цьому контексті є створення спеціалізованих моделей штучного інтелекту, навчених на основі історичних аудиторських звітів, результатів перевірок, описів ризиків та чинних нормативних актів. Важливо, щоб навчальні набори регулярно оновлювалися відповідно до змін законодавства, постанов НБУ, міжнародних стандартів і внутрішніх процедур аудиту.

Застосування такої галузево-орієнтованої моделі може радикально підвищити ефективність ризик-орієнтованого аудиту інформаційної безпеки, оскільки вона не лише аналізуватиме дані, а й зможе передбачати ймовірність повторення інцидентів, виявляти кореляції між подіями у різних системах і

пропонувати оптимальні сценарії усунення вразливостей. Доцільність використання спеціалізованих ШІ продемонстровано у таблиці 1.4.

Таблиця 1.4 – Результати порівняння універсальних ШІ та корпоративних моделей

Параметр	Універсальні ШІ-моделі (ChatGPT, Gemini, Claude тощо)	Корпоративні / спеціалізовані ШІ-моделі для IT-аудиту
Джерела даних	Масові відкриті інтернет-дані	Закриті корпоративні дані, історичні аудиторські звіти, внутрішні політики та журнали подій
Відповідність нормативним вимогам	Не адаптовані до вимог НБУ, ISO/IEC 27001, NIST, COBIT	Повністю інтегровані з внутрішніми процедурами та регуляторними вимогами
Точність висновків	Можливі «галюцинації», вигадані факти	Висока точність, достовірність підтверджується корпоративними даними та аудитом
Контроль конфіденційності	Дані можуть потрапити у хмарні сервіси, ризик витоку	Закрите корпоративне середовище (on-premise або приватна хмара), повний контроль над даними
Адаптація до специфіки організації	Загальна, не враховує внутрішні політики та специфіку інфраструктури	Підлаштована під конкретну організацію, галузеві ризики та процеси
Можливості автоматизації	Підготовка шаблонів, структуризація даних, попередній аналіз текстів	Автоматичне виявлення аномалій, кореляція подій, формування попередніх аналітичних висновків, прогнозування ризиків
Ризики	Галюцинації, некоректна оцінка ризиків, витік конфіденційної інформації, відсутність доказової бази	Обмежені, контролюються корпоративною політикою та аудитом, ризики зведені до мінімуму

Для ефективного застосування ШІ у сфері IT-аудиту необхідні спеціалізовані галузеві рішення, інтегровані безпосередньо з інфраструктурою підприємства. Одним із ключових напрямків може стати аналіз журналів подій за допомогою SIEM-систем, де ШІ здатен автоматично виявляти підозрілі дії.

1.7 Постановка завдання

Аналіз постанов НБУ, міжнародних стандартів та сучасних методологій аудиту, виконаний у першому розділі, дозволив визначити ключові недоліки традиційного підходу до аудита інформаційної безпеки у фінансово-кредитних установах. З’ясовано, що відсутній доступ до технічних даних, низька інтеграція аудиторів у процеси IT та ІБ, а також обмежена здатність реагувати на реальні

ризики призводять до поверхневості й недостатньої актуальності аудиторських перевірок.

Регуляторні вимоги задають лише загальні рамки діяльності, тоді як практичної адаптованої методики, що враховує специфіку банківських процесів та сучасний ландшафт кіберзагроз, наявні документи не надають. Порівняння з міжнародними підходами - ISO/IEC 27001, ISO/IEC 27005, COBIT, NIST CSF, NIST SP 800-53, PCI DSS - продемонструвало, що ефективність аудиту значно підвищується тоді, коли він базується на аналізі фактичних інцидентів та технічних даних, а не лише на формальних відповідях підрозділів. Саме тому, врахувавши всі виявлені обмеження та недоліки, було визначено необхідність розроблення власного ризик-орієнтованого методу аудиту інформаційної безпеки, який одночасно відповідав би вимогам регулятора, враховував би особливості фінансової установи, забезпечував би гнучку адаптацію до змін у загрозах і технологіях, підвищував би точність та об’єктивність оцінювання контролів, усував би недоліки формальних підходів та інтегрував аудит у практичні процеси ІТ і ІБ, у тому числі в реагування на інциденти.

У зв’язку з цим ставиться завдання створити цілісну методику ризик-орієнтованого аудиту інформаційної безпеки, що передбачає побудову загального процесу аудиту з урахуванням актуальних кіберризиків, визначення джерел даних та методів їх аналізу (включаючи роботу з інцидентами та журналами подій), формування карти ризиків та встановлення пріоритетності аудиторських процедур, розробку програми аудиту на основі цієї пріоритизації, створення моделі взаємодії аудиту з ІТ- та ІБ-підрозділами, визначення критеріїв оцінювання ефективності контролів, а також структури звітності та порядку формування рекомендацій. Такий підхід забезпечує логічне переходження від аналітичної частини першого розділу до практичної розробки в другому розділі, де формується цілісний авторський метод ризик-орієнтованого аудиту інформаційної безпеки.

2 РОЗРОБКА МЕТОДУ РИЗИК-ОРІЄНТОВАНОГО АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Для ефективного управління інформаційною безпекою у фінансово-кредитних установах необхідно організувати систематичний аудит і постійний моніторинг подій у інформаційних системах та бізнес-процесах. Аудит інформаційної безпеки дозволяє своєчасно виявляти слабкі місця, порушення встановлених процедур та потенційні загрози. Моніторинг і аналіз подій забезпечують оперативне реагування на інциденти, оцінку їхнього впливу та коригування заходів безпеки для зниження ризиків. Своєчасне виявлення інцидентів і їх ретельний аналіз є основою для прийняття обґрунтованих управлінських рішень і підвищення стійкості організації до кібератак.

2.1 Аналіз журналу інцидентів, ідентифікація ризиків та загальний процес аудиту

Необхідно провести аналіз інцидентів інформаційної безпеки, що мали місце у фінансово-кредитній установі протягом визначеного періоду. Такий аналіз дає змогу виявити інциденти, які потребують проведення позапланового аудиту або додаткового вивчення. На його основі визначаються рівень критичності подій, їх вплив на бізнес-процеси та інформаційні системи. У випадках, коли інциденти не потребують окремого аудиту, подальшу роботу слід здійснювати в межах планового аудиту, погодженого з керівництвом організації.

Також необхідно здійснити вивчення нормативно-правових актів і документів, що регламентують питання інформаційної безпеки у банківській сфері. Особливу увагу слід приділяти постановам Національного банку України, які встановлюють вимоги до побудови системи управління інформаційною безпекою, а також міжнародним стандартам, таким як ISO/IEC 27001, ISO/IEC 27005, COBIT і NIST SP 800-53. Такий аналіз забезпечує формування цілісного уявлення про вимоги до аудиторського процесу та його відповідність сучасним практикам управління ризиками.

На основі отриманих результатів необхідно сформувати карту ризиків процесів, у якій будуть відображені основні загрози, рівні їх критичності, пріоритетність, типи ризиків і напрями впливу на інформаційну безпеку. Інформацію для створення карти ризиків слід отримувати з відкритих джерел (нормативних документів Національного банку, міжнародних стандартів, аналітичних звітів), а також з внутрішніх джерел - журналів інцидентів та результатів попередніх аудитів.

Приклад карти ризиків зображено у таблиці 2.1.

Таблиця 2.1 – Приклад карти ризиків аудиту ІБ

Ризик	Ймовірність	Вплив	Рівень ризику	Заходи з мінімізації
Несвоєчасне надання логів і звітів ІБ-службою	Висока	Середній	Високий	Встановлення чітких SLA, впровадження технічного координатора, централізоване управління доступами
Неправильна інтерпретація технічних даних аудиторами	Середня	Високий	Високий	Залучення технічного координатора, проведення попередніх тренінгів для аудиторів
Маніпуляції з даними або приховування інформації	Низька	Високий	Середній	Логування дій координатора, участь другого співробітника при критичних діях, регулярні перевірки аудиторським комітетом
Витік конфіденційної інформації під час аудиту	Середня	Високий	Високий	Контроль доступів, шифрування переданих даних, формалізація процесів у політиці

Після створення карта ризиків була погоджена з керівництвом та відповідальними особами за окремі процеси, що забезпечило її актуальність і практичну придатність для подальшого використання [26].

Після затвердження карти ризиків була опрацьована програма аудиту, у якій визначено об’єкти перевірки, етапи роботи, методи збору інформації, критерії оцінки результатів та порядок звітування. Було підготовлено відповідний службовий лист на адресу підрозділів, які підлягали перевірці, із зазначенням мети, строків і обсягу аудиту.

Такий підхід забезпечить офіційне інформування відповідальних осіб та

створив умови для прозорої взаємодії між аудитом і підрозділами установи.

Під час проведення аудиту було організовано зустрічі з представниками перевірюваних підрозділів. У ході зустрічей було зібрано необхідну інформацію щодо специфіки діяльності, функціонування систем і наявних політик безпеки. Кожна зустріч протоколювалася, що дозволило забезпечити відтворюваність та документальне підтвердження усіх обговорених питань. Зібрана інформація стала основою для подальшого етапу перевірки - тестування систем [26].

Під час тестування було дотримано принципу обов'язкового погодження дій із власниками систем, якими зазвичай виступають керівники напрямів. Тестування проводилося залежно від типу перевірюваної системи: для мережевої інфраструктури використовувалися інструменти сканування портів і сервісів (зокрема, nmap), для вебсистем - засоби виявлення вразливостей, а для баз даних - методи перевірки доступів і політик збереження даних. Усі дії виконувалися з дотриманням етичних норм аудиту, без втручання у стабільну роботу систем чи порушення конфіденційності інформації.

У процесі перевірки виявлені інциденти та порушення політик інформаційної безпеки були задокументовані. Про кожен зафіксований випадок було повідомлено керівництво установи та власників систем. Для підтвердження результатів до звітів було додано скріншоти, технічні витяги з журналів подій та інші підтверджувальні матеріали. Такий підхід забезпечив об'єктивність результатів і можливість їх незалежної перевірки.

У випадках, коли власник системи не погоджувався із висновками аудиту або мав заперечення щодо наданих зауважень, питання передавалося на розгляд вищого рівня управління. Така ескалація тривала до моменту ухвалення остаточного рішення, яке не завжди приймалося на користь аудиторської сторони, однак забезпечувало баланс інтересів і дотримання корпоративних процедур. У разі погодження з результатами аудиту власником системи розроблявся план усунення виявлених недоліків, який проходив погодження з аудиторською групою. Аудитори брали участь у формуванні цього плану, надаючи аналітичні матеріали, рекомендації та технічні пропозиції щодо

усунення вразливостей [27].

Тестування систем проводилося у стислий термін, із дотриманням принципів оперативності та ефективності. Особлива увага приділялася раціональному використанню часу, оскільки в межах одного процесу могло бути перевірено десятки або навіть сотні систем. Такий підхід дозволив мінімізувати часові витрати та одночасно забезпечити повноту перевірки. Зібрані результати стали основою для формування підсумкового звіту з аудиту, у якому узагальнено інформацію про виявлені ризики, надано рекомендації та визначено напрямки подальшого підвищення рівня інформаційної безпеки.

Загалом проведений ризик-орієнтований аудит відзначався високим рівнем структурованості та ефективності. Основна відмінність від традиційного аудиту полягала у фокусуванні не на повному обсязі перевірок, а на тих процесах і системах, які мали найвищий рівень ризику. Це дозволило досягти балансу між глибиною дослідження, оперативністю виконання та практичною значущістю отриманих результатів. Проведена робота сприяла удосконаленню системи управління інформаційною безпекою, оптимізації аудиторських процедур та підвищенню рівня готовності установи до реагування на сучасні кіберзагрози.

Аудит інформаційних систем дозволяє не лише виявляти технічні вразливості, а й оцінювати їхній вплив на досягнення стратегічних цілей підприємства. Одним із визначальних чинників об’єктивності аудиту є наявність формалізованих метрик та чітко окреслених критеріїв оцінювання [28]. Відсутність кількісних показників призводить до надмірної суб’єктивізації висновків аудиторів, що унеможливлює порівняльний аналіз результатів у динаміці чи між підрозділами. Серед базових метрик, які можуть бути застосовані: середній час виявлення інциденту (MTTD), середній час реагування (MTTR), відсоток систем з актуальними оновленнями, рівень відповідності політик фактичним налаштуванням. Крім того, впровадження шкал зрілості процесів (наприклад, за моделлю Capability Maturity Model) дозволяє ідентифікувати прогалини в управлінні та формувати цільовий профіль розвитку ІБ [29]. Зростання цифровізації банківських послуг вимагає переосмислення

підходів до аудиту – від формальної перевірки документів до глибинного аналізу бізнес-процесів. Таким чином, поєднання якісних та кількісних критеріїв в аудиторській методології сприяє не лише прозорості перевірок, але й підвищенню ефективності управління ризиками.

Ключові метрики для оцінки ефективності аудиту інформаційної безпеки зображено у таблиці 2.2

Таблиця 2.2 - Ключові метрики для оцінки ефективності аудиту інформаційної безпеки

Метрика	Формула / спосіб вимірювання	Коментар
Кількість інцидентів за квартал	Логи SIEM	Динаміка за період
Середній час реакції на інцидент (MTTR)	Сума часу реагування / кількість інцидентів	Оцінка ефективності реагування
Частка облікових записів без MFA	Кількість акаунтів без MFA / загальна кількість	Визначення критичних вразливих точок

Введення кількісних показників в аудит інформаційної безпеки дозволяє значно підвищити об'єктивність та аналітичну цінність результатів перевірки. Завдяки метрикам, які відображають рівень відповідності, кількість виявлених вразливостей, час реагування на інциденти, частоту оновлення політик безпеки тощо, аудитори можуть не лише фіксувати поточний стан ІБ, а й виявляти динаміку змін, тенденції покращення або погіршення. Це, своєю чергою, створює основу для порівняння між підрозділами, періодами або типами систем.

2.2 Процеси та організація аудиту інформаційної безпеки відповідно до вимог НБУ та міжнародних стандартів

У сучасних умовах цифровізації фінансового сектору аудит інформаційної безпеки набуває особливої значущості, оскільки від ефективності функціонування системи управління інформаційною безпекою залежить стабільність діяльності фінансово-кредитних установ та рівень їх кіберстійкості. Регуляторні вимоги Національного банку України, а також міжнародні стандарти у сфері інформаційної безпеки визначають необхідність системного,

процесно-орієнтованого підходу до організації та проведення аудиту.

У цьому підрозділі розглянуто модель процесу аудиту інформаційної безпеки у фінансово-кредитних установах відповідно до вимог нормативно-правових актів Національного банку України та міжнародних стандартів [15, 16, 17]. Особливу увагу приділено послідовності етапів аудиту, ролям учасників процесу, механізмам взаємодії між аудиторами та службою інформаційної безпеки, а також можливостям застосування інструментів автоматизації для підвищення ефективності аудиторських процедур.

Алгоритм проведення аудиту відповідно до вимог Національного банку до СУІБ зображено на рисунку 1.1.

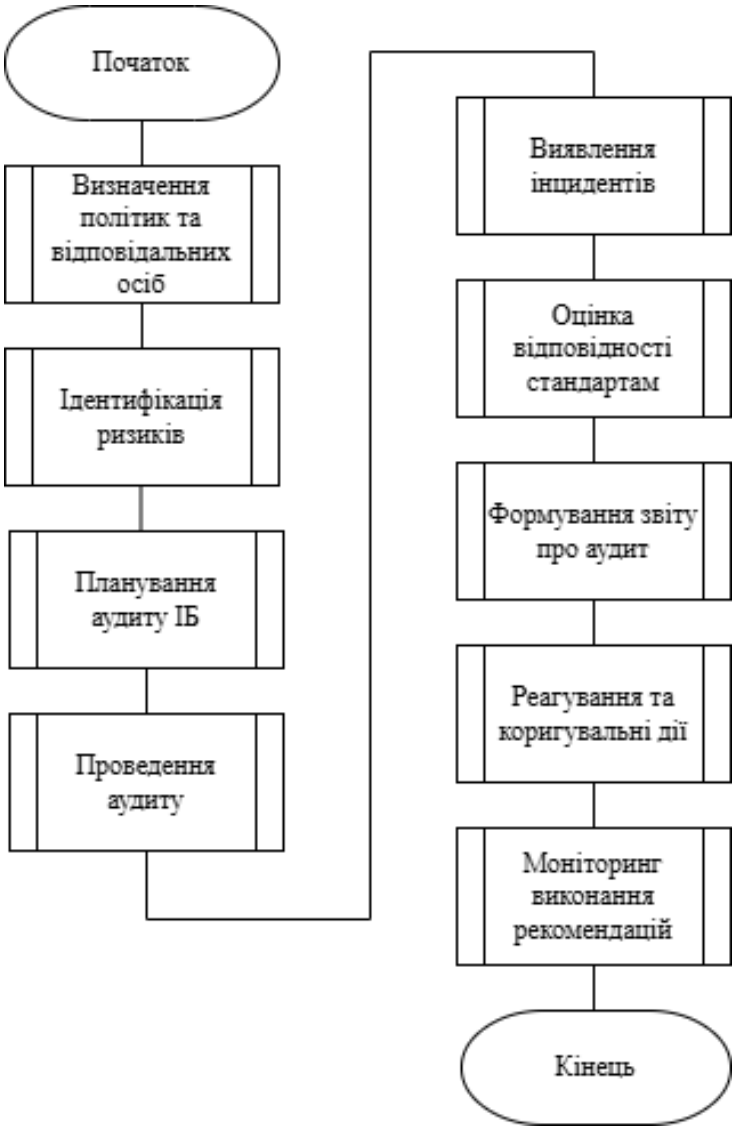


Рисунок 2.1 – Схема проведення аудиту відповіднно до чиного законодавства

Зображена блок-схема демонструє послідовність етапів процесу аудиту інформаційної безпеки (ІБ) у фінансово-кредитних установах відповідно до вимог постанов Національного банку України. Процес аудиту починається з визначення політики інформаційної безпеки та призначення відповідальних осіб, що регламентується постановою НБУ №95. На цьому етапі формується нормативна основа аудиту, уточнюються цілі, принципи та межі перевірки, а також визначаються учасники процесу [16].

Зазначений підхід, визначений нормативними актами Національного банку України, формує базову регуляторну рамку проведення аудиту інформаційної безпеки у фінансово-кредитних установах та встановлює обов'язкові організаційні й контрольні вимоги. Водночас практика аудиту інформаційної безпеки потребує застосування більш гнучких і деталізованих методологій, які дозволяють комплексно оцінювати ризики, ефективність контролів та рівень зрілості системи управління інформаційною безпекою. Саме тому поряд із вимогами НБУ доцільним є використання міжнародних стандартів, які доповнюють регуляторний підхід та забезпечують процесну, ризик-орієнтовану модель аудиту. зображено на рисунку 1.4.

Зображена блок-схема відображає процес аудиту інформаційної безпеки відповідно до міжнародних стандартів ISO/IEC 27001, COBIT та NIST CSF. Процес розпочинається з етапу ідентифікації активів, загроз і ризиків, під час якого здійснюється збір даних про інформаційні ресурси організації, визначаються потенційні вразливості та ризики, що можуть вплинути на безпеку. Цей етап базується на підходах, визначених у стандартах ISO/IEC 27001 та NIST [17].

Аналіз міжнародних стандартів ISO/IEC 27001, COBIT та NIST показує, що ефективний аудит інформаційної безпеки базується на процесно-орієнтованому, ризик-орієнтованому підході з чітким розподілом обов'язків, визначенням ролей та забезпеченням належної комунікації між підрозділами організації.

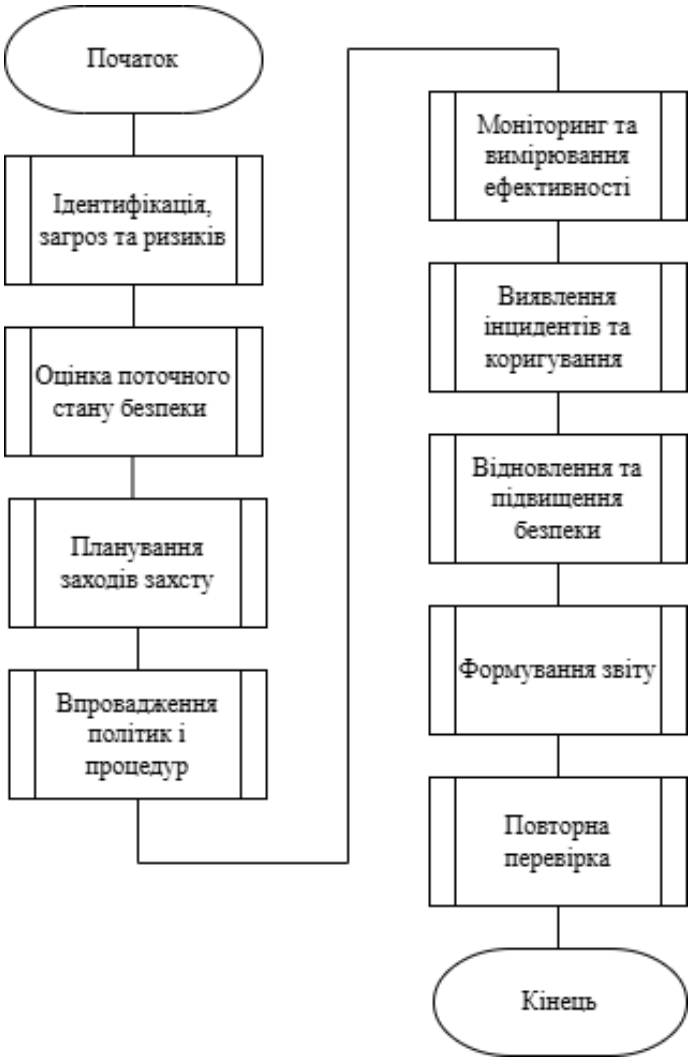


Рисунок 2.2 - Схема проведення аудиту відповіднно до міжнародних стандартів

Блок-схема процесу аудиту за міжнародними стандартами демонструє послідовність дій, починаючи від ідентифікації активів, загроз та ризиків до перевірки контролів і моніторингу, що забезпечує циклічність та інтеграцію аудиту у загальну систему управління ризиками. Для підвищення ефективності виконання цих процедур доцільним є залучення ризик-координатора, який відповідає за централізовану координацію доступу аудитора до технічних даних, пояснення структури інформаційних систем та підтримку процесів аналізу ризиків. Введення цієї ролі не суперечить вимогам Національного банку України та міжнародних стандартів, оскільки законодавство та стандарти лише вимагають наявності відповідальних осіб та належних процедур.

На рисунку 2.3, продемонстровано порядок запиту доступу, погодження прав, проведення аудиту та моніторингу.

Рисунок 2.3 – Схема взаємодії аудиторів та ризик-координаторів

Залучення ризик-координатора створює основу для більш структурованого та контрольованого процесу аудиту, оскільки він забезпечує аудиторам централізований доступ до технічних даних, пояснює архітектуру інформаційних систем та координує взаємодію зі службою інформаційної безпеки. Це значно підвищує точність та об’єктивність оцінки ризиків, дозволяє своєчасно ідентифікувати критичні інциденти та формувати актуальну карту ризиків на основі реальних даних. На наступному етапі, інтеграція інструментів автоматизації аудиту, таких як Power BI, CaseWare IDEA, ACL Robotics або Tableau, дозволяє ефективно обробляти великі обсяги інформації, візуалізувати результати перевірок і автоматизувати рутинні операції. Ризик-координатор

виступає ключовим посередником між аудиторами та автоматизованими системами, забезпечуючи правильний доступ до даних, коректне налаштування інструментів та контроль тестових процедур, що в комплексі підвищує ефективність і достовірність аудиторських висновків. Таким чином, поєднання ролі ризик-координатора з автоматизацією аудиту забезпечує цілісну, процесно-орієнтовану та технологічно підкріплену систему оцінки інформаційної безпеки фінансово-кредитної установи.

Схема автоматизації аудиту зображено на рисунку 2.4.

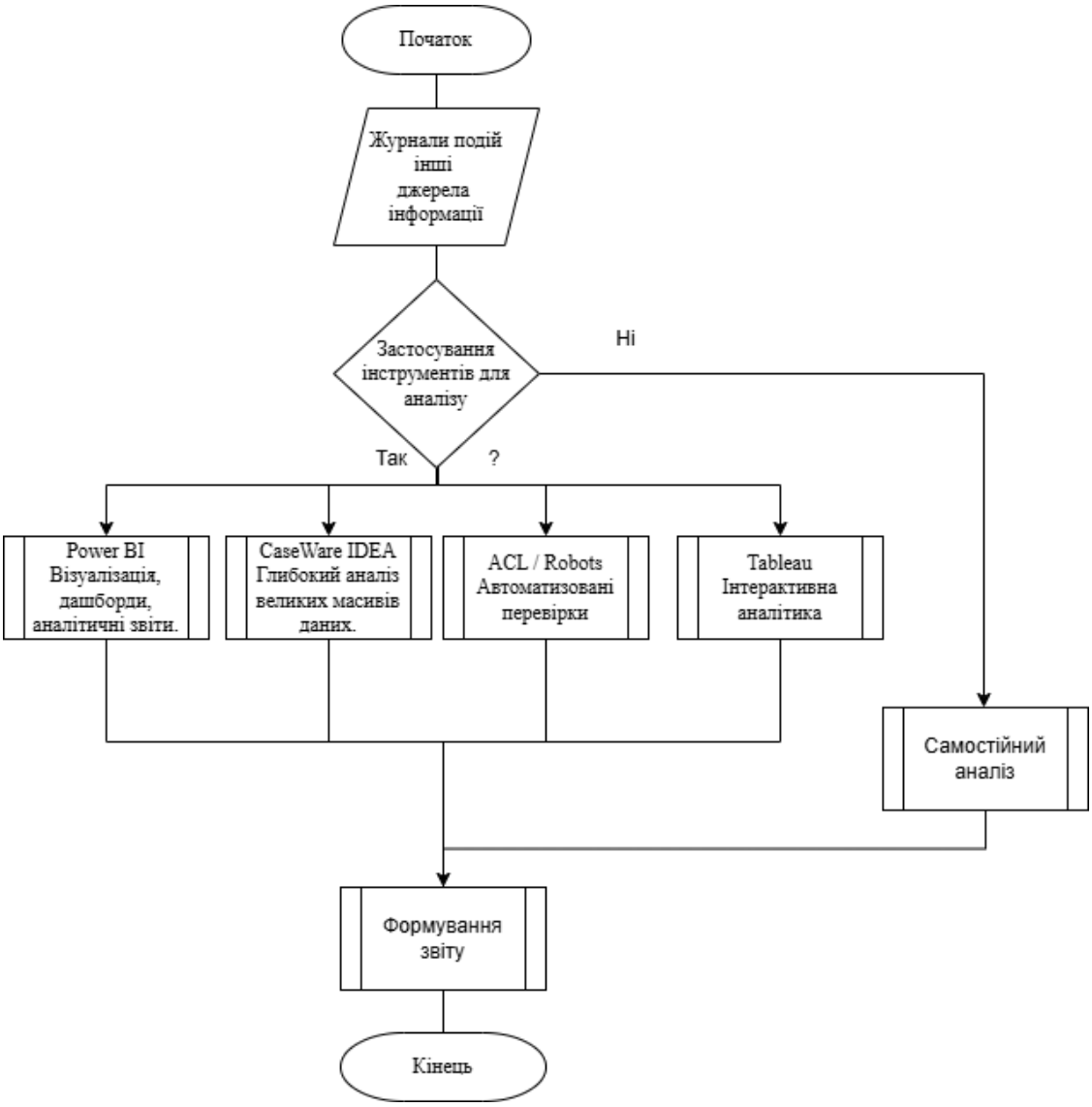


Рисунок 2.4 – Схема автоматизації аудиту

Розгляд інструментів для автоматизації аудиту показав, що сучасні рішення здатні суттєво підвищити ефективність перевірок, скоротити рутинну роботу та забезпечити більш глибокий аналіз даних. Power BI забезпечує швидку візуалізацію та інтерактивний аналіз даних без спеціалізованих аудиторських функцій, тоді як CaseWare IDEA та ACL Robotics пропонують розширені можливості для комплексного аудиту, автоматизації перевірок та контролю відповідності. Tableau надає гнучкі можливості для візуалізації та аналізу аномалій, проте його безкоштовна версія має обмеження щодо конфіденційності даних.

У розділі розглянуто процес аудиту інформаційної безпеки у фінансово-кредитних установах відповідно до вимог Національного банку України та міжнародних стандартів ISO/IEC 27001, COBIT і NIST. Показано послідовність етапів аудиту, роль відповідальних осіб та значення процесної, ризик-орієнтованої моделі перевірок. Обґрунтовано доцільність залучення ризик-координатора для централізованої координації доступу до даних і забезпечення об’єктивності оцінки ризиків. Крім того, продемонстровано, що інтеграція інструментів автоматизації аудиту підвищує ефективність перевірок, дозволяє обробляти великі обсяги інформації та формує достовірну карту ризиків на основі фактичних даних, що забезпечує комплексну оцінку інформаційної безпеки.

2.3 Формування карти ризиків

Ризик-орієнтований аудит інформаційної безпеки – це підхід до проведення аудиту, при якому основна увага та ресурси аудиторської діяльності зосереджуються на областях, процесах, системах та активах, які несуть найвищі ризики для досягнення цілей організації, зокрема щодо конфіденційності, цілісності та доступності інформації. Управління ризиками має важливе значення для підтримання дієвої системи внутрішнього контролю кожної компанії. Менеджмент організації несе відповідальність за ідентифікацію ризиків та управління ними під час провадження діяльності. Водночас роль

внутрішнього аудиту полягає в засвідченні факту належного управління ризиками. З цією метою аудитори використовують ризик-орієнтований підхід до проведення внутрішнього аудиту. Основних аспекти ризик-орієнтованого аудиту зображено на таблиці 3.3.

Такий підхід дозволяє:

– пріоритезувати аудиторські зусилля;
– ефективніше виявляти критичні вразливості та недоліки контролів;
– надавати керівництву релевантну інформацію про найбільші загрози.

Таблиця 2.3 – Параметри ризик-орієнтованого аудиту

Параметр	Опис
Основна увага аудиту	Процеси, системи та активи з високим ризиком
Цілі	Конфіденційність, цілісність, доступність інформації
Переваги	Пріоритизація ресурсів, релевантні висновки, виявлення критичних вразливостей

Оцінка ризиків ІБ базується на взаємодії загрози (Threat), вразливості (Vulnerability) та вартості активу (Asset Value). Основними компонентами оцінки є ймовірність реалізації загрози та розмір шкоди (наслідки).

Формули для оцінки ризиків у ІТ потрібні для структурованого і об’єктивного підходу до управління ризиками. Їх застосування дозволяє аудиторам, ІТ-спеціалістам та керівництву банку зрозуміти, які загрози є критичними, а які менш важливими, і розподілити ресурси на захист найцінніших активів.

Базова формула ризику

$$\text{Risk} = \text{Probability} \times \text{Impact}$$

Визначає загальний рівень ризику для конкретного активу або процесу. Показує, наскільки ймовірно настання загрози і яку шкоду вона може завдати.

Probability (Ймовірність) – оцінка того, наскільки можлива реалізація загрози (наприклад, атака на сервер або витік даних).

Impact (Вплив/наслідки) – оцінка шкоди для організації у разі реалізації

ризику: фінансова, репутаційна, операційна. Використовується для якісної або умовно-кількісної оцінки ризиків. Наприклад, висока ймовірність і високий вплив = критичний ризик, низька ймовірність і низький вплив = низький ризик.

Очікувана тривалість одного збитку (SLE)

$$SLE = Asset\ Value\ (AV) \times Exposure\ Factor\ (EF)$$

Визначає очікуваний збиток від одного інциденту для конкретного активу.

Дає змогу кількісно оцінити потенційні втрати у грошовому або ресурсному вираженні.

Asset Value (AV) – вартість активу, який підлягає захисту (наприклад, сервер, база даних, платіжна система).

Exposure Factor (EF) – коефіцієнт впливу, тобто яка частка вартості активу буде втрачена або пошкоджена внаслідок інциденту (від 0 до 1).

Наприклад, сервер коштує 100 000 грн, EF = 0.3 → SLE = 30 000 грн.

Це означає, що один інцидент може завдати збитків на 30 000 грн.

Annualized Loss Expectancy (ALE)

$$ALE = SLE \times ARO$$

Визначає очікувані річні збитки від конкретного ризику. Дозволяє керівництву планувати бюджет на заходи безпеки та пріоритезувати ресурси.

SLE – збиток від одного інциденту (розрахований за попередньою формулою).

ARO (Annualized Rate of Occurrence) – очікувана кількість інцидентів на рік (наприклад, 0.5 – один інцидент кожні два роки, 3 – три інциденти на рік).

Наприклад, SLE = 30 000 грн, ARO = 0.5 → ALE = 15 000 грн річних очікуваних збитків. Це допомагає визначити, на які активи і ризики потрібно виділяти кошти на захист у першу чергу.

Матриця ризику (Risk Matrix) візуалізує співвідношення ймовірності та впливу ризику та допомагає швидко визначити пріоритетність ризиків для аудиту та контролів. Приклад матриці ризику зображено у таблиці 2.4.

Таблиця 2.4 – Приклад матриці ризику

	Низький Вплив (1)	Середній Вплив (3)	Високий Вплив (5)
Висока Ймовірність (5)	5	15	25 (Критичний)
Середня Ймовірність (3)	3	9	15
Низька Ймовірність (1)	1	3	5

Було виконано аналіз методології ризик-орієнтованого аудиту інформаційної безпеки та розглянуто ключові підходи до оцінки ризиків у банківських установах. Було показано, що застосування формул Risk = Probability × Impact, SLE та ALE дозволяє кількісно та якісно визначати пріоритетність ризиків, планувати ресурси та впроваджувати ефективні заходи контролю. Було сформовано приклад матриці ризику, що наочно відображає взаємодію ймовірності та впливу, що дає змогу аудиторам і керівництву швидко визначати критичні загрози. Результати виконаного аналізу свідчать, що ризик-орієнтований підхід забезпечує системність і прозорість аудиту, підвищує ефективність управління інформаційною безпекою та дозволяє оптимально використовувати ресурси для захисту найцінніших активів банківської установи.

2.4Формування програми аудиту

Програма аудиту – частина документування аудиторської перевірки є внутрішнім документом аудитора. Зміст програми спирається на внутрішньофірмові правила (стандарти).

Програма аудиту включає перелік аудиторських процедур, що застосовуються в конкретній аудиторській перевірці, а також їх характер, терміни, обсяг та конкретних виконавців. Програма аудиту включає всю діяльність, необхідну для планування, організації та проведення аудитів.

Аудитору необхідно скласти та документально оформити програму аудиту, що визначає характер, часові рамки та обсяг запланованих аудиторських процедур, необхідних для здійснення загального плану аудиту. Програма аудиту є набором інструкцій для аудитора, який виконує перевірку, а також засобом контролю та перевірки належного виконання роботи. У програму аудиту також можуть бути включені передумови підготовки фінансової (бухгалтерської) звітності, що перевіряються, по кожній з областей аудиту і час, запланований на різні області або процедури аудиту.

Програма аудиту – це документ, що містить перелік завдань у певній послідовності їх виконання, за допомогою яких виходять достатні та надійні аудиторські докази відповідно до перевірки відповідних даних клієнта. Іншими словами, програма аудиту - це докладні інструкції, які повинні виконувати працівники аудиторської фірми в процесі здійснення аудиту фінансової звітності або виконання інших завдань.

Для розробки програм можна використовувати стандартні аудиторські програми або контрольні листи з аудиту, які розробляються аудиторською фірмою. Стандартні аудиторські програми є власними розробками аудиторської фірми, вони втілюють накопичений професійний досвід виконання різних видів робіт і тому є своєрідним ноу-хау.

Водночас неможливо розробити універсальні програми перевірки, тому що немає повністю схожих підприємств, навіть якщо вони працюють в одній галузі, мають схожі виробничі та організаційні структури. Завжди існуватимуть обставини щодо конкретного підприємства, які формують фактори невід’ємного ризику та ризику суттєвих спотворень. Тому, коли використовуються стандартні програми або контрольні листи, необхідно їх доопрацьовувати відповідно до умов конкретного завдання. Приклад програми аудиту зображено у таблиці 2.5.

Визначення ключових дат є критичним елементом програми аудиту інформаційної безпеки, оскільки забезпечує структурованість процесу, контроль виконання та дотримання встановлених строків. Чітко визначені Main Dates

дозволяють керівництву та аудиторській групі синхронізувати діяльність, планувати ресурси та забезпечувати своєчасне виконання перевірок.

Таблиця 2.5 – Приклад програми аудиту

№	Елемент програми	Опис
1	Об’єкти перевірки	Серверні системи, бази даних, платіжні системи, мережеве обладнання, політики та процедури ІБ, журнали подій, доступи користувачів, резервне копіювання.
2	Етапи аудиту	1. Планування та підготовка. 2. Збір інформації (аналіз документації, інтерв’ю, сканування). 3. Оцінка контролів та вразливостей. 4. Формування висновків та рекомендацій. 5. Підготовка фінального звіту.
3	Методи збору інформації	Інтерв’ю з персоналом, аналіз політик та процедур, тестування контролів, сканування систем, аудит журналів подій, перевірка конфігурацій ІТ-систем.
4	Критерії оцінки	- Відповідність внутрішнім політикам та регламентам. - Відповідність нормативним вимогам НБУ та міжнародним стандартам. - Ефективність впроваджених контролів. - Пріоритетність ризиків (використання матриці ризику).
5	Ризики та контрольні точки	- Несанкціонований доступ до систем. - Витік конфіденційної інформації. - Недотримання політик резервного копіювання. - Невчасне оновлення ПЗ та систем. Контрольні точки: управління доступами, моніторинг подій, криптографічний захист, відновлення після інциденту.
6	Відповідальні	- Аудиторська група: головний аудитор, ІТ-аудитор. - Технічний координатор служби ІБ. - Менеджмент банку (затвердження програми).
7	Терміни проведення	Плановий аудит: 1 місяць (з попереднім погодженням етапів з підрозділами).

У таблиці представлено узагальнену програму аудиту інформаційної безпеки, яка систематизує основні елементи аудиторського процесу: перелік об’єктів перевірки, послідовність етапів аудиту, методи збору та аналізу інформації, критерії оцінки відповідності та ефективності контролів, ключові ризики і контрольні точки, а також визначає відповідальних осіб і терміни проведення перевірки. Така структура забезпечує комплексний, керований і ризик-орієнтований підхід до оцінки стану інформаційної безпеки у фінансово-кредитній установі.

2.5 Розробка організаційної моделі взаємодії між аудитом і службою інформаційної безпеки

У процесі аудиту інформаційної безпеки в банках часто виникають проблеми з інтерпретацією технічних деталей, затримками у наданні інформації та непорозуміннями щодо обсягу перевірки. Для подолання цих бар'єрів доцільно впровадити роль технічного координатора з боку служби ІБ – фахівця, який забезпечує технічний супровід аудиту в межах своєї компетенції, пояснює архітектуру, політики, журнали подій, механізми контролю, виступає єдиною контактною особою між службою ІБ та аудиторами у технічному контексті, а також фіксує, узгоджує і верифікує надані дані. Така роль вже застосовується у ряді фінансових установ як best practice під час перевірок критичних ІТ-систем і дозволяє зменшити кількість хибних висновків аудитів. ІТ-аудит відіграє ключову роль у цифровій трансформації, забезпечуючи прозорість процесів і мінімізуючи ризики через автоматизовані засоби контролю.

Впровадження координатора дає низку переваг: спрощує комунікацію між сторонами, зменшуючи навантаження на працівників ІБ, які не беруть безпосередньої участі в аудиті; прискорює процес перевірки завдяки централізованому доступу до інформації та глибокому розумінню систем; знижує кількість непорозумінь, оскільки технічні нюанси оперативно роз'яснюються аудитору, що формує точнішу картину реального стану інформаційної безпеки. На практиці, що більшість затримок під час аудитів пов'язані саме з технічними складнощами у комунікації або з потребою погоджень між кількома рівнями ІБ-структури. Крім того, координатор виступає посередником між аудиторами та технічними фахівцями, забезпечуючи узгодженість дій і своєчасне надання необхідних даних. Його участь сприяє підвищенню ефективності перевірок, оскільки аудитори можуть зосередитись на аналітичній роботі, а не на організаційних питаннях. Наявність координатора також підвищує рівень довіри між підрозділами, оскільки усуває ризик перекручення або затримки інформації. У довгостроковій перспективі така роль може стати ключовим елементом системи управління ризиками, інтегруючи процес аудиту у щоденну діяльність фінансових установ. На рисунку 2.5,

продемонстровано порядок запиту доступу, погодження прав, проведення аудиту та моніторингу.

Рисунок 2.5 – Схема взаємодії між аудитором і службою ІБ

Разом з тим, роль технічного координатора створює і певні ризики, які потребують врахування. Насамперед – це ризик витоку інформації, адже координатор має доступ до повної логіки перевірки. Також існує потенційний конфлікт інтересів, оскільки координатор належить до служби, що перевіряється, що може впливати на його об’єктивність. Не менш серйозним є ризик маніпуляцій із даними, наприклад, навмисного затримання або вибіркового надання логів. У практиці були випадки, коли ІБ-координатори свідомо приховували або фільтрували інформацію, що унеможливлювало

виявлення інцидентів. Щоб уникнути таких ситуацій, необхідно впровадити дієві механізми протидії.

По-перше, слід забезпечити логування всіх взаємодій координатора з аудиторами – запити, відповіді, доступи мають фіксуватись у спеціалізованих журналах.

По-друге, критичні дії (наприклад, надання логів або доступу до систем) мають виконуватись лише за участі іншого співробітника ІБ або за погодженням з аудиторами.

По-третє, необхідна формалізація процесу у вигляді окремої політики, де буде чітко прописано функціонал координатора, межі його відповідальності, процедури контролю та санкції за порушення. І, нарешті, дії координатора повинні бути максимально прозорими: аудитор має знати, які саме джерела, методи та інструменти були використані для підготовки відповідей. Рекомендується, щоб роль координатора, а також звіти про його дії, регулярно переглядалися аудиторським комітетом банку для недопущення зловживань і втрати об’єктивності.

2.6 Формування звіту та рекомендацій аудиту

Після завершення етапів аналізу ризиків та виконання аудиторської програми розпочалося формування звіту з аудиту інформаційної безпеки. Цей документ є підсумковим результатом проведеної роботи та містить узагальнення усіх зібраних під час перевірки даних, висновки, а також рекомендації щодо підвищення рівня захищеності інформаційних систем. Формування звіту здійснювалося відповідно до затвердженої структури, що забезпечує його прозорість, логічність і практичну цінність для керівництва установи.

На початку звіту наведено загальні відомості про проведений аудит: мету, об’єкти перевірки, часові рамки, склад аудиторської групи та нормативно-правову базу, на яку спирався процес оцінювання. Далі подано короткий опис методики ризик-орієнтованого підходу, використаного під час перевірки, із зазначенням основних критеріїв оцінки ризиків, пріоритетності процесів і

систем. У звіті також зазначено, що перевірка проводилася на основі створеної карти ризиків, що дозволило сконцентрувати увагу на найбільш критичних ділянках, де ймовірність інцидентів або їхній вплив на бізнес-процеси є найвищими.

Основну частину звіту становить опис результатів аудиту. Для кожного об’єкта перевірки наведено виявлені невідповідності, порушення політик інформаційної безпеки, технічні вразливості та недоліки в організаційних заходах. Оцінювання здійснювалося за визначеними критеріями ризику з присвоєнням рівня критичності (високий, середній, низький). Кожен випадок порушення було задокументовано з наведенням підтверджувальних матеріалів - скріншотів, витягів із журналів подій, описів конфігурацій та результатів тестування.

Це забезпечило об’єктивність висновків і можливість незалежної перевірки результатів аудиту.Завершальна частина звіту містить рекомендації щодо усунення виявлених недоліків, оптимізації процедур безпеки та вдосконалення системи управління ризиками. Для кожної проблемної ділянки запропоновано конкретні заходи - як організаційного, так і технічного характеру, із зазначенням відповідальних підрозділів і орієнтовних строків реалізації. У випадках, коли недоліки потребують значних ресурсів або модернізації інфраструктури, надано пропозиції щодо поетапного впровадження змін [31].

Після узгодження звіт був переданий керівництву установи для розгляду. У разі прийняття звіту власниками систем розробляється план усунення недоліків, який затверджується керівником служби безпеки або відповідальним за інформаційну безпеку. Таким чином, звіт не лише підсумовує результати проведеного аудиту, а й слугує практичним інструментом для подальшого підвищення рівня захищеності інформаційних активів організації та вдосконалення процесів управління інформаційною безпекою.

Після завершення аналізу отриманих результатів та узагальнення виявлених порушень розпочалося формування рекомендацій за підсумками аудиту інформаційної безпеки. Цей етап мав на меті не лише зафіксувати

недоліки, а й запропонувати конкретні, практично реалізовані шляхи їх усунення та запобігання повторному виникненню аналогічних ризиків у майбутньому. Формування рекомендацій здійснювалося на основі принципів ризик-орієнтованого підходу, тобто з урахуванням рівня критичності кожного виявленого ризику, його впливу на бізнес-процеси та ресурсних можливостей установи.

Для кожного виявленого порушення або інциденту було розроблено відповідні пропозиції, які поділялися на організаційні, технічні та процедурні заходи. Організаційні рекомендації стосувалися вдосконалення політик, положень та внутрішніх регламентів у сфері інформаційної безпеки, уточнення ролей і відповідальності персоналу, підвищення рівня обізнаності працівників щодо сучасних кіберзагроз. Технічні рекомендації включали оновлення або посилення систем захисту (антивірусних рішень, міжмережевих екранів, систем виявлення вторгнень, засобів шифрування тощо), корекцію налаштувань безпеки в інформаційних системах, усунення вразливостей, виявлених під час тестування. Процедурні рекомендації охоплювали вдосконалення процесів моніторингу, управління інцидентами, резервного копіювання, контролю доступу та оновлення програмного забезпечення [32].

Кожна рекомендація супроводжувалася зазначенням пріоритетності виконання - високої, середньої або низької, залежно від рівня ризику, який вона покликана знизити. Для заходів високого пріоритету було визначено скорочені терміни реалізації, а також рекомендовано проведення повторного аудиту або проміжного контролю виконання. Для середньо- та низькоризикових рекомендацій встановлювалися планові строки виконання із подальшим моніторингом результатів у межах чергового циклу аудиту.

Усі рекомендації були сформульовані у зрозумілій, чіткій і практично орієнтованій формі, що забезпечує можливість їх безпосереднього застосування відповідальними структурними підрозділами. Для підвищення ефективності впровадження пропозицій аудиторська група не лише окреслила перелік необхідних дій, а й надала пояснення щодо їх технічної реалізації. У випадках,

коли це було доцільно, до рекомендацій додавалися приклади можливих технічних рішень, алгоритми усунення вразливостей, схематичні діаграми взаємодії компонентів безпеки або короткі методичні описи дій персоналу. Такий підхід сприяв тому, що рекомендації мали не лише аналітичний, а й прикладний характер.

У підсумку, розроблені та погоджені рекомендації стали ключовим елементом практичного результату ризик-орієнтованого аудиту, адже вони спрямовані не лише на усунення поточних недоліків, а й на довгострокове підвищення рівня зрілості системи управління інформаційною безпекою.

2.7 Розробка методу ризик-орієнтованого аудиту інформаційної безпеки

Аудит інформаційної безпеки базується на вимогах Національного банку України, міжнародних стандартах [9,10,11,15] та практичних підходах до оцінювання ефективності кіберзахисту. На основі аналізу цих джерел розроблено метод ризик-орієнтованого аудиту інформаційної безпеки, який забезпечує відповідність регуляторним вимогам і міжнародним стандартам, а також враховує актуальний рівень ризиків та постійні зміни у ландшафті кіберзагроз. Основна ідея методу полягає у переході від формального аудиту лише за чек-листами до гнучкого та динамічного підходу, коли обсяг і глибина перевірок визначаються не планом, а фактичними ризиками та інцидентами.

У межах цього підходу аудит розпочинається зі збирання та аналізу оперативної інформації про інциденти, події безпеки та стан контролів. Аудиторам необхідно отримати дані першої та другої лінії захисту, журнали інцидентів, інформацію із систем SIEM і засобів моніторингу, а також результати попередніх аудитів. Це забезпечує можливість оцінити реальний стан інформаційних систем, виявити тенденції, визначити сфери з підвищеною активністю загроз і сформувати базу для подальшої оцінки ризиків.

На основі зібраних відомостей формується карта ризиків, яка включає ідентифіковані загрози, рівні їх критичності, пріоритети аудиторських дій,

власників ризиків, типологію ризиків та можливий вплив на бізнес-процеси. Карта ризиків у цьому методі не є статичним документом - вона регулярно оновлюється відповідно до нових інцидентів, результатів моніторингу та технічних тестувань. Це дозволяє сформувати достовірний ризиковий профіль установи та визначити, які процеси потребують першочергової уваги під час аудиту [33].

Програма аудиту будується відповідно до встановлених пріоритетів ризиків. Таким чином ресурси не розподіляються рівномірно на всі системи, а сфокусовані на найкритичніших ділянках IT-інфраструктури. Це підвищує ефективність аудиту і дозволяє зосередитися на тих елементах, де ймовірність інцидентів або потенційний збиток є найвищими.

Важливою складовою методу є активна участь ризик-координаторів - технічних фахівців з IT або служби інформаційної безпеки, які забезпечують комунікацію між аудиторами та експлуатантами систем. Їх роль полягає у поясненні архітектури систем, наданні технічної інформації, супроводі тестувань та підтвердженні достовірності даних. Такий формат взаємодії підвищує точність аудиторських висновків, зменшує ризик непорозумінь та дозволяє ефективно організувати роботу в умовах складних технічних перевірок [30].

Ключовим принципом методу є підтвердження висновків на основі практичних тестувань, а не лише документів. Для цього застосовуються аналіз логів, перевірка налаштувань, технічні тести доступів та контролів, вибіркові перевірки даних у базах, а також автоматизовані засоби моніторингу й сканування вразливостей. Використання таких інструментів дозволяє аудиторам отримувати незалежні дані, що мінімізує ризик маніпуляцій інформацією і забезпечує об’єктивність результатів аудиту.

Після проведення перевірок сформовані висновки та рекомендації уточнюються спільно з ризик-координаторами для забезпечення технічної точності та релевантності. Це дозволяє привести рекомендації у відповідність до фактичних можливостей та архітектури систем і підвищує їх практичну застосовність.

Запропонований метод створює основу для побудови адаптивного, безперервного та технічно обґрунтованого аудиту інформаційної безпеки. Завдяки постійному оновленню ризик-профілю аудит перетворюється на механізм оперативного реагування на нові загрози та вразливості. Інтеграція результатів аудиту з системами моніторингу сприяє формуванню єдиного інформаційного простору для управління ризиками та підвищує ефективність внутрішнього контролю в банківській установі. У результаті ризик-орієнтований аудит забезпечує більш точну оцінку стану кібербезпеки.

Порівняння методів аудиту та запропонований зображено у таблиці 2.6

Таблиця 2.6 – Результати порівняння методів проведення аудиту

Критерій	Класичний аудит ІБ	Запропонований метод
Оцінка ризиків	Проводиться періодично за статичною картою ризиків	Оновлюється динамічно за журналами інцидентів
Джерела даних	Документи та звіти ІТ/ІБ	Реальні інциденти, SIEM, автоматизовані тести
Взаємодія	Формальна, без технічної участі ІТ/ІБ	Командна робота з ризик-координаторами
Інструменти	Переважно ручний аналіз	Автоматизовані засоби тестування й моніторингу
Об’єктивність	Залежність від наданої інформації	Незалежність через власні технічні перевірки
Мета	Перевірка відповідності	Безперервне вдосконалення на основі ризиків

У процесі розроблення методу ризик-орієнтованого аудиту інформаційної безпеки формується підхід, що має забезпечити перехід від традиційної моделі оцінювання до більш динамічного та гнучкого механізму аналізу ризиків. Використання карти ризиків як ключового інструмента дозволяє поступово визначати пріоритетні напрями аудиторської перевірки, враховуючи характер інцидентів, рівень загроз та ефективність існуючих контролів.

Паралельно опрацьовується роль ризик-координаторів і можливість застосування технічних засобів тестування, що має підвищити об’єктивність та підтверджуваність аудиторських висновків у майбутній реалізації методу.

Розроблюваний підхід покликаний створити основу для впровадження безперервного, адаптивного та технічно орієнтованого аудиту, який

відповідатиме вимогам Національного банку України та міжнародних стандартів у сфері інформаційної безпеки. Очікується, що подальша робота над методом дозволить підвищити ефективність управління ризиками, сприятиме зміцненню системи контролю інформаційної безпеки та підвищенню стійкості IT-інфраструктури фінансово-кредитної установи.

2.8 Висновки до другого розділу

Було розроблено метод ризик-орієнтованого аудиту інформаційної безпеки, який ґрунтується на аналізі ризиків конкретних інформаційних систем, процесів та активів фінансово-кредитної установи. Метод поєднує вимоги Національного банку України [4, 5, 6], положення міжнародних стандартів ISO/IEC 27001, COBIT 5, NIST SP 800-53, NIST Cybersecurity Framework (CSF) та PCI DSS, а також практичні підходи до оцінки ефективності кіберзахисту. Основні елементи методу включають аналіз фактичних подій і даних SIEM, формування карти ризиків, підтвердження висновків практичними тестуваннями контролів. Важливу роль у процесі виконують ризик-координатор, що забезпечує структуровану комунікацію, доступ до даних і технічний супровід аудиту, зменшуючи вплив людського фактора і підвищуючи об’єктивність оцінки. Запропонований метод дозволяє перейти від формальної перевірки відповідності до дійсно ризик-орієнтованого аудиту, що забезпечує ефективне управління кіберризиками, підвищує точність і актуальність висновків та створює основу для подальшого впровадження автоматизації і технологій штучного інтелекту у внутрішній аудит інформаційної безпеки. Такий підхід сприяє постійній адаптації аудиторських процедур до змін у технологічному середовищі та розвитку нових загроз. Він також забезпечує кращий зворотний зв’язок для керівництва банку та підвищує обізнаність персоналу про кіберризики.

3 ПРАКТИЧНЕ ВПРОВАДЖЕННЯ РИЗИК-ОРІЄНТОВАНОГО АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1 Інтеграція та автоматизація аудиту

У межах практичного етапу впровадження ризик-орієнтованого аудиту інформаційної безпеки було проведено аналіз можливостей інтеграції різних інструментів автоматизації аудиту, серед яких розглядались Power BI, CaseWare IDEA, ACL Robotics та Tableau. Аналіз охоплював технічну сумісність із корпоративною інфраструктурою, вартість ліцензій, питання підтримки та безпеки, а також відповідність внутрішнім політикам використання програмного забезпечення у фінансово-кредитній установі.

До впровадження нового методу аудиту в Банку процеси внутрішнього аудиту здійснювалися виключно за допомогою стандартних інструментів Office 365, переважно Excel, SharePoint та Outlook. Аудиторські перевірки виконувалися на відповідність внутрішнім політикам, процедурам та нормативним вимогам, а весь аналіз даних проводився вручну за допомогою зведених таблиць Excel. Для формування вибірок аудитори завантажували дані у вигляді CSV або XLSX-файлів та налаштовували моделі аналізу самостійно, що вимагало високого рівня володіння складними формулами, логічними блоками обробки даних та макросами VBA. Рівень автоматизації фактично був відсутній: кожна перевірка виконувалася з нуля, а макроси не були уніфікованими чи централізованими, що створювало залежність від людського фактору.

Значна частина часу йшла на технічні операції, такі як очищення та сортування даних, ручне формування висновків і копіювання результатів аналізу до фінальних звітів. Через це збільшувалась тривалість проведення аудиту, а ризики помилок у формулах або при обробці даних були досить високими. Відсутність єдиного шаблону та уніфікованої методології призводила до того, що різні аудитори будували зведені таблиці по-своєму, що ускладнювало узгодження результатів та контроль якості. Будь-які зміни у внутрішніх

процедурах вимагали повної переробки Excel-моделей, а передача роботи від одного аудитора іншому була проблематичною через відсутність документації та індивідуальний підхід до логіки макросів. Усе це робило процес трудомістким, немасштабованим і таким, що потребував суттєвого покращення та переходу до більш стандартизованих та автоматизованих рішень.

На даний час реалізовано лише інструменти екосистеми Microsoft, зокрема Power BI та супутні рішення, оскільки вони офіційно погоджені з підрозділом інформаційної безпеки фінансової установи та відповідають внутрішнім політикам. Впроваджене рішення дозволяє підключати наявні джерела даних та створювати автоматизовані панелі моніторингу ризиків, що значно спрощує збір інформації для формування карти ризиків і оцінки актуальних загроз. Розглядається можливість розширення існуючої ліцензії Power BI для підключення додаткових джерел даних та реалізації більш складних аналітичних сценаріїв у майбутньому.

Використання інших спеціалізованих систем, таких як CaseWare IDEA, ACL Robotics та Tableau, на даному етапі відхилено через низку причин: відсутність фінансування на придбання комерційних ліцензій, непогодження служби інформаційної безпеки щодо використання стороннього програмного забезпечення в межах внутрішньої інфраструктури фінансової установи , а також складність інтеграції цих рішень із наявними корпоративними системами та базами даних. Крім того, впровадження сторонніх систем потребувало б додаткового навчання персоналу та розробки внутрішніх методичних матеріалів для коректного використання. Також відсутність централізованого контролю за інтеграцією могла б створити ризики несумісності даних та дублювання інформації. Незважаючи на це, проведений аналіз показав потенціал цих систем для подальшого підвищення ефективності аудиту та можливості масштабування процесів у майбутньому. Таким чином, етап автоматизації аудиту реалізовано частково, із збереженням відповідності політикам безпеки та можливістю подальшого розширення функціоналу у разі отримання фінансування та погодження з підрозділом інформаційної безпеки.

Таблиця 3.1 – Результати порівняння інструментів аудиту до і після впровадження нового підходу

Параметр	До впровадження інструментів автоматизації	Після впровадження
Інструменти для аналізу	Office 365: Excel, SharePoint, Outlook; ручне формування зведених таблиць	Power BI та супутні рішення Microsoft, офіційно погоджені підрозділом ІБ
Рівень автоматизації	Відсутній; всі обчислення та аналіз даних вручну	Часткова автоматизація панелей моніторингу та візуалізації даних
Обробка даних	Завантаження CSV/XLSX, очищення та сортування вручну; формули та макроси налаштовувалися індивідуально	Підключення джерел даних до Power BI, централізоване формування панелей та звітів
Уніфікація процесу	Відсутня; кожен аудитор використовував власні моделі, макроси та логіку	Єдиний підхід у межах Microsoft Power BI; стандартизовані панелі для аудиторів
Ризики помилок	Високі: помилки формул, некоректне сортування даних, суб'єктивність	Значно зменшені: використання централізованих панелей з фактичними даними
Час на підготовку та аналіз	Тривалий: велика частина часу витрачалася на технічні операції	Скорочений: дані підключаються та візуалізуються у Power BI, підготовка карти ризиків спрощена
Масштабованість	Обмежена; важко передавати роботу іншим аудиторам через відсутність документації	Покращена: стандартизовані панелі дозволяють легко масштабувати процес та додавати нові джерела даних
Можливості подальшого розвитку	Висока залежність від індивідуальних навичок аудиторів, складно розширювати процес	Можливість підключення додаткових джерел даних та розширення аналітичних сценаріїв у майбутньому

На поточному етапі впровадження ризик-орієнтованого аудиту автоматизація аудиторських процесів реалізована частково та обмежується використанням інструментів екосистеми Microsoft. Відмова від інших спеціалізованих систем зумовлена технічними, фінансовими та організаційними обмеженнями, що дозволяє забезпечити безпеку та відповідність внутрішнім політикам. Разом із цим, сформовано основу для подальшого розширення функціоналу та інтеграції додаткових аналітичних інструментів після отримання фінансування та погодження з підрозділом ІБ, що відкриває перспективу підвищення ефективності та масштабованості аудиту у майбутньому.

3.2 Використання технологій штучного інтелекту у аудиті

До початку впровадження елементів штучного інтелекту інфраструктура фінансової установи повністю ґрунтувалася на традиційних підходах до обробки та аналізу даних. Усі процеси виконувалися виключно з використанням людського ресурсу та стандартних можливостей інформаційних систем, які забезпечували лише базові операції збору, зберігання та обрахунку даних. Будь-яка аналітика формувалася вручну на основі результатів, отриманих із внутрішніх систем, без застосування алгоритмів машинного навчання, інтелектуальної обробки даних або автоматизованих механізмів виявлення аномалій. У фінансовій установі були відсутні як інструменти ШІ, так і технології, що дозволяють проводити аналітику, прогнозування чи автоматичну інтерпретацію даних. Внаслідок цього аудиторам та аналітикам доводилося самостійно інтерпретувати результати, здійснювати логічні зіставлення, виявляти невідповідності та формувати висновки. Весь процес був повністю залежним від людського досвіду, навичок та уважності, що значно збільшувало операційне навантаження, створювало ризики помилок і обмежувало можливості для масштабування та підвищення ефективності аналітичних процедур.

Разом із тим, активне впровадження технологій штучного інтелекту (ШІ) у фінансово-кредитній установі викликало питання регламентації з боку Національного банку України (НБУ) та Державної служби спеціального зв’язку та захисту інформації України (ДССЗЗІ). На даний момент регулятори працюють над створенням методичних рекомендацій щодо безпечного застосування ШІ у фінансовій сфері, зокрема у частині захисту конфіденційних даних та недопущення витоку інформації.

Банком придбано корпоративну ліцензію та погоджено з підрозділом інформаційної безпеки використання моделі ШІ Copilot від Microsoft. Проте її функціональні можливості не повністю відповідають потребам аудиту, оскільки Copilot орієнтований переважно на персональну взаємодію з користувачем, а не на обробку великих обсягів аудиторських даних або інтеграцію з внутрішніми

системами контролю. Питання щодо розроблення або впровадження внутрішнього ядра ШІ, спеціалізованого для аудиту інформаційної безпеки, наразі не розглядається через високу вартість реалізації, необхідність створення ізольованої обчислювальної інфраструктури та обмеження, пов’язані з регуляторними вимогами.

Таким чином, використання ШІ в аудиті наразі перебуває на початковому етапі - у форматі експериментального застосування схвалених рішень, з подальшою перспективою розвитку після затвердження чітких нормативних вимог та визначення безпечної архітектури використання.

Було здійснено часткове впровадження ризик-орієнтованого методу аудиту інформаційної безпеки. Зокрема, представника відділу внутрішнього аудиту було включено до групи швидкого реагування на інциденти інформаційної безпеки, що дозволило налагодити оперативний обмін інформацією та підвищити об’єктивність оцінки ризиків.

Разом із тим, доступ до вивантажень із SIEM та інших систем моніторингу поки не реалізовано через високу вартість ліцензійного розширення. Це питання залишається відкритим і потребує додаткового погодження з керівництвом установи. Часткове впровадження показало ефективність інтеграції аудиторів до процесів реагування на інциденти, актуалізувало необхідність автоматизації збору даних і виявило організаційні та технічні бар’єри, які потребують подальшого врегулювання для повноцінного функціонування ризик-орієнтованого аудиту.

У межах практичного етапу впровадження ризик-орієнтованого аудиту інформаційної безпеки було здійснено часткове впровадження елементів штучного інтелекту та інтеграцію аудиторів до групи швидкого реагування на інциденти. Таблиця нижче демонструє порівняння ключових параметрів аудиту до впровадження та після часткового впровадження нового підходу, включаючи рівень автоматизації, інтеграцію з системами, роль аудиторів та ефективність процесів.

Таблиця 3.2 – Резульати порівняння використання ШІ

Параметр	До впровадження	Після часткового впровадження
Використання ШІ	Повна відсутність: жодних алгоритмів машинного навчання, автоматизованих механізмів аналізу або прогнозування	Початковий етап: експериментальне використання Microsoft Copilot для окремих завдань; не інтегровано у процеси аудиту великого обсягу даних
Обробка даних та аналітика	Повністю ручна: аудитори та аналітики самостійно формували висновки, порівнювали дані та виявляли невідповідності	Часткове спрощення процесу через доступ до певних даних та участь аудитора у групі швидкого реагування; автоматизація обробки даних відсутня
Інтеграція з внутрішніми системами	Відсутня; усі дані формувалися вручну з внутрішніх систем	Часткова: аудитори отримують доступ до тестових даних та деяких систем, але SIEM та інші системи моніторингу ще не інтегровані
Регуляторні обмеження	Не застосовувалися; всі процеси виконувалися стандартними методами	Активно враховуються: впровадження ШІ обмежене корпоративними політиками та очікуванням методичних рекомендацій НБУ та ДССЗЗІ
Роль аудиторів	Залежність від індивідуальних навичок та досвіду; високий ризик помилок	Підвищення об’єктивності оцінки ризиків завдяки включенню до групи швидкого реагування; можливість отримувати оперативні дані про інциденти
Масштабованість та ефективність	Обмежена через ручну обробку даних і високу трудомісткість	Часткове підвищення ефективності процесів реагування, але повна масштабованість потребує інтеграції систем та подальшого впровадження ШІ

До впровадження елементів штучного інтелекту процеси аудиту та обробки даних у Банку були повністю ручними і залежали від досвіду та уважності персоналу, що збільшувало ризики помилок та обмежувало ефективність. Часткове впровадження ризик-орієнтованого методу, зокрема інтеграція аудитора у групу швидкого реагування на інциденти, підвищило оперативність отримання даних і об’єктивність оцінки ризиків, проте автоматизація обробки даних та повна інтеграція систем моніторингу ще не реалізована. Отримані результати демонструють потенціал використання ШІ та централізованого доступу до даних для підвищення ефективності аудиту, а також виявляють організаційні та технічні бар’єри, що потребують вирішення для повноцінного функціонування ризик-орієнтованого аудиту в майбутньому.

3.3 Організаційна взаємодія та ризик-координатора

До початку впровадження ризик-координаторів у процес супроводу аудиту підготовчий етап займав приблизно 20% усього часу, виділеного на проведення аудиту, і при цьому залишався одним з найбільш трудомістких та непередбачуваних. Значну частину цього часу аудиторам доводилося витрачати на детальне вивчення архітектури процесу, який потрапляв у сферу перевірки: структури бізнес-процесів, взаємодії між підрозділами, наявних контрольних точок, ролей та відповідальностей. У багатьох випадках інформація була розпорошеною по різних системах або зберігалася у різних підрозділах, що вимагало додаткових зусиль для її збору та верифікації.

Окремим викликом була побудова комунікації з відповідальними за процес особами. Аудиторам доводилося самостійно ідентифікувати всіх стейкхолдерів, координувати взаємодію з лінійними менеджерами, керівниками напрямів, операційними підрозділами та іншими залученими структурами. Це включало численні зустрічі, уточнення інформації, запити документів, нагадування та контроль строків надання відповідей. Такий підхід не тільки збільшував часові витрати, а й створював залежність від завантаженості інших підрозділів.

Ще одним значним елементом навантаження був етап погодження аудиторського звіту. Узгодження з усіма зацікавленими сторонами потребувало часу, оскільки аудитор мав отримати коментарі, розглянути зауваження, внести корективи, усунути суперечності між різними підрозділами та забезпечити єдине узгоджене формулювання висновків. Консолідація всіх правок часто затягувалася через велику кількість учасників процесу та різницю у підходах до оцінки ризиків.

Запровадження ролі ризик-координатора суттєво змінило ситуацію, оскільки саме ця функція бере на себе значну частину комунікаційної та організаційної роботи. Ризик-координатор здатен забезпечувати структурування інформації, підтримувати взаємодію з власниками процесів, контролювати дотримання строків, а також супроводжувати процес погодження звіту, що дозволяє аудиторам зосередитися безпосередньо на аналітичній та оціночній

частині аудиту. Це значно зменшує часові витрати на підготовчий етап і підвищує ефективність проведення аудиту загалом.

Наявність людини з середини процесу, яка може допомогти орієнтуватись в процесі краще дає змогу значно зменшити час на підготовку до аудиту. Було також затверджено координатора зі сторони ІТ, яким призначено керівника підрозділу з впровадження змін у інфраструктуру банку. Його роль полягає у технічному супроводі аудиту, забезпеченні доступу до необхідних середовищ і конфігурацій, а також у наданні підтримки аудиторській групі під час проведення перевірок. Координатор відповідає за організацію безпечного доступу до систем та баз даних, контроль виконання тестових процедур і документування результатів перевірок, що дозволяє мінімізувати ризики порушення безпеки та втрати конфіденційних даних.

Водночас ризик-координатора зі сторони служби інформаційної безпеки поки не призначено через бюрократичні складнощі, пов’язані з необхідністю оновлення посадової інструкції відповідного співробітника. Це обмежує можливості для повноцінного контролю над аудитом та оперативного реагування на потенційні загрози, оскільки відсутність координатора з ІБ ускладнює комунікацію між аудиторською групою та службою безпеки при перевірках систем.

Крім того, групу аудиторів було включено до тестової групи одного з ключових бізнес-процесів банку. Проведення подальших тестувань наразі дозволено лише після погодження з відділом інформаційної безпеки та виключно у тестових середовищах, що забезпечує безпеку виробничих систем, проте створює ризик затримок у виявленні вразливостей та повноцінному аналізі контролів. У практичній діяльності тимчасовим компромісним рішенням стало дозволення тестування під особисту відповідальність начальника ІТ-аудиту, що дозволяє частково реалізовувати аудиторські процедури до завершення формального погодження, зберігаючи при цьому контроль за безпекою й конфіденційністю даних.

Навіть часткове впровадження запропонованого методу вже продемонструвало ефективність залучення аудиторів до процесів реагування на інциденти інформаційної безпеки. Це дозволило оперативно обмінюватися даними про події, підвищило об’єктивність оцінки ризиків та актуалізувало необхідність подальшої автоматизації збору та обробки інформації. Крім того, практика впровадження виявила організаційні бар’єри, пов’язані з координацією між службами ІТ та інформаційної безпеки, бюрократичними процедурами та обмеженнями доступу до ключових даних.

Таблиця 3.3 – Результати порівняння підготовчого етапу та супроводу аудиту

Параметр	До впровадження	Після впровадження ризик-координатора
Час на підготовчий етап	~20% від загального часу аудиту; значна частина витрачається на вивчення архітектури процесів та комунікацію з підрозділами	Значне скорочення часу завдяки структурованій координації та підтримці ризик-координатора
Вивчення архітектури процесів	Аудитори самостійно досліджували бізнес-процеси, ролі, контрольні точки; інформація розпорошена	Ризик-координатор забезпечує структуровану інформацію про процеси та ролі, спрощує доступ до даних
Комунікація з власниками процесів	Високий обсяг ручної роботи: зустрічі, уточнення, запити документів, контроль строків	Координатор бере на себе більшість комунікаційної роботи, аудитори зосереджуються на аналітичній частині
Погодження звітів та консолідація правок	Часозатратно; великі об’єми коментарів та суперечностей між підрозділами	Координатор супроводжує процес погодження, контролює строки та забезпечує єдине формулювання висновків
Роль ІТ-координатора	Не передбачена	Забезпечує технічний супровід аудиту, доступ до середовищ і конфігурацій, контроль тестових процедур
Роль координатора ІБ	Відсутня; ускладнює комунікацію між аудиторами та службою безпеки	Поки не призначений через бюрократичні складнощі; обмежує повноцінний контроль та реагування
Масштабованість та ефективність	Обмежена; багато операцій залежить від навичок та завантаженості персоналу	Підвищення ефективності процесу, скорочення часу на підготовку, поліпшення об’єктивності оцінки ризиків
Тестування бізнес-процесів	Обмежене; ризик затримок через узгодження	Часткове тестування дозволено в тестових середовищах, контроль за безпекою під особисту відповідальність начальника ІТ-аудиту

Водночас часткове впровадження методу дало змогу оцінити потенціал інтеграції аудиторів у реальні бізнес-процеси банку. Було встановлено, що залучення представників IT і внутрішнього аудиту до оперативних груп дозволяє підвищити точність оцінки ризиків та своєчасність реагування на інциденти. Також під час реалізації часткових перевірок з'ясувалося, що необхідно продовжувати роботу над вдосконаленням процедур доступу, автоматизації збору даних та документування результатів аудиту, що у майбутньому забезпечить більш ефективне функціонування ризик-орієнтованого підходу.

Таким чином, навіть на цьому етапі практичного впровадження запропонований метод ризик-орієнтованого аудиту інформаційної безпеки продемонстрував свою доцільність. Він дозволяє підвищити об'єктивність аудиту, оптимізувати взаємодію між різними службами банку, актуалізувати питання автоматизації та контролю даних, а також визначити ключові напрямки для подальшого вдосконалення методології та технологічної підтримки аудиту.

3.4 Підсумкові висновки щодо практичного етапу оцінки ризиків та формування карти аудиту

У фінансовій установі формування карт ризиків базується передусім на вимогах чинного законодавства, зокрема постановах та нормативних документах Національного банку України. Для деталізації, класифікації та опису ризиків використовуються міжнародні стандарти, методології провідних регуляторів або спеціально розроблені внутрішні чек-листи, створені на основі таких стандартів. Унаслідок цього процес аудиту переважно набуває форми перевірки на відповідність лише встановленому чек-листу чи регуляторним вимогам, а не комплексної аналітичної оцінки ризиків. Такий підхід має низку суттєвих обмежень.

По-перше, використання лише чек-листів не дозволяє оперативно реагувати на швидкі зміни у глобальному та локальному ризик-ландшафті. Фінансова сфера сьогодні стикається з новими викликами, такими як кіберзагрози, еволюція шахрайських схем, новітні технології, зміни в клієнтській

поведінці, а також нестабільність ринкового середовища. Часто ці ризики ще не відображені в законодавчих вимогах або методологічних документах, а тим більше - у внутрішніх чек-листах, які можуть не оновлюватися належним чином. У таких умовах програма аудиту, складена на основі застарілих інструментів, не відображає реальної картини ризиків і може бути спрямована на перевірку аспектів, що вже втратили актуальність, замість аналізу нових критичних зон.

По-друге, такий підхід суттєво знижує гнучкість аудиту. Передбачене чек-листом поле для аналізу є фіксованим, а отже, аудитор може пропустити потенційно значущі відхилення, які просто не включені до документа. Це обмежує глибину аудиторського проникнення та створює передумови для невиявлення суттєвих ризиків у процесах Банку. Підготовка програми аудиту без повного розуміння актуального профілю ризиків унеможливлює правильну пріоритизацію, оскільки аудитор змушений орієнтуватися на формальні критерії замість реальної загрози чи впливу на бізнес.

По-третє, критично важливим аспектом є те, що інформація, яка використовується в аудиторському процесі, отримується шляхом запитів до власників процесів. Ці дані не завжди проходять незалежну верифікацію та, відповідно, можуть бути неповними або отриманими з помилками. На практиці трапляються випадки, коли дані подаються із запізненням, у застарілому вигляді або навіть із викривленнями, зумовленими людським фактором чи небажанням демонструвати недоліки. Унаслідок цього аудитор може спиратися на необ’єктивну інформацію, що вагомо впливає на якість фінальних висновків.

Загалом статичність нормативної бази, залежність від чек-листів, відсутність динамічної адаптації до поточних ризиків та ненадійність джерел даних значно знижують релевантність та ефективність аудиторських перевірок. Це обмежує здатність фінансової установи оперативно реагувати на зміни у ризик-ландшафті та приймати своєчасні управлінські рішення, засновані на об’єктивній інформації.

Після впровадження нового методу ситуація з оцінюванням ризиків, формуванням карти ризиків та побудовою програми аудиту в фінансовій

установі суттєво змінилася, хоча сам процес оцінки ризиків і надалі здійснюється вручну аудиторами, без використання автоматизованих інструментів чи алгоритмів. Основна відмінність полягає в тому, що аудитори тепер спираються не на формальні чек-листи, а на реальні технічні дані та фактичний стан інформаційних систем, що дозволяє побудувати більш об’єктивну і релевантну картину ризиків. Замість статичних та часто застарілих документів аудитори отримують доступ до звітів першої та другої лінії захисту, журналів подій, даних SIEM, конфігурацій контролів та інших джерел, що відображають реальні інциденти, відхилення й особливості роботи IT-інфраструктури.

Актуальність карти ризиків визначалася на основі результатів опитування 30 аудиторів, які брали участь у перевірках із використанням як традиційного, так і удосконаленого підходів, а також шляхом вибіркової перевірки ключових бізнес-процесів. Було опитано 10 аудиторів, які зазначили, що використання карти ризиків дозволило їм швидше визначати критичні зони перевірки та концентрувати ресурси на найбільш значущих процесах. Аудитори відзначили, що карта ризиків підвищила об’єктивність оцінки, оскільки відображала фактичний стан систем і процесів, а не лише формальні документи. Під час опитування аудитори оцінювали частку ризиків, включених до карти, що мають фактичне підтвердження у вигляді журналів подій, даних SIEM та конфігурацій контролів. Узагальнення відповідей респондентів показало, що в середньому 85–90% ідентифікованих ризиків підтверджуються фактичними технічними даними, що й було прийнято як показник актуальності карти ризиків.

Отриманий результат свідчить про те, що формування карти ризиків на основі реальних технічних даних забезпечує значно вищу відповідність ідентифікованих ризиків фактичному стану інформаційних систем порівняно з підходом, що базується виключно на формальних чек-листах і нормативних вимогах.

Програма аудиту також суттєво змінилася: замість орієнтації на загальні вимоги тепер пріоритети визначаються через аналіз реальних подій, слабких місць систем, частоти інцидентів та значущості конкретних процесів. Завдяки

цьому аудитори можуть точніше сформувати перелік процедур і приділити більше уваги тим зонам, де дійсно існують підвищені загрози.

Оцінка ефективності планування аудиту здійснювалася на основі результатів опитування 30 аудиторів, а також шляхом порівняння фактичних витрат часу на підготовчий етап аудиту до та після впровадження ролі ризик-координатора. У межах дослідження аудитори фіксували тривалість етапу планування для аналогічних за обсягом і складністю перевірок.

$$\text{Скорочення часу (\%)} = \frac{\text{Час до} - \text{Час після}}{\text{Час до}} \times 100$$

− Час до — фактичний час (години/дні), витрачений на планування аудиту до впровадження ризик-координатора.

− Час після — фактичний час, витрачений після впровадження ризик-координатора. Час до=10 днів,Час після=7 днів

$$\text{Скорочення часу (\%)} = \frac{10 - 7}{10} \times 100 = 30\%$$

Отримане скорочення часу на 30% свідчить про підвищення ефективності підготовчого етапу аудиту завдяки структурованій координації та централізованому доступу до даних через ризик-координатора

Важливу роль у новому процесі відіграє ризик-координатор, який забезпечує аудиторам доступ до потрібних даних, пояснює архітектуру систем, допомагає уточнювати технічні деталі та сприяє коректному тлумаченню інформації. Оцінка ефективності взаємодії аудиторів з підрозділами здійснювалася на основі результатів опитування 30 аудиторів, а також шляхом фіксації фактичних витрат часу на комунікацію під час проведення аудиторських перевірок до та після впровадження ролі ризик-координатора. У межах дослідження враховувалася кількість зустрічей, запитів документів, уточнень та процедур узгодження з власниками процесів.

За результатами узагальнення зібраних даних встановлено, що до впровадження ризик-координатора сумарний час на комунікацію з підрозділами складав у середньому 10 днів, тоді як після впровадження — близько 6 днів, що відповідає скороченню часу взаємодії приблизно на 40%.

Паралельно аудитори в межах опитування оцінювали рівень об’єктивності аудиторських висновків до та після впровадження удосконаленого підходу за умовною шкалою. Узагальнення результатів опитування показало, що використання фактичних технічних даних, залучення ризик-координатора та виконання практичних перевірок (аналіз логів, перегляд налаштувань, тестування контролів, вибірки з баз даних) забезпечили зростання об’єктивності оцінки на рівні 20–30%. Для оцінки зниження ризику надання неправдивих або неповних даних було здійснено вибіркову перевірку інформації, наданої власниками процесів, порівняно з фактичними технічними записами систем (логами, журналами подій, конфігураціями контролів). Було визначено частку даних, які не потребували уточнень або виправлень після порівняння із “сирими” технічними джерелами. На підставі цих спостережень експертно оцінено, що ризик надання неповних або неправдивих даних знизився приблизно на 70–80%, оскільки робота з фактичними записами значно ускладнює можливість помилок або маніпуляцій з боку власників процесів. Особливо важливим є те, що ризик неправдивих або неповних даних, які раніше надавали власники процесів, знизився приблизно на 70–80%, адже аудитори працюють зі "сирими" технічними записами, які важко підмінити або інтерпретувати неправильно. У підсумку рекомендації стали більш точними, конкретними та прив’язаними до фактичного стану контролів і систем, а ризик суб’єктивності значно зменшився. У фінансово-кредитній установі оцінка ризиків та формування карти ризиків раніше здійснювалися переважно на основі формальних чек-листів та нормативних вимог, що обмежувало актуальність і релевантність аудиту. Таблиця 3.4 демонструє ключові відмінності між підходами.

Таблиця 3.4 - Результати порівняння процесу оцінки ризиків

Параметр	До впровадження	Після впровадження ризик-орієнтованого методу
Основа формування карти ризиків	Чек-листи, стандарти, нормативні вимоги; статична інформація	Реальні технічні дані: журнали подій, SIEM, конфігурації контролів; більш актуальна інформація (~85–90%)
Пріоритизація аудиту	За формальними критеріями, орієнтація на нормативні вимоги	Аналіз слабких місць систем, частоти інцидентів та значущості процесів; час планування скоротився на ~30%
Джерела даних	Запити до власників процесів; ризик неповних або неправдивих даних	«Сирі» технічні дані; ризик помилкових даних зменшився на 70–80%
Об’єктивність оцінки	Високий рівень суб’єктивності, залежність від пояснень власників процесів	Зросла на 20–30% завдяки перевіркам фактів та участі ризик-координатора
Роль ризик-координатора	Відсутній	Забезпечує доступ до даних, пояснює архітектуру систем, допомагає у тлумаченні даних та коректному формуванні висновків
Практичне підтвердження ризиків	Не здійснювалося; аудитори спиралися на документи та відповіді	Перевірка через аналіз логів, тестування контролів, вибірки з баз даних
Гнучкість аудиту	Низька; обмежена лише чек-листами	Вища; дозволяє реагувати на актуальні ризики та формувати релевантну програму аудиту
Ризик суб’єктивності та помилок	Високий	Значно знижений, рекомендації стали точними, конкретними та прив’язаними до фактичного стану систем

Загалом новий метод дозволив перетворити аудит із формальної перевірки на відповідність у дійсно ризик-орієнтований процес, який відображає реальний стан ІТ- та ІБ-процесів у Банку та дає змогу ефективніше визначати пріоритети, незважаючи на те, що всі оцінки й надалі здійснюються вручну, без будь-якої автоматизації.

3.5 Вплив впровадження ризик-орієнтованого аудиту на процеси контролю інформаційної безпеки

У результаті впровадження методу ризик-орієнтованого аудиту інформаційної безпеки у фінансово-кредитній установі вдалося досягти низки важливих організаційних, методологічних та практичних змін, які істотно підвищили якість і об’єктивність аудиторських процедур. Насамперед було впроваджено використання інструментів екосистеми Microsoft, передусім Power

BI, що дало змогу оптимізувати процес збору та структурування даних, отриманих від першої та другої ліній захисту. Завдяки створеним панелям огляду ризиків з'явилася можливість швидше аналізувати отриману інформацію та формувати основу для карти ризиків, хоча автоматична оцінка ризиків не застосовується - усі розрахунки та інтерпретація показників продовжують здійснюватися аудиторами вручну. Водночас було визначено обмеження у впровадженні інших спеціалізованих систем (CaseWare IDEA, ACL Robotics, Tableau), що дозволило уникнути порушення вимог безпеки та мінімізувати ризики невідповідності внутрішнім політикам.

У межах роботи також було впроваджено низку організаційних змін, спрямованих на посилення взаємодії між підрозділами. Представника внутрішнього аудиту включено до групи швидкого реагування на інциденти інформаційної безпеки, що суттєво підвищило швидкість доступу до інформації про події, які формують актуальні ризики. Це дозволило аудиторам отримувати первинні дані без затримок і зменшило залежність від опосередкованих звітів. Додатково призначено IT-координатора, який забезпечує технічний супровід аудитів, налагоджує доступ до тестових середовищ та забезпечує взаємодію між аудиторським підрозділом і технічними командами. Хоча координатора зі сторони інформаційної безпеки поки не призначено, створені передумови для подальшого розширення моделі взаємодії.

Завдяки включенню аудиторів до тестової групи одного з ключових бізнес-процесів удалося отримати практичний досвід оцінювання контролів у реальних умовах, що виявило як технічні проблеми, так і організаційні бар'єри. Відсутність доступу до логів SIEM та інших систем моніторингу залишається суттєвим стримувальним фактором, проте сформовано чітке обґрунтування необхідності такого доступу та визначено наступні кроки для погодження з ІБ-підрозділом.

Попри обмежене використання інструментів автоматизації та початковий рівень експериментального застосування технологій ШІ, результати впровадження підтвердили ефективність ризик-орієнтованого підходу. Метод

дозволив істотно підвищити об’єктивність оцінки ризиків, зменшити залежність від формальних чек-листів, зосередити увагу аудиторів на найбільш вразливих ділянках та забезпечити тіснішу інтеграцію аудиту в ІТ- та ІБ-процеси фінансових установ. Отримані результати створюють підґрунтя для розширення автоматизації, покращення доступу до технічних даних і поступового інтегрування безпечних технологій ШІ у подальшу практику аудиту. У фінансово-кредитній установі до впровадження ризик-орієнтованого методу аудит здійснювався переважно на основі формальних чек-листів та ручного збору даних, що обмежувало об’єктивність та актуальність перевірок.

3.6 Висновки до третього розділу

Впровадження ризик-орієнтованого методу аудиту інформаційної безпеки дозволило фінансово-кредитній установі значно підвищити об’єктивність та якість аудиторських процедур. Використання Power BI для структурування даних оптимізувало збір і аналіз інформації, а включення представників аудиту до тестових груп та створення ролі ІТ-координатора забезпечило оперативний доступ до реальних даних і покращило взаємодію між підрозділами. Хоча автоматизація оцінки ризиків і використання ШІ залишаються на початковому етапі, новий підхід дозволив зосередити ресурси на найбільш критичних ділянках, зменшити залежність від формальних чек-листів і створити базу для подальшого розвитку технологічної та організаційної підтримки ризик-орієнтованого аудиту.

4 ЕКОНОМІЧНА ЧАСТИНА

4.1 Проведення комерційного та технологічного аудиту науково-технічної розробки

Оскільки результати МКР на тему «Метод ризик-орієнтованого аудиту інформаційної безпеки у фінансово-кредитних установах» має перспективу комерційного використання та можуть бути інтегровані у побудови ефективної системи аудиту відповідно до вимог Постанов НБУ, стандартів ISO/IEC 27001, ISO/IEC 27005, COBIT та NIST SP 800-30, виникає потреба у проведенні комерційного аудиту цієї науково-технічної розробки.

Основною метою такого аудиту є оцінювання науково-технічного потенціалу створеного методу, визначення його конкурентоспроможності та ринкових перспектив, а також формування економічного обґрунтування, яке може бути використане для залучення інвестицій і подальшої комерціалізації розробки.

У оцінюванні науково-технічного рівня і комерційного потенціалу розробки взяли участь три експерти: Войтович О. П., к.т.н., доц. кафедри захисту інформації, Дудатьєв А. В., к.т.н., доц. кафедри захисту інформації, Майданевич Л. О., к.філ.н., доц. кафедри захисту інформації.

Оцінки було проставлено згідно з рекомендованими критеріями, які зображені в додатку Г.

Результати оцінювання зображено в табл. 4.1.

Середньоарифметична сума балів розраховується за формулою:

$$\text{СБ} = \frac{\sum_{i=1}^{3} \text{СБ}_i}{3} \tag{4.1}$$

Таблиця 4.1 – Результати оцінювання науково-технічного рівня і комерційного потенціалу розробки експертами

Критерії	Бали		
	Войтович О. П.	Дудатьєв А. В..	Майданевич Л. О.
Технічна здійсненність концепції	3	3	3
Ринкові переваги (наявність аналогів)	3	4	2
Ринкові переваги (ціна продукту)	3	4	3
Ринкові переваги (технічні властивості)	3	3	4
Ринкові переваги (експлуатаційні витрати)	3	4	3
Ринкові переваги (розмір ринку)	3	4	3
Ринкові переваги (конкуренція)	4	4	4
Практична здійсненність (наявність фахівців)	3	4	4
Практична здійсненність (наявність фінансів)	3	3	4
Практична здійсненність (необхідність нових матеріалів)	4	4	3
Практична здійсненність (термін реалізації)	4	4	4
Практична здійсненність (розробка документів)	4	4	4
Сума балів	40	45	41
Середньоарифметична сума балів, $СБ_с$	42		

Отже, за результатами аналізу (табл. 4.1) можна зробити висновок, що науково-технічний рівень та комерційний потенціал запропонованої розробки є високими. Такий показник було досягнуто завдяки значному підвищенню об’єктивності аудиту та перевагам ризик-орієнтованого аудиту.

Дослідження сучасних підходів до оцінювання ризиків та побудови ефективної системи аудиту відповідно до вимог Постанов НБУ, міжнародних стандартів [9, 10,11,15]. Особлива увага приділяється практичному аналізу даних журналів інцидентів, участі ризик-координаторів та застосуванню автоматизованих інструментів, таких як Power BI та системи, що дозволяє значно підвищити точність і об’єктивність оцінки ризиків, а також забезпечити відповідність принципам ризик-орієнтованого аудиту [34].

За результатами розрахунків, наведених в таблиці 4.1, зроблено висновок щодо науково-технічного рівня і рівня комерційного потенціалу розробки.

При цьому доцільно використати рекомендації, наведені в табл. 4.2.

Таблиця 4.2 – Науково-технічні рівні та комерційні потенціали розробки

Середньоарифметична сума балів СБ, розрахована на основі висновків експертів	Науково-технічний рівень та комерційний потенціал розробки
41…48	Високий
31…40	Вищий середнього
21…30	Середній
11…20	Нижчий середнього
0…10	Низький

Також доцільно провести аналіз рівня конкурентоспроможності запропонованої розробки.

Конкурентоспроможність визначається через сукупність якісних, технологічних та економічних показників, що характеризують безпечність та практичну цінність рішення у порівнянні з існуючими підходами.

Оцінювання рівня конкурентоспроможності науково-технічної розробки передбачає кілька послідовних етапів. У цьому випадку порівняльний аналіз буде здійснюватися відносно традиційних методів проведення аудитів.

Зокрема, порівняння проводитиметься зі стандартною моделлю аудиту інформаційної безпеки, що ґрунтується на підході аудиту на відповідність. Такий підхід передбачає перевірку дотримання встановлених політик, регламентів і вимог нормативних документів, зокрема стандартів ISO/IEC та Постанов НБУ. Хоча аудит на відповідність забезпечує контроль наявності необхідних процедур і документів, він не дає змоги повною мірою оцінити реальний рівень ризиків, не враховує змінність загрозового середовища та часто не дозволяє своєчасно ідентифікувати потенційні вразливості.

На відміну від таких рішень, запропонований метод ризик-орієнтованого аудиту передбачає глибший аналітичний підхід, який базується на оцінюванні ймовірності та впливу ризиків, аналізі журналів інцидентів, залученні ризик-координаторів та застосуванні автоматизованих інструментів, таких як Power BI і SIEM-системи. Це дозволяє здійснювати оперативну, об’єктивну та багатовимірну оцінку стану інформаційної безпеки, визначати пріоритети для

обробки ризиків, мінімізувати ймовірність інцидентів та забезпечувати значно вищий рівень ефективності порівняно з традиційним аудитом на відповідність.

4.1.1 Розрахунок одиничних параметритичних індексів

Якщо збільшення величини параметра свідчить про підвищення якості нової розробки, одиничний параметричний індекс розраховується за формулою:

$$q_i = \frac{P_i}{P_{базі}}, \tag{4.2}$$

де q_i – одиничний параметричний індекс, розрахований за i-м параметром;

P_i – значення i-го параметра розробки;

$P_{базі}$ – аналогічний параметр базової розробки-аналога, з якою проводиться порівняння.

Тобто для технічного показника, наприклад, продуктивності роботи, розрахунок буде такий:

$$q_1 = \frac{5}{4} = 1{,}25.$$

Для економічного показника розрахунок буде такий:

$$q_1 = \frac{5000}{7000} = 0{,}75.$$

Технічні та економічні параметри аналога та нової науково-технічної розробки доцільно подати у вигляді таблиці 4.3.

Таблиця 4.3 – Технічні та економічні параметри аналога нової науково-технічної розробки

Параметр	Одиниця виміру	Аналог	Нова розробка	Індекс зміни значення параметра	Коефіцієнт вагомості
Технічні					
Продуктивність	5-бальна шкала	3	5	1,67	0,25
Сумісність	5-бальна шкала	3	5	1,67	0,05
Функціональність	5-бальна шкала	4	5	1,25	0,05
Безпека	5-бальна шкала	3	5	1,67	0,25
Масштабованість	5-бальна шкала	3	5	1,67	0,40
Економічні					
Вартість інтеграції	грн	6000	7000	1,17	0,3
Вартість підтримки	грн	4000	5000	1,25	0,3
Час впровадження	години	12	8	0,67	0,4

Таким чином, можна перейти до розрахунку групових параметритичних індексів.

4.1.2 Розрахунок групових параметритичних індексів

Значення групового параметричного індексу за технічними параметрами визначається з урахуванням вагомості (частки) кожного параметра за формулою:

$$I_{\text{ТП}} = \sum_{i=1}^{n} q_i \cdot \alpha_i, \quad (4.3)$$

де $I_{\text{ТП}}$ – груповий параметричний індекс за технічними показниками (порівняно з аналогом);

q_i – одиничний параметричний показник i-го параметра;

α_i – вагомість i-го параметричного показника, $\sum_{i=1}^{n} \alpha_i = 1$;

n – кількість технічних параметрів, за якими оцінюється конкурентоспроможність.

Тобто розрахунок групового параметричного індексу за технічними параметрами матиме такий вигляд:

$$I_{\text{ТП}} = 1{,}67 \cdot 0{,}25 + 1{,}67 \cdot 0{,}05 + 1{,}25 \cdot 0{,}05 + 1{,}67 \cdot 0{,}25 + 1{,}67 \cdot 0{,}4 = 1{,}65$$

Груповий параметричний індекс за економічними параметрами (за ціною споживання) розраховується за формулою:

$$I_{\text{ЕП}} = \sum_{i=1}^{m} q_i \cdot \beta_i, \quad (4.4)$$

де $I_{\text{ЕП}}$ – груповий параметричний індекс за економічними показниками;

q_i – економічний параметр i-го виду;

β_i – частка i-го економічного параметра, $\sum_{i=1}^{m} \beta_i = 1$;

m – кількість економічних параметрів, за якими здійснюється оцінювання.

Тобто розрахунок групового параметричного індексу за економічними параметрами матиме вигляд:

$$I_{\text{ЕП}} = 0{,}857 \cdot 0{,}3 + 0{,}8 \cdot 0{,}3 + 1{,}5 \cdot 0{,}4 = 1{,}097$$

Далі варто перейти до розрахунку інтегрального показника.

4.1.3 Розрахунок інтегрального показника

На основі групових параметричних індексів за нормативними, технічними та економічними показниками розраховують інтегральний показник конкурентоспроможності за формулою:

$$K_{\text{ІНТ}} = I_{\text{НП}} \cdot \frac{I_{\text{ТП}}}{I_{\text{ЕП}}}, \tag{4.5}$$

$$K_{\text{ІНТ}} = 1 \cdot \frac{1{,}65}{1{,}10} = 1{,}50.$$

На основі інтегрального показника $K_{\text{ІНТ}} = 1{,}50$ можна стверджувати, що запропонований метод ризик-орієнтованого аудиту має високий рівень конкурентоспроможності порівняно з традиційним аудитом на відповідність та може бути успішно впроваджений у фінансово-кредитних установах. Таке значення показника пояснюється тим, що технічні характеристики ризик-орієнтованого аудиту (глибина аналізу, точність оцінки ризиків, оперативність та масштабованість) значно перевищують показники традиційного підходу, а економічні витрати на впровадження та підтримку залишаються оптимальними. Саме поєднання підвищеної ефективності технічних параметрів і економічної доцільності забезпечує конкурентну перевагу запропонованого методу аудиту та підтверджує його практичну цінність для організацій, що прагнуть до високого рівня інформаційної безпеки.

4.2 Розрахунок витрат на здійснення науково-дослідної роботи

Витрати на здійснення науково-дослідної роботи групуються за такими статтями:

– витрати на оплату праці;

– відрахування на соціальні заходи;

– матеріали;

– паливо та енергія для науково-виробничих цілей;

– витрати на службові відрядження;

– спецустаткування для наукових (експериментальних) робіт;

– програмне забезпечення для наукових (експериментальних) робіт;

– витрати на роботи, які виконують сторонні підприємства, установи і організації;

– інші витрати;

– накладні (загальновиробничі) витрати.

Варто розглянути кожну статтю окремо.

4.2.1 Витрати на оплату праці

Для початку, варто розрахувати основну заробітну плату дослідників. Для цього необхідно використати формулу:

$$З_о = \sum_{i=1}^{k} \frac{M_{ni} \cdot t_i}{T_p}, \quad (4.6)$$

де k – кількість посад дослідників, залучених до процесу досліджень;

M_{ni} – місячний посадовий оклад конкретного дослідника, грн;

t_i – кількість днів роботи конкретного дослідника, дн.;

T_p – середня кількість робочих днів в місяці, T_p = 22 дні.

Для зручності варто винести результати розрахунків у таблицю 4.4.

Таблиця 4.4 – Витрати на заробітну плату дослідників

Найменування посади	Місячний посадовий оклад, грн	Оплата за робочий день, грн	Кількість днів роботи	Витрати на заробітну плату, грн
Головний аудитор	50000	2273	12	27276
Аудитор ІБ	40000	1818	10	18180
Ризик координатор	35000	1591	17	27047
Всього				72 503

Основна заробітна плата робітників розраховується за формулою:

$$З_р = \sum_{i=1}^{n} C_i \cdot t_i, \quad (4.7)$$

де C_i – погодинна тарифна ставка робітника відповідного розряду, за виконану відповідну роботу, грн/год;

t_i – час роботи робітника при виконанні визначеної роботи, год.

Погодинну тарифну ставку робітника відповідного розряду C_i можна визначити за формулою:

$$C_i = \frac{M_M \cdot K_i \cdot K_c}{T_p \cdot t_{ЗМ}}, \quad (4.8)$$

де M_M – розмір прожиткового мінімуму працездатної особи або мінімальної місячної заробітної плати (залежно від діючого законодавства), грн – наразі ММ = 8000,00 грн;

K_i – коефіцієнт міжкваліфікаційного співвідношення для встановлення тарифної ставки робітнику відповідного розряду;

K_c – мінімальний коефіцієнт співвідношень місячних тарифних ставок робітників першого розряду з нормальними умовами праці виробничих об'єднань і підприємств до законодавчо встановленого розміру мінімальної заробітної плати.

T_p – середня кількість робочих днів в місяці, приблизно T_p = 22 дні;

$t_{ЗМ}$ – тривалість зміни, год.

$$C_i = \frac{8000 \cdot 1{,}1 \cdot 1{,}8}{22 \cdot 8} = 90 \text{ грн.}$$

$$З_р = 90 \cdot 14 = 1260 \text{ грн.}$$

Для зручності всі витрати варто винести в таблицю 4.5.

Таблиця 4.5 – Величина витрат на основну заробітну плату робітників

Найменування робіт	Тривалість роботи, год	Розряд роботи	Тарифний коефіцієнт	Погодинна тарифна ставка, грн	Величина оплати на робітника, грн
Дослідження існуючих методів аудиту	14	2	1,1	90	1 260
Розробка методики ризик-орієнтованого аудиту	25	7	2,2	180	4 500
Ідентифікація та класифікація ризиків	12	3	1,35	110	1 320
Аналіз журналів інцидентів та історичних даних	15	3	1,35	110	1 650
Побудова карти ризиків та моделей оцінки ризиків	20	6	2,0	163,63	3 272,6
Автоматизація збору та обробки даних	18	5	1,7	139,09	2 503,6
Тестування та перевірка моделі аудиту	16	3	1,35	110	1 760
Валідація та оптимізація процедури аудиту	12	6	2,0	163,63	1 963,56
Підготовка рекомендацій щодо впровадження	10	3	1,35	110	1 100
Проведення фінального звітування та презентацій	5	1	1,0	81,81	409,05
Всього					18 738

Додаткова заробітна плата робітників розраховується за формулою:

$$З_{дод} = (З_о + З_р) \cdot \frac{Н_{дод}}{100\%}, \quad (4.9)$$

де $Н_{дод}$ – норма нарахування додаткової заробітної плати.

Нехай це буде 11%.

$$З_{дод} = (72503 + 18738{,}81) \cdot \frac{11\%}{100\%} = 10036{,}60.$$

Наступним етапом доцільно перейти до наступної статті – відрахування на соціальні заходи.

4.2.2 Відрахування на соціальні заходи

До статті «Відрахування на соціальні заходи» належать відрахування внеску на загальнообов'язкове державне соціальне страхування та для здійснення заходів щодо соціального захисту населення (ЄСВ – єдиний соціальний внесок).

Нарахування на заробітну плату розраховується як 22% від суми основної та додаткової заробітної плати за формулою:

$$З_н = (З_о + З_р + З_{дод}) \cdot \frac{Н_{зп}}{100\%}, \quad (4.10)$$

де $Н_{зп}$ – норма нарахування на заробітну плату, тобто $Н_{зп}$ = 22%.

$$З_н = (72503 + 18738{,}81 + 10036{,}60) \cdot \frac{22\%}{100\%} = 22281{,}25.$$

Далі варто розрахувати вартість сировини та матеріалів.

4.2.3 Сировина та матеріали

Всі процеси відбуваються у електронному форматі, працівники мають власні інструменти для досліджень та розробки, та все ж є необхідність у записниках.

Витрати на матеріали у вартісному вираженні розраховуються окремо для кожного виду матеріалів за формулою:

$$M = \sum_{j-1}^{n} H_j \cdot Ц_j \cdot K_j - \sum_{j=1}^{n} B_j \cdot Ц_{вj}, \quad (4.11)$$

де H_j – норма витрат матеріалу j-го найменування, кг;

n – кількість видів матеріалів;

$Ц_j$– вартість матеріалу j-го найменування, грн/кг;

K_j– коефіцієнт транспортних витрат, (K_j= 1,1);

B_j – маса відходів j-го найменування, кг;

$Ц_{вj}$ – вартість відходів j-го найменування, грн/кг.

Результати всіх розрахунків зображено у таблиці 4.6.

Найменування матеріалу, марка, тип, сорт	Ціна за 1 шт., грн.	Норма витрат, шт	Величина відходів, шт	Ціна відходів, грн/шт	Вартість витраченого матеріалу, грн
Блокнот формату А5, Kite	54	4	0	0	237,6
Папір офісний формату А4	12	2000	0	0	26400
USB-накопичувач	300	3	0	0	990
Ручка кулькова, чорна, Kite	22	4	0	0	96,8
Всього					27724,4

Наступним етапом варто розрахувати витрати на комплектуючі та спецустаткування для наукових робіт.

4.2.4 Розрахунок витрат на комплектуючі та спецустаткування для наукових робіт

Витрати на комплектуючі та спецустаткування для наукових робіт не передбачені, оскільки у них немає потреби.

4.2.5 Програмне забезпечення для наукових (експериментальних) робіт

Балансова вартість програмного забезпечення розраховується за формулою:

$$В_{прг} = \sum_{i=1}^{k} Ц_{iпрг} \cdot C_{прг.i} \cdot K_j, \quad (4.12)$$

де $Ц_{iпрг}$ – ціна придбання одиниці програмного засобу цього виду, грн;

$C_{прг.i}$ – кількість одиниць програмного забезпечення відповідного найменування, які придбані для проведення досліджень, шт.;

K_j – коефіцієнт, що враховує інсталяцію, налагодження програмного засобу тощо, (Кі = 1,10);

k – кількість найменувань програмних засобів.

Отримані результати винесені у таблицю 4.7.

Таблиця 4.7 – Витрати на придбання програмних засобів по кожному виду

Найменування програмного засобу	Кількість, шт	Ціна за одиницю, грн	Вартість, грн
Power BI (Microsoft)	1	13 000 (Pro ліцензія/рік)	13 000
CaseWare IDEA	1	35 000 (річна ліцензія)	35 000
ACL Robotics (Diligent)	1	40 000 (річна ліцензія)	40 000
Tableau	1	15 000 (річна ліцензія)	15 000

Наступним етапом варто розрахувати витрати на амортизацію обладнання, програмних засобів та приміщень.

4.2.6 Амортизація обладнання, програмних засобів та приміщень

В спрощеному вигляді амортизаційні відрахування по кожному виду обладнання, приміщень та програмному забезпеченню тощо можуть бути розраховані з викням прямолінійного методу амортизації за формулою (4.13).

$$\text{А}_{\text{обл}} = \frac{\text{Ц}_\text{б}}{\text{Т}_\text{в}} \cdot \frac{t_{\text{вик}}}{12}, \tag{4.13}$$

Результати розрахунків варто винести в таблицю 4.8.

Таблиця 4.8 – Амортизаційні відрахування по кожному виду обладнання

Найменування обладнання	Кількість, шт	Балансова вартість, грн	Строк корисного використання, років	Термін використання обладнання, місяців	Амортизаційні відрахування, грн
Приміщення	1	120000	20	1	500,00
Ноутбук Asus	7	11000	2	1	1833,33
	Всього				2333,33

Отже, сума амортизації -2333,33 грн.

4.2.7 Палива та енергія для науково-виробничих цілей

$$\text{В}_e = \sum_{i=1}^{n} W_{yi} \cdot t_i \cdot \text{Ц}_e \cdot \frac{K_{\text{вэ}}}{\eta_i}, \tag{4.14}$$

де W_{yi} – встановлена потужність обладнання на певному етапі розробки, кВт;

t_i – тривалість роботи обладнання на етапі дослідження, год;

Ц$_e$ – вартість 1 кВт-години електроенергії, грн, Ц$_e$ = 10,5 грн;

$K_{вэ}$ – коефіцієнт, що враховує використання потужності, $K_{вэ} < 1$, $K_{вэ} = 0{,}38$;

η_i – коефіцієнт корисної дії обладнання, $\eta_i < 1$, $\eta_i = 0{,}9$.

Результати проведених розрахунків занесено до таблиці 4.9.

Найменування обладнання	Встановлена потужність, кВт	Тривалість роботи, год	Сума, грн
Ноутбук Asus №1	0,025	40	10,28
Ноутбук Asus №2	0,04	56	23,03
Ноутбук Asus №3	0,045	120	55,52
Ноутбук Asus №4	0,050	40	20,56
Ноутбук Asus №5	0,025	30	7,71
Ноутбук Asus №6	0,025	20	5,14
Ноутбук Asus №7	0,04	26	10,69
Всього			132,93

Отже, загальна вартість становить 132,93 грн.

4.2.8 Службові відрядження

У службових відрядженнях немає потреби, тому кошти на них також не виділяються.

4.2.9 Витрати на роботи, які виконують сторонні підприємства, установи та організації

Зазначені витрати не передбачені.

4.2.10 Інші витрати

До статті «Інші витрати» належать витрати, які не знайшли відображення у зазначених статтях витрат і можуть бути віднесені безпосередньо на собівартість досліджень за прямими ознаками.

Витрати за статтею «Інші витрати» розраховуються як 50…100% від суми основної заробітної плати дослідників та робітників за формулою:

$$I_в = (З_о + З_р) \cdot \frac{H_{ів}}{100\%}, \quad (4.15)$$

$$I_в = (27724{,}4 + 29598{,}06) \cdot \frac{50\%}{100\%} = 28661{,}23.$$

Отже, інші витрати становлять 28661,23 грн.

4.2.11 Накладні (загальновиробничі витрати)

Витрати за статтею «Накладні (загальновиробничі) витрати» розраховуються як 100% від суми основної заробітної плати дослідників та робітників за формулою:

$$В_{нзв} = (З_о + З_р) \cdot \frac{Н_{зв}}{100\%}, \quad (4.16)$$

де $Н_{зв}$ – норма нарахування за статтею «Накладні (загальновиробничі) витрати».

$$В_{нзв} = (27724{,}4 + 29598{,}06) \cdot \frac{100\%}{100\%} = 57322{,}46.$$

Витрати на проведення науково-дослідної роботи розраховуються як сума всіх попередніх статей витрат за формулою:

$$В_{заг} = З_о + З_р + З_{дод} + З_н + М + К_в + В_{спец} + В_{прг} + А_{обл} + В_е + В_{св} + В_{сп} + І_в + В_{нзв}, \quad (4.17)$$

$$В_{заг} = 48936{,}23 + 27724{,}4 + 29598{,}06 + 8638{,}77 + 1890{,}00 + 2333{,}33 + 132{,}93 + 0{,}00 + 0{,}00 + 28661{,}23 + 57322{,}46 = 205237{,}41.$$

Загальні витрати ЗВ на завершення науково-дослідної (науково-технічної) роботи та оформлення її результатів розраховується за формулою:

$$ЗВ = \frac{В_{заг}}{\eta}, \quad (4.18)$$

де η – коефіцієнт, який характеризує етап (стадію) виконання науково-дослідної роботи. Оскільки наукова робота знаходиться на стадії розробки промислового зразка, то $\eta = 0{,}7$.

$$ЗВ = \frac{205237,41}{0,7} = 293196,3$$

Отже, загальновиробничі витрати становлять 293196,3 грн.

4.3 Розрахунок економічної ефективності науково-технічної розробки від її впровадження безспосередньо замовником

У цій магістерській роботі розроблено спеціалізовану методику та набір процедур для ризик-орієнтованого аудиту інформаційної безпеки, що може бути впроваджено у внутрішню аудиторську практику фінансово-кредитних установ. Можливе **покращення фінансових та операційних показників установи** у кожному з років, протягом яких очікується отримання ефекту від впровадження методу аудиту, розраховується за формулою:

$$\Delta П_i = (\pm \Delta П_я \cdot N + П_я \cdot \Delta N_i), \quad (4.19)$$

де $\Delta П_я$ – покращення основного якісного показника від впровадження на підприємстві результатів науково-технічної розробки в аналізованому році;

N – основний кількісний показник, який визначає обсяг діяльності підприємства у році до впровадження результатів нової науково-технічної розробки;

$П_я$ – основний якісний показник, який визначає результати діяльності підприємства у кожному із років після впровадження науково-технічної розробки;

ΔN – зміна основного кількісного показника діяльності підприємства в результаті впровадження науково-технічної розробки в аналізованому році.

$$\Delta П_1 = 0,2 \cdot 800 + 2,5 \cdot 50 = 285 \text{ тис. грн.}$$

$$\Delta П_2 = \Delta П_3 = \Delta П_4 = \Delta П_5 = 0,12 \cdot 800 + 2,5 \cdot 50 = 223,4 \text{ тис. грн.}$$

Далі потрібно розрахувати приведену вартість збільшення всіх чистих прибутків ПП, що їх може отримати замовник від можливого впровадження

науково-технічної розробки на власному підприємстві. Розрахунок відбувається за формулою:

$$ПП = \sum_{i=1}^{T} \frac{\Delta П_i}{(1+\tau)^t}, \quad (4.20)$$

де $\Delta П_i$ – збільшення чистого прибутку у кожному з років, протягом яких виявляються результати впровадження науково-технічної розробки, грн;

T – період часу, протягом якого очікується отримання позитивних результатів від впровадження науково-технічної розробки, роки;

τ – ставка дисконтування, за яку можна взяти щорічний прогнозований рівень інфляції в країні, $\tau = 0{,}1$;

t – період часу (в роках) від моменту початку впровадження науковотехнічної розробки до моменту отримання підприємством збільшеної величини чистого прибутку в аналізованому році.

$$ПП = \frac{285}{(1+0{,}1)^1} + \frac{223{,}4}{(1+0{,}1)^2} + \frac{223{,}4}{(1+0{,}1)^3} + \frac{223{,}4}{(1+0{,}1)^4} + \frac{223{,}4}{(1+0{,}1)^5} = 902{,}83 \text{ тис. грн.}$$

Далі потрібно розрахувати величину початкових інвестицій PV, які замовник має вкласти для здійснення науково-технічної розробки. Для цього можна використати формулу:

$$PV = k_{\text{розр}} \cdot ЗВ, \quad (4.21)$$

де розр k – коефіцієнт, що враховує витрати розробника (замовника) на впровадження науково-технічної розробки. Це можуть бути витрати на підготовку приміщень, розробку технологій, навчання персоналу, маркетингові заходи тощо; зазвичай $k_{\text{розр}} = 2 \ldots 5$, але може бути і більшим. У випадку даного дослідження та розробки $k_{\text{розр}} = 2$;

ЗВ – загальні витрати на проведення науково-технічної розробки та оформлення її результатів, грн.

$PV = 2 \cdot 226559{,}66 \approx 453119{,}32$ грн.

Абсолютний економічний ефект $E_{\text{абс}}$ або чистий приведений дохід (NPV, Net Present Value) для розробника (замовника) від можливого впровадження науково-технічної розробки можна розрахувати за формулою:

$$E_{\text{абс}} = \text{ПП} - PV, \tag{4.22}$$

де ПП – приведена вартість збільшення всіх чистих прибутків від можливого впровадження науково-технічної розробки, грн;

PV – теперішня вартість початкових інвестицій, грн.

$E_{\text{абс}} = 902{,}83 - 453{,}12 \approx 449{,}71$ тис. грн.

Для остаточного прийняття рішення необхідно розрахувати внутрішню економічну дохідність $E_{\text{в}}$ або показник внутрішньої норми дохідності (IRR, Internal Rate of Return) вкладених замовником коштів. Внутрішня економічна дохідність інвестицій $E_{\text{в}}$, які можуть бути вкладені замовником у впровадження науково-технічної розробки, розраховується за формулою:

$$E_{\text{в}} = \sqrt[\text{Т}_{\text{ж}}]{1 + \frac{E_{\text{абс}}}{PV}} - 1, \tag{4.23}$$

де $E_{\text{абс}}$ – абсолютний економічний ефект вкладених інвестицій, грн;

PV – теперішня вартість початкових інвестицій, грн;

$\text{Т}_{\text{ж}}$ – життєвий цикл науково-технічної розробки, тобто час від початку її розробки до закінчення отримування позитивних результатів від її впровадження, роки.

$$E_{\text{в}} = \sqrt[1]{1 + \frac{449{,}711}{453{,}122}} - 1 = 0{,}411.$$

Далі розраховується період окупності інвестицій $T_{\text{ок}}$ (DPP, Discounted Payback Period), які можуть бути вкладені розробником (замовником) у

впровадження та комерціалізацію науково-технічної розробки. Розрахунок відбувається за формулою:

$$T_{\text{ок}} = \frac{1}{E_{\text{в}}}, \tag{4.24}$$

де $E_{\text{в}}$ – внутрішня економічна дохідність вкладених інвестицій.

$$T_{\text{ок}} = \frac{1}{0{,}411} = 2{,}43.$$

Оскільки $T_{\text{ок}} < 3$ років, можна зробити висновок, що впровадження науково-технічної розробки замовником є економічно ефективним.

4.4 Висновки до четвертого розділу

Отже, для повного дослідження економічної ефективності було проведено оцінювання науково-методичного рівня та комерційного потенціалу ризик-орієнтованого аудиту трьома експертами за визначеними критеріями. Результат розрахунку середнього балу становить 42, що свідчить про високий рівень науково-методичної цінності та практичної значущості методу.

Також було проведено аналіз конкурентоспроможності запропонованого підходу. Груповий параметричний індекс за технічними показниками склав 1,16, за економічними – 0,785, інтегральний показник конкурентоспроможності – 1,50, що підтверджує переваги технічних характеристик та економічної ефективності методу. Проведений аналіз показав, що метод є конкурентоспроможним і може бути успішно інтегрований у внутрішню систему аудиту фінансово-кредитних установ.

Крім того, проведено розрахунок витрат на здійснення робіт з розробки та впровадження ризик-орієнтованого аудиту загальні витрати на впровадження: 226 560 грн (зарплата, ПЗ, додаткові витрати);

Ці розрахунки показали, що впровадження методу є економічно доцільним, забезпечує підвищення ефективності аудиторської діяльності та оптимізацію ресурсів фінансово-кредитної установи.

ВИСНОВКИ

У рамках магістерської роботи проведено комплексне дослідження процесу аудиту інформаційної безпеки у фінансово-кредитних установах, проаналізовано відомі нормативні акти, зокрема постанови Національного банку України, та міжнародні стандарти ISO/IEC 27001, COBIT і NIST, результати аналізу показали необхідність удосконалення існуючих методів і методик аудиту, оскільки традиційні підходи, що базуються на формальних чек-листах і ручному зборі даних, обмежують об’єктивність оцінки ризиків та точність аудиторських висновків.

Удосконалено метод ризик-орієнтованого аудиту шляхом впровадження ролі ризик-координатора, формування динамічної карти ризиків на основі фактичних даних про інциденти та тестування контролів, а також інтеграції сучасних інструментів автоматизації, що дозволило структурувати інформацію про бізнес-процеси, підвищити об’єктивність оцінки ризиків і точність рекомендацій, а також скоротити час на підготовчий етап і комунікацію з підрозділами. Результати практичного впровадження показали, що застосування ризик-орієнтованого аудиту дозволяє скоротити витрати часу на підготовку та планування аудиту на 20–30%, підвищити релевантність карти ризиків до 75–80% та поліпшити ефективність взаємодії між аудиторами і службою інформаційної безпеки, а інтеграція технічних інструментів і процедур тестування контролів забезпечує більшу достовірність аудиторських висновків і зменшує ризик суб’єктивності.

Крім того, у роботі обґрунтовано економічну доцільність запропонованого методу шляхом оцінювання його науково-методичного рівня, комерційного потенціалу та конкурентоспроможності. Результати експертного оцінювання підтвердили високий рівень наукової та практичної значущості ризик-орієнтованого аудиту, а розраховані показники конкурентоспроможності засвідчили переваги технічних характеристик і економічної ефективності запропонованого підходу. Проведений розрахунок витрат на розробку та

впровадження методу показав, що його використання є економічно обґрунтованим і доцільним для фінансово-кредитних установ, оскільки забезпечує оптимізацію ресурсів, підвищення ефективності аудиторської діяльності та можливість практичного впровадження у внутрішні системи контролю інформаційної безпеки.

Отже, розроблений та впроваджений метод ризик-орієнтованого аудиту інформаційної безпеки дозволяє підвищити ефективність аудиторських процедур, концентрувати ресурси на найбільш критичних процесах і активах та зміцнює кіберстійкість фінансово-кредитних установ.

СПИСОВ ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Кривов’язюк М., Войтович, О. (2025) Особливості банківської інфраструктури в Україні та стандарти аудиту. Матеріали LIV Всеукраїнської науково-технічної конференції підрозділів ВНТУ, Вінниця, 24-27 березня 2025 р. URL: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2025/paper/view/23704

2 Кривов’язюк М., Войтович, О. (2025) Підхід ризик-орієнтованого аудиту інформаційної безпеки. Матеріали LV Всеукраїнська науково-технічна конференція факультету інформаційних технологій та комп'ютерної інженерії https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2026/paper/view/26572/22057

3 Войтович, О., Волинець, В. (2025). Особливості законодавства щодо аудиту кібербезпеки в різних регіонах світу. Measuring and Computing Devices in Technological Processes, (3), 23–29. https://doi.org/10.31891/2219-9365-2025-83

4 Національний банк України. Постанова № 4 від 16.01.2021 “Про затвердження порядку проведення інспекційних перевірок у сфері інформаційної кібербезпеки банків”.

5 Національний банк України. Постанова № 43 від 19.05.2021 “Про затвердження Положення про захист інформації в платіжних системах”.

6 Національний банк України. Постанова № 95 від 28.09.2020 “Про організацію заходів із забезпечення інформаційної безпеки в банках України”

7 TZI. Аудит безпеки інформаційних систем. URL: https://tzi.com.ua/audbezib.html

8 IBM. (2024). X-Force Threat Intelligence Index 2024. URL: https://www.ibm.com/reports/threat-intelligence

9 National Institute of Standards and Technology. (2012). Guide for Conducting Risk Assessments (NIST SP 800-30 Rev. 1). URL: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

10 COBIT 2019. Framework for Governance and Management of Enterprise IT. ISACA. URL: https://www.isaca.org/resources/cobit

11 Orna. (2023). NIST, ISO, COBIT, ITIL: Which Cyber Framework Rules Them All. URL: https://www.orna.app/post/nist-iso-cobit-itil-which-cyber-framework-rules-them-all

12 National Institute of Standards and Technology. (2020). Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53 Rev. 5). URL: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

13 National Institute of Standards and Technology. (2006). Guide to Computer Security Log Management (NIST SP 800-92). URL: https://csrc.nist.gov/publications/detail/sp/800-92/final

14 PCI DSS v3.2.1 - Payment Card Industry Data Security Standard.

15 KR-Labs. Аудит інформаційної безпеки. URL: https://kr-labs.com.ua/service/cybersecurity/audyt-informatsijnoyi-bezpeky/

16 ISO/IEC 27001:2013 - Information technology – Security techniques – Information security management systems – Requirements.

17 ISO/IEC 27005:2018 - Information technology – Security techniques – Information security risk management.

18 OWASP. (2023). Web Security Testing Guide. URL: https://owasp.org/www-project-web-security-testing-guide/

19 Capability Maturity Model Integration (CMMI). URL: https://cmmiinstitute.com/cmmi

20 Power BI (аналітична платформа бізнес-інтелекту) (електронний ресурс). URL: https://www.microsoft.com/ua-ua/power-platform/products/power-bi?market=ua

21 CaseWare International Inc. (2025). IDEA Audit Software. URL: https://www.caseware.com/products/idea/ (дата звернення: ..2025).

22 ACL Robotics (платформа автоматизації та безперервного аудиту) (електронний ресурс). URL: https://help.highbond.comTableau https://www.tableau.com/

23 Tableau Analytics Platform (платформа візуалізації та аналітики даних) (електронний ресурс). URL: https://www.tableau.com

24 ISACA. (2025). The Role of Digital Transformation Audits-Transform While Upholding Governance Standards. URL: https://www.isaca.org/resources/news-and-trends/industry-news/2025/the-role-of-digital-transformation-audits-transform-while-upholding-governance-standards

25 Xin, J., Du, K., & Xia, Y. (2024). The Impact of Enterprise Digital Transformation on Audit Fees-An Intermediary Role Based on Information Asymmetry. *Sustainability*, 16(22), 9970. URL: https://www.mdpi.com/2071-1050/16/22/9970

26 Benbouzid, D., Plociennik, C., Lucaj, L., Maftei, M., Merget, I., Burchardt, A., Hauer, M. P., Naceri, A., & van der Smagt, P. (2024). Pragmatic auditing: a pilot-driven approach for auditing Machine Learning systems. *arXiv preprint.* URL: https://arxiv.org/abs/2405.13191

27 Al Frijat, Y. S., & Al-Hajaia, E. M. (2025). Auditor's technical, digital, and creativity skills and their role in supporting audit outcomes in light of digital transformation strategy. *Corporate Board: Role, Duties and Composition*, 21(1), 60–70. URL: https://virtusinterpress.org/IMG/pdf/cbv21i1art6.pdf

28 Xiaoxiao Wang, Huimin Dong. (2025). Audit informatization, digital economy development, and corporate risk costs. *Finance Research Letters*, 83, 107679. ISSN 1544-6123. https://doi.org/10.1016/j.frl.2025.107679

29 Microsoft Corporation. (2025). Power BI Desktop. URL: https://www.microsoft.com/ru-ru/power-platform/products/power-bi/desktop (дата звернення: ..2025).

30 Войтович, О. П., Пилявець, І. Ю., Радченко, Є. В. (2025). Використання штучного інтелекту в аудиті інформаційної безпеки. Матеріали науково-практичної інтернет-конференції «Молодь в науці: дослідження, проблеми, перспективи»,https://conferences.vntu.edu.ua/index.php/mn/mn2025/paper/view

31 Diligent / HighBond. (2025). Getting Started with Robotics Tutorial. URL: https://help.highbond.com/helpdocs/highbond/enus/Content/get_started/tutorials/getting_started_with_robotics.htm (дата звернення: ..2025).

32 Tableau Software. (2025). Tableau – Business Intelligence & Analytics. URL: https://www.tableau.com/ (дата звернення: ..2025).

33 ЛІГА:ЗАКОН. (2024). Законодавчі акти у сфері інформаційної безпеки. URL: https://ips.ligazakon.net/document/FZ002245

34 Козловський В. О. , Лесько О. Й., Кавецький В. В.Методичні вказівки до виконання економічної частини магістерських кваліфікаційних робіт. Вінниця . ВНТУ. 2021. 42 с.

ДОДАТКИ

99

Додаток А. **ПРОТОКОЛ ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ**

Назва роботи: Метод ризик-орієнтованого аудиту інформаційної безпеки у фінансово-кредитних установах

Автор роботи: Кривов'язюк Максим Юрійович
Тип роботи: магістерська кваліфікаційна робота
Підрозділ кафедра захисту інформації ФІТКІ , група 1 БС-24м

Коефіцієнт подібності текстових запозичень, виявлених у роботі системою StrikePlagiarism **2.34** %

Висновок щодо перевірки кваліфікаційної роботи (відмітити потрібне)

√ Запозичення, виявлені у роботі, є законними і не містять ознак плагіату, фабрикації, фальсифікації. Роботу прийняти до захисту

☐ У роботі не виявлено ознак плагіату, фабрикації, фальсифікації, але надмірна кількість текстових запозичень та/або наявність типових розрахунків не дозволяють прийняти рішення про оригінальність та самостійність її виконання. Роботу направити на доопрацювання.

☐ У роботі виявлено ознаки плагіату та/або текстових маніпуляцій як спроб укриття плагіату, фабрикації, фальсифікації, що суперечить вимогам законодавства та нормам академічної доброчесності. Робота до захисту не приймається.

Експертна комісія:

В. о. зав. кафедри ЗІ д. т. н., проф. Володимир ЛУЖЕЦЬКИЙ
Гарант освітньої програми «Безпека інформаційних і комунікаційних систем» к.т.н., доцент Олеся ВОЙТОВИЧ

Особа, відповідальна за перевірку Валентина КАПЛУН

З висновком експертної комісії ознайомлений(-на)

Керівник Олеся ВОЙТОВИЧ
Здобувач Максим КРИВОВ'ЯЗЮК

Додаток Б

Приклад листа про початок перевірки

БАНК «ФІНАНС ТРЕЙД»
СЛУЖБОВИЙ ЛИСТ
№ 24/ІБ-112 від 14.10.2025 р.

Кому:
Керівникам структурних підрозділів
(ІТ-департамент, департамент електронних платежів, служба інформаційної безпеки, операційний департамент)

Від:
Відділу внутрішнього аудиту інформаційної безпеки

Тема: Проведення планового аудиту інформаційної безпеки

Шановні колеги,

На виконання внутрішнього плану контролю за станом інформаційної безпеки та відповідно до затвердженої **карти ризиків**, повідомляємо про початок проведення **планового аудиту інформаційної безпеки** у структурних підрозділах банку.

Мета аудиту: оцінка ефективності реалізованих заходів захисту інформації, перевірка відповідності внутрішніх процесів вимогам Постанов НБУ №95, №4, №43 та міжнародним стандартам ISO/IEC 27001, NIST, COBIT.

Період проведення аудиту: з **21 жовтня по 1 листопада 2025 року**.

Об'єкти перевірки:

- Системи управління доступом і привілеями користувачів;
- Логи подій безпеки та журнали адміністрування;
- Процеси реагування на інциденти;
- Захист мережевої інфраструктури та платіжних сервісів;
- Виконання політик резервного копіювання та оновлення систем.

Методи збору інформації:

- Аналіз документації та технічних журналів;
- Проведення інтерв'ю з відповідальними особами;
- Тестування конфігурацій і контрольних механізмів;
- Огляд внутрішніх процедур та рівня відповідності нормативам.

Просимо забезпечити надання необхідних матеріалів, доступів і супровід відповідальних працівників під час аудиторських перевірок.

Результати аудиту будуть узагальнені у звіті, який подається на розгляд Комітету з інформаційної безпеки.

З повагою,

_____
(П.І.Б.)
Керівник відділу внутрішнього аудиту ІБ
Банк «Фінанс Трейд»

101

ІЛЮСТРАТИВНА ЧАСТИНА

МЕТОД РИЗИК-ОРІЄНТОВАНОГО АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ФІНАНСОВО-КРЕДИТНИХ УСТАНОВАХ

Виконав: студент 2 курсу групи 1БС-24 м спеціальності 125 Кібербезпека та захист інформації

_____Максим КРИВОВ'ЯЗЮК

Керівник: к. т. н., доц., доцент каф. ЗІ

_____Олеся ВОЙТОВИЧ

«19» грудня 2025 р.

.

Порівняльний аналіз нормативно-правових актів

Номер	Ключові вимоги та положення	Мета документа	Відповідність міжнародним стандартам
№95	Обов'язковість створення Системи управління інформаційною безпекою (СУІБ). Призначення відповідальної особи за ІБ на рівні керівництва. -Регулярне проведення аудиту ІБ. -Управління ризиками та інцидентами безпеки. - Розроблення політик і процедур ІБ.	Створення єдиної методологічної бази для побудови систем ІБ у банках України.	Відповідає ISO/IEC 27001, ISO/IEC 27005 (управління ризиками).
№4	- Розширення повноважень НБУ щодо контролю кібербезпеки. - Право інспекторів НБУ на доступ до ІТ-систем банку. - Встановлення обов'язку повідомляти про кіберінциденти у визначені терміни. - Запровадження санкцій за невиконання вимог.	Посилення відповідальності банків за стан кіберзахищеності; підвищення ефективності державного нагляду.	Узгоджується з принципами NIST Cybersecurity Framework та практиками COBIT (контроль і управління ІТ).
№43	- Регулювання ІБ та кіберзахисту платіжної інфраструктури. - Вимога відповідності стандартам PCI DSS. - Управління каскадними ризиками у платіжних системах. - Контроль за безпекою даних платіжних карток.	Захист критично важливої платіжної інфраструктури від кіберзагроз; інтеграція у глобальну систему безпеки.	Відповідає PCI DSS, частково - ISO/IEC 27032 (кібербезпека).

Схема проведення аудиту відповіднно до чиного законодавства

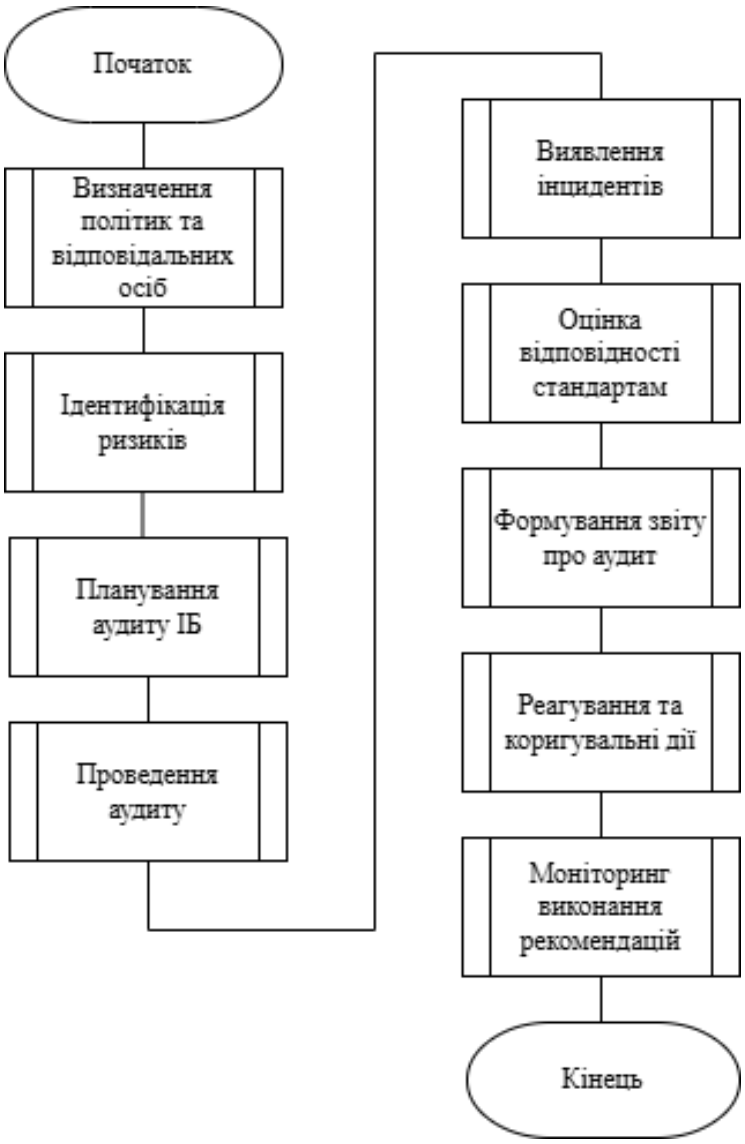


Схема проведення аудиту відповіднно до міжнародних стандартів

Схема взаємодії аудиторів та ризик-координаторів

Схема автоматизації аудиту

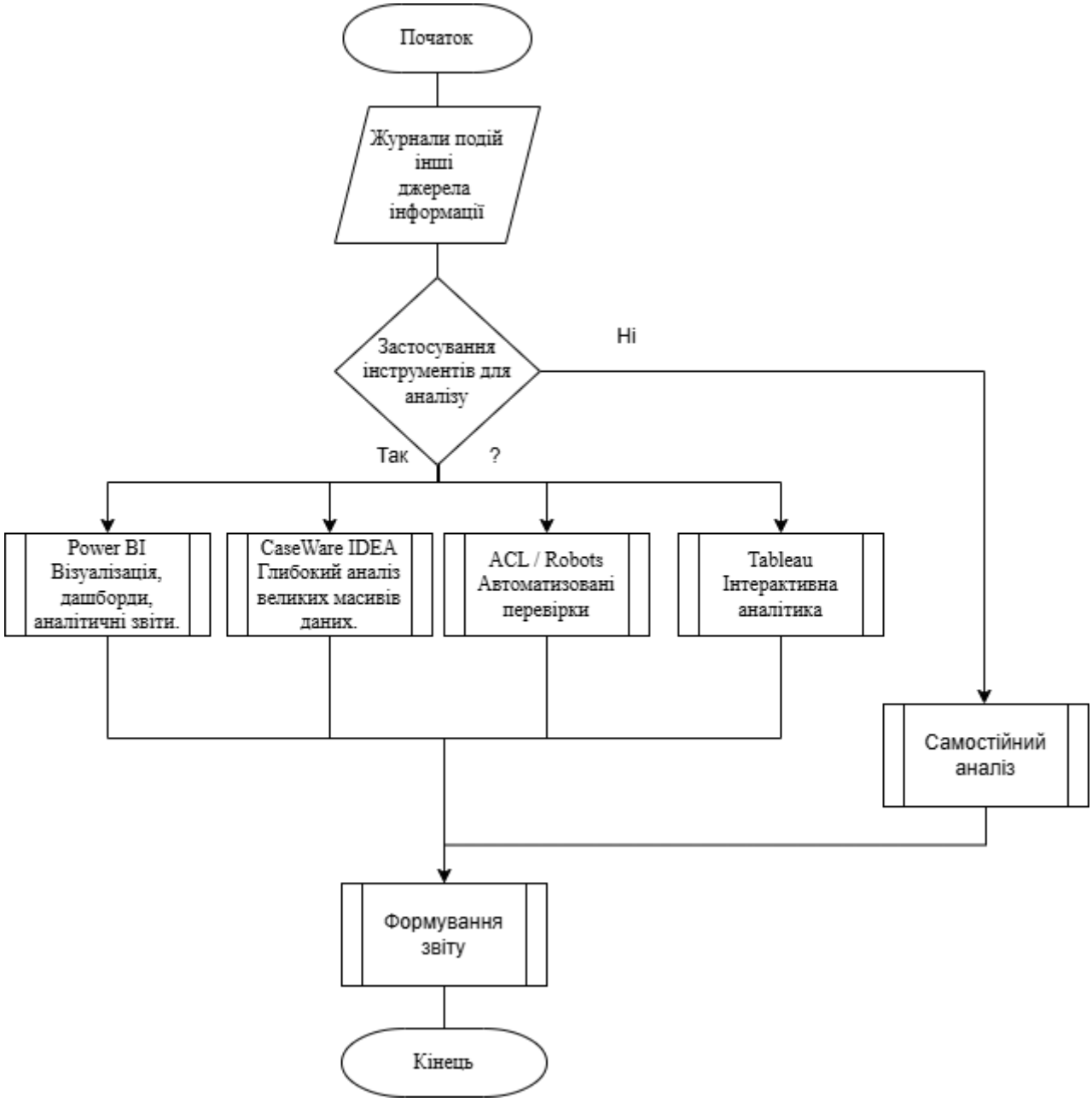
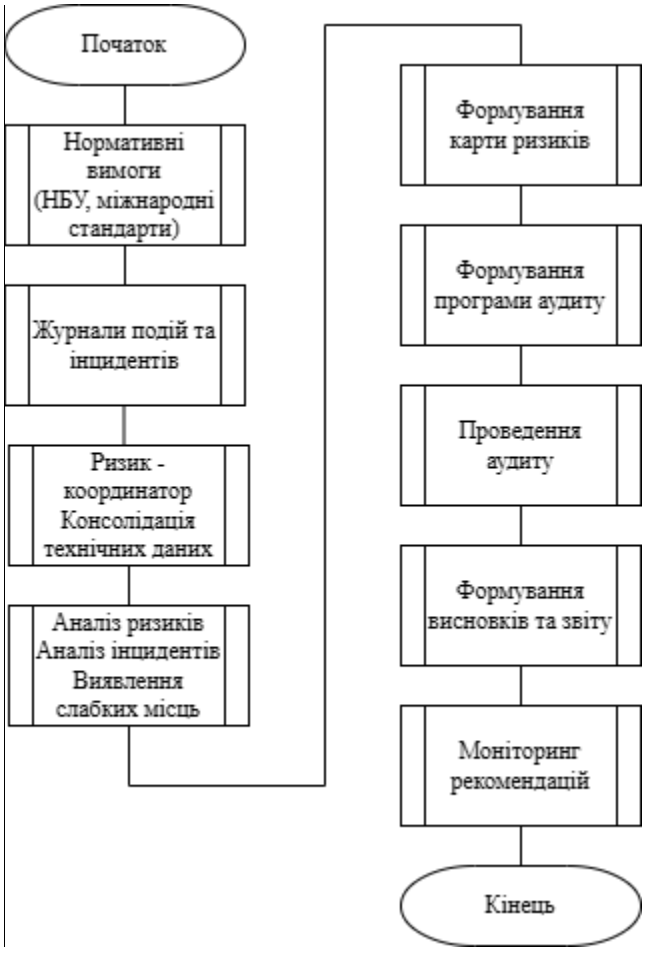


Схема методу ризик-орієнтованого аудиту



Результати порівняння процесу оцінки ризиків

Параметр	До впровадження	Після впровадження ризик-орієнтованого методу
Основа формування карти ризиків	Чек-листи, стандарти, нормативні вимоги; статична інформація	Реальні технічні дані: журнали подій, SIEM, конфігурації контролів; більш актуальна інформація (~85–90%)
Пріоритизація аудиту	За формальними критеріями, орієнтація на нормативні вимоги	Аналіз слабких місць систем, частоти інцидентів та значущості процесів; час планування скоротився на ~30%
Джерела даних	Запити до власників процесів; ризик неповних або неправдивих даних	«Сирі» технічні дані; ризик помилкових даних зменшився на 70–80%
Об’єктивність оцінки	Високий рівень суб’єктивності, залежність від пояснень власників процесів	Зросла на 20–30% завдяки перевіркам фактів та участі ризик-координатора
Роль ризик-координатора	Відсутній	Забезпечує доступ до даних, пояснює архітектуру систем, допомагає у тлумаченні даних та коректному формуванні висновків
Практичне підтвердження ризиків	Не здійснювалося; аудитори спиралися на документи та відповіді	Перевірка через аналіз логів, тестування контролів, вибірки з баз даних
Гнучкість аудиту	Низька; обмежена лише чек-листами	Вища; дозволяє реагувати на актуальні ризики та формувати релевантну програму аудиту
Ризик суб’єктивності та помилок	Високий	Значно знижений, рекомендації стали точними, конкретними та прив’язаними до фактичного стану систем

Показники економічної ефективності ризик-орієнтованого аудиту інформаційної безпеки

№	Показник	Значення
1	Кількість експертів	3
2	Середній експертний бал	42
3	Груповий параметричний індекс (технічні показники)	1,16
4	Груповий параметричний індекс (економічні показники)	0,785
5	Інтегральний показник конкурентоспроможності	1,50
6	Загальні витрати на впровадження	226 560 грн
7	Економічна доцільність впровадження	Доцільне
8	Потенціал інтеграції	Високий