

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

**Навчально-науковий інститут
«Інститут інформаційних технологій в економіці»**

Кафедра системного аналізу та кібербезпеки

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «КІБЕРБЕЗПЕКА»

Галузь знань 12 «Інформаційні технології»

Спеціальність 125 «Кібербезпека»

Форма навчання: очна (денна)
очна (денна), заочна, дистанційна

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

на тему: **«Оцінка кіберризиків у роботі фінансового департаменту
ТОВ «Спектр-Агро»**

здобувача Тригуба Євгенія Вячеславовича
(прізвище, ім'я, по батькові)

Науковий керівник к.е.н. Труш М.С.
(науковий ступінь, учене звання, ПІБ)

(підпис)

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

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

(підпис)

Київ 2026

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

**Навчально-науковий інститут «Інститут інформаційних технологій в економіці»
Кафедра системного аналізу та кібербезпеки**

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «КІБЕРБЕЗПЕКА»

СПЕЦІАЛЬНІСТЬ 125 «КІБЕРБЕЗПЕКА»

ПОГОДЖЕНО

Керівник проєктної групи (гарант)
освітньо-професійної програми

ЗАТВЕРДЖУЮ

Завідувач кафедри

Бегун А.В.

(підпис)

Джалладова І.А.

(підпис)

2026р.

2026р.

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

здобувачу вищої освіти Тригубу Євгенію Вячеславовичу
(прізвище, ім'я, по батькові)

очної (денної)

форми навчання

очної (денної), заочної, дистанційної

на підготовку кваліфікаційної бакалаврської роботи
на тему **«Оцінка кіберризиків у роботі фінансового департаменту
ТОВ «Спектр-Агро»»**

Тему затверджено наказом ректора Університету від «_____» _____ 20__р. № _____

Кваліфікаційна бакалаврська робота виконується на матеріалах

ТОВ «СПЕКТР-АГРО»

План кваліфікаційної бакалаврської роботи

Розділ 1	ТЕОРЕТИКО-МЕТОДИЧНІ ОСНОВИ ОЦІНЮВАННЯ КІБЕРРИЗИКІВ У ФІНАНСОВІЙ ДІЯЛЬНОСТІ ПІДПРИЄМСТВА (назва розділу)
Розділ 2	АНАЛІТИКО-ДОСЛІДНИЦЬКА ДІАГНОСТИКА КІБЕРРИЗИКІВ У РОБОТІ ФІНАНСОВОГО ДЕПАРТАМЕНТУ ТОВ «СПЕКТР-АГРО» (назва розділу)
Розділ 3	КОНСТРУКТИВНІ ШЛЯХИ ПІДВИЩЕННЯ КІБЕРБЕЗПЕКИ ФІНАНСОВОГО ДЕПАРТАМЕНТУ ТОВ «СПЕКТР-АГРО» (назва розділу)
Об'єкт дослідження:	фінансові процеси підприємства як джерела кіберризиків.
Предмет дослідження:	методи та моделі оцінювання кіберризиків на підприємстві.
Мета кваліфікаційної бакалаврської роботи:	оцінювання кіберризиків у фінансовій діяльності підприємства (на прикладі фінансового департаменту ТОВ «Спектр-Агро») та визначення конструктивних шляхів підвищення рівня кібербезпеки.

Розділ 1

- розкрити сутність, класифікацію та сучасні підходи до розуміння кіберризиків у фінансових процесах;
- сформувати теоретичні засади систем управління кіберризиками та охарактеризувати міжнародні стандарти їх оцінювання;
- проаналізувати методичні підходи та моделі оцінювання кіберризиків, придатні для застосування у фінансових департаментах підприємств.

Розділ 2

- охарактеризувати діяльність ТОВ «Спектр-Агро» та структуру фінансового департаменту як об'єкта дослідження;
- проаналізувати поточний стан кіберзагроз і вразливостей фінансових процесів підприємства за останні два роки;
- застосувати методики оцінювання кіберризиків на фактичних даних ТОВ «Спектр-Агро» та отримати результати практичного аналізу.

Розділ 3

- обґрунтувати стратегічні напрями удосконалення системи управління кіберризиками підприємства;
- розробити комплекс організаційних та технічних заходів щодо мінімізації кіберризиків фінансового департаменту;
- оцінити ефективність запропонованих рішень та спрогнозувати їх вплив на рівень кіберзахищеності підприємства.

Завдання підготував

Науковий керівник

(підпис)

Труш М. С.

(ініціали, прізвище)

Завдання одержав

здобувач

(підпис)

Тригуб Є.В.

(ініціали, прізвище)

«_____» _____ 2026р.

РЕФЕРАТ

Кваліфікаційна бакалаврська робота містить 102 сторінки, 12 таблиць, 3 рисунка, список використаних джерел з 53 найменувань.

«Оцінка кіберризиків у роботі фінансового департаменту підприємства

ТОВ «Спектр-Агро»

(назва кваліфікаційної бакалаврської роботи)

Об'єктом дослідження є фінансові процеси підприємства як джерела кіберризиків.

Предмет дослідження є методи та моделі оцінювання кіберризиків на підприємстві.

Мета кваліфікаційної роботи - оцінювання кіберризиків у фінансовій діяльності підприємства (на прикладі фінансового департаменту ТОВ «Спектр-Агро») та визначення конструктивних шляхів підвищення рівня кібербезпеки.

Для досягнення поставленої мети визначено такі завдання дослідження: узагальнити поняття та класифікацію кіберризиків у фінансових процесах; проаналізувати сучасні міжнародні стандарти управління кіберризи́ками; обґрунтувати доцільні методи оцінювання ризиків; з'ясувати структуру та специфіку діяльності фінансового департаменту підприємства; визначити актуальні кіберзагрози та вразливості; провести оцінювання кіберризиків за обраними підходами; розробити пропозиції з удосконалення кіберзахисту та оцінити їх ефективність.

У результаті дослідження для ТОВ «Спектр-Агро» запропоновані заходи, які поєднують організаційні, технічні та управлінські рішення, дозволяють підвищити рівень захищеності фінансових даних, зменшити ймовірність кіберінцидентів та підвищити кіберстійкість підприємства.

Рік виконання кваліфікаційної бакалаврської роботи 2026.

Рік захисту роботи 2026.

Ключові слова: кіберризики, кібербезпека, фінансові процеси, управління ризиками, методи оцінювання, моделі оцінювання, фінансовий департамент, вразливості, загрози, ТОВ «Спектр-Агро».

В і д г у к
про кваліфікаційну бакалаврську роботу
здобувача навчально-наукового інституту
«Інститут інформаційних технологій в економіці»
освітньо-професійної програми «Кібербезпека»

Тригуба Євгенія Вячеславовича

(прізвище, ім'я, по батькові)

на тему «Оцінка кіберризиків у роботі фінансового департаменту підприємства
ТОВ «Спектр-Агро»

1. Актуальність теми кваліфікаційної роботи і доцільність її розроблення зумовлена зростанням інтенсивності кіберзагроз у фінансових процесах підприємств, що особливо проявляється в умовах цифровізації та воєнного стану. Це потребує своєчасної оцінки кіберризиків у фінансовому департаменті ТОВ «Спектр-Агро» для підвищення рівня кіберзахищеності та мінімізації потенційних фінансових втрат.
2. Позитивні риси кваліфікаційної роботи: Робота вирізняється актуальністю теми, логічною структурою, ґрунтовним теоретичним опрацюванням і практичною спрямованістю запропонованих рішень щодо підвищення кібербезпеки фінансових процесів підприємства.
3. Наявність самостійних розробок автора проявляється у власній ідентифікації кіберризиків фінансового департаменту, застосуванні комбінованих методик їх оцінювання та обґрунтованні практичних заходів із підвищення кіберстійкості підприємства.
4. Цінність теоретичних висновків та практичних рекомендацій полягає в можливості їх безпосереднього використання для підвищення ефективності управління кіберризиками та вдосконалення системи кібербезпеки фінансового департаменту підприємства
5. Наявність недоліків: Наявні недоліки роботи мають несуттєвий характер і пов'язані з можливістю подальшого розширення окремих розрахунків та деталізації альтернативних варіантів практичних рішень.
6. Загальна оцінка кваліфікаційної бакалаврської роботи та її допущення до захисту перед ЕК: _____

Науковий керівник _____ доцент кафедри, к.е.н.

(посада, науковий ступінь, учене звання)

Труш М.С.

(підпис)

(прізвище, ініціали)

“ ____ ” _____ 2026р.

Рецензія

на кваліфікаційну бакалаврську роботу здобувача
освітньо-професійної програми «Кібербезпека»

Тригуба Євгенія Вячеславовича

(прізвище, ім'я, по батькові)

Тема: «Оцінка кіберризиків у роботі фінансового департаменту підприємства
ТОВ «Спектр-Агро»

Актуальність теми кваліфікаційної роботи і доцільність її розроблення зумовлена зростанням інтенсивності кіберзагроз у фінансових процесах підприємств, що особливо проявляється в умовах цифровізації та воєнного стану. Це потребує своєчасного оцінювання кіберризиків у фінансовому департаменті ТОВ «Спектр-Агро» для підвищення рівня кіберзахищеності та мінімізації потенційних фінансових втрат.

Якість проведеного дослідження характеризується ґрунтовністю теоретичного аналізу, обґрунтованим вибором методів оцінювання кіберризиків та логічною узгодженістю отриманих результатів із поставленою метою роботи.

Позитивні риси кваліфікаційної бакалаврської роботи: робота характеризується актуальністю дослідження, структурованістю викладу, глибоким теоретичним опрацюванням проблеми та наявністю практичних рекомендацій щодо підвищення рівня кібербезпеки фінансових процесів підприємства.

Зауваження до кваліфікаційної бакалаврської роботи полягають у доцільності подальшого розширення окремих аналітичних розрахунків і деталізації альтернативних практичних рішень, що не впливає на загальну позитивну оцінку роботи.

Практична значимість висновків і рекомендацій полягає в можливості їх безпосереднього застосування для зменшення кіберризиків і підвищення рівня кібербезпеки фінансових процесів підприємства.

Місце роботи та посада рецензента ТОВ «СПЕКТР–АГРО»

менеджер систем з інформаційної безпеки

Сергій Клименко

(підпис, ПІБ)

ЗМІСТ

ВСТУП	3
РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДИЧНІ ОСНОВИ ОЦІНЮВАННЯ КІБЕРРИЗИКІВ У ФІНАНСОВІ ДІЯЛЬНОСТІ ПІДПРИЄМСТВА	
1.1. Сутність, класифікація та сучасні підходи до розуміння кіберризиків у фінансових процесах	8
1.2. Теоретичні основи систем управління кіберризиками та міжнародні стандарти їх оцінювання	15
1.3. Методичні підходи та моделі оцінки кіберризиків, придатні для фінансових департаментів підприємств	29
РОЗДІЛ 2. АНАЛІТИКО-ДОСЛІДНИЦЬКА ДІАГНОСТИКА КІБЕРРИЗИКІВ У РОБОТІ ФІНАНСОВОГО ДЕПАРТАМЕНТУ ТОВ «СПЕКТР-АГРО»	
2.1. Характеристика підприємства ТОВ «Спектр-Агро» та фінансового департаменту як об'єкта дослідження	41
2.2. Аналіз поточного стану кіберзагроз і вразливостей фінансових процесів підприємства за останні два роки	51
2.3. Практичне застосування методик оцінки кіберризиків на фактичних даних ТОВ «Спектр-Агро»	60
РОЗДІЛ 3. КОНСТРУКТИВНІ ШЛЯХИ ПІДВИЩЕННЯ КІБЕРБЕЗПЕКИ ФІНАНСОВОГО ДЕПАРТАМЕНТУ ТОВ «СПЕКТР-АГРО»	
3.1. Обґрунтування стратегічних напрямів удосконалення системи управління кіберризиками	74
3.2. Розроблення комплексу організаційних та технічних заходів щодо мінімізації кіберризиків фінансового департаменту	82
3.3. Прогнозування ефективності запропонованих рішень та оцінювання їх впливу на рівень кіберзахищеності підприємства	90
ВИСНОВКИ	96
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	98

ВСТУП

Актуальність. Сучасний етап розвитку суспільства відзначається швидкою інформатизацією, яка охоплює всі сфери діяльності, включаючи правові відносини, економіку, державне управління та соціальну інфраструктуру. Впровадження нових технологій створює нові виклики, серед яких важливими є кіберризики – від несанкціонованого доступу до критично важливих систем до атак на особисті та фінансові дані.

Зростання кількості та складності кіберзагроз вказує на недостатність національних підходів до їх регулювання. Багато країн, зокрема Україна, стикаються з проблемою фрагментарності законодавства щодо кіберзлочинності та управління кіберризиками, а також недостатньою гармонізацією з міжнародними стандартами. Оскільки кіберпростір не має кордонів, а наслідки атак часто є транснаціональними, виникає потреба у створенні єдиних правових і управлінських механізмів для запобігання загрозам та встановлення відповідальності.

В умовах війни проти України значно зросла кількість кібератак на державні установи, критичну інфраструктуру та приватні підприємства. Це робить питання ідентифікації, оцінювання та зменшення кіберризиків особливо актуальним для українського бізнесу, щоб забезпечити безперервність діяльності та захист інформаційних ресурсів.

Згідно з міжнародними аналітичними звітами, фінансові компанії все частіше стають жертвами комбінованих атак, які поєднують соціальну інженерію, експлуатацію технічних вразливостей та інсайдерські загрози. Керівники підприємств вважають кіберризики однією з найбільших загроз для бізнесу останнього десятиліття, що підкреслює їхній вплив на фінансову стабільність, ділову репутацію та довіру клієнтів. У таких умовах системне оцінювання кіберризиків і впровадження механізмів їх зменшення у фінансових департаментах є необхідними для ефективного управління та стратегічного розвитку підприємства.

У аграрному бізнесі, до якого належить ТОВ «Спектр-Агро», фінансовий департамент обробляє чутливу інформацію: платіжні документи, дані контрагентів, кредитні операції, інвестиційні показники, фінансову звітність тощо. Тому фінансовий департамент є одним з найбільш вразливих до кіберзагроз підрозділів підприємства.

Актуальність теми також зумовлена ускладненням кіберзагроз і новими формами атак, такими як фішинг з використанням штучного інтелекту, атаки на ланцюги постачання програмного забезпечення, шкідливі дії інсайдерів, компрометація облікових записів тощо. Без сучасної системи управління кіберризиками фінансовий департамент може стати джерелом значних фінансових втрат, операційних збоїв і юридичної відповідальності через порушення вимог законодавства у сфері захисту інформації.

Огляд наукових публікацій. Теоретичні основи кібербезпеки та управління кіберризиками досліджувалися як зарубіжними, так і вітчизняними науковцями. Аналіз наукових джерел показує, що проблематика кіберризиків розглядалася в працях багатьох дослідників. Значний внесок у методологію кіберризик-менеджменту зробили B. Schneier, R. Anderson, H. Spafford, які розробили принципи комплексного захисту інформації. Економічні аспекти впливу кіберзагроз на підприємства висвітлені в працях L. Gordon, M. Loeb, T. Moore.

Незважаючи на наявність наукової бази, питання оцінювання кіберризиків у фінансовій діяльності підприємств реального сектору економіки залишається недостатньо дослідженим. Більшість існуючих методик орієнтовані на державні інституції або ІТ-компанії і потребують адаптації до специфіки фінансових департаментів, які мають свої бізнес-процеси, технологічні середовища та вимоги до захисту інформації. Це підкреслює необхідність комплексного дослідження, адаптованого до умов українського бізнесу та специфіки діяльності ТОВ «Спектр-Агро».

У межах дипломної роботи сформульовано такі проблемні гіпотези дослідження:

1. Передбачається, що існуючий підхід до управління кіберризиками у фінансовому департаменті ТОВ «Спектр-Агро» не забезпечує повного охоплення специфічних фінансових загроз, що підвищує ймовірність виникнення кіберінцидентів.

2. Передбачається, що використання міжнародних стандартів і методик оцінювання кіберризиків (ISO 27005, NIST SP 800-30, OCTAVE, FAIR) сприятиме підвищенню якості аналізу ризиків і систематизації процесів їх моніторингу.

3. Передбачається, що комплексне поєднання організаційних, технічних та управлінських заходів забезпечить підвищення рівня кіберзахисту фінансових процесів підприємства та сприятиме зменшенню ризиків компрометації фінансових даних.

Мета кваліфікаційної роботи – оцінювання кіберризиків у фінансовій діяльності підприємства (на прикладі фінансового департаменту ТОВ «Спектр-Агро») та визначення конструктивних шляхів підвищення рівня кібербезпеки.

Для досягнення цієї мети визначено такі **завдання**:

1. Розкрити зміст поняття кіберризиків у фінансових процесах та узагальнити існуючі наукові підходи до їх класифікації.
2. Дослідити підходи, закладені в міжнародних стандартах і фреймворках управління кіберризиками, та визначити їх практичну значущість для підприємств.
3. Проаналізувати методики оцінювання кіберризиків і обґрунтувати доцільність їх використання у фінансових департаментах підприємств.
4. Охарактеризувати діяльність ТОВ «Спектр-Агро» та визначити особливості функціонування його фінансового департаменту як об'єкта дослідження.
5. Виявити актуальні кіберзагрози й вразливості, притаманні фінансовим процесам досліджуваного підприємства.
6. Провести оцінювання рівня кіберризиків у фінансовому департаменті підприємства з використанням обраних методичних підходів.

7. Обґрунтувати та розробити практичні заходи, спрямовані на зменшення рівня кіберризиків і посилення кіберзахисту фінансових процесів.
8. Визначити результативність запропонованих заходів з позиції їх впливу на підвищення кіберстійкості підприємства.

Об’єкт дослідження – фінансові процеси підприємства як джерела кіберризиків.

Предмет дослідження – методи та моделі оцінювання кіберризиків у фінансовому департаменті ТОВ «Спектр-Агро».

Наукова новизна полягає в уточненні теоретико-методичних підходів до оцінювання кіберризиків у фінансових процесах підприємства з урахуванням сучасних кіберзагроз. У роботі набули подальшого розвитку підходи до систематизації кіберризиків фінансового департаменту та обґрунтовано використання міжнародних стандартів кібербезпеки в практиці управління фінансовими ризиками підприємства.

Методична основа та методи дослідження. Методичну основу даної роботи становлять наукові праці українських і зарубіжних учених з проблем кібербезпеки та управління ризиками, міжнародні стандарти й рекомендації у сфері інформаційної безпеки, а також нормативно-правові акти України. Інформаційну базу формують внутрішні документи ТОВ «Спектр-Агро», статистика кіберінцидентів, аналітичні звіти з кібербезпеки, законодавство України та нормативні акти в сфері інформаційної безпеки. Для досягнення поставленої мети в роботі використано комплекс загальнонаукових і спеціальних методів дослідження, зокрема аналіз і синтез, порівняння та систематизацію – для узагальнення теоретичних положень; матричні та напівкількісні методи – для оцінювання рівня кіберризиків; експертні оцінки – для обґрунтування практичних заходів, спрямованих на підвищення рівня кібербезпеки фінансових процесів підприємства.

Практичне значення отриманих результатів кваліфікаційної роботи полягає в можливості їх використання у діяльності фінансового департаменту ТОВ «Спектр-Агро» з метою підвищення рівня кібербезпеки та зменшення

кіберризиків фінансових процесів. Розроблені підходи до ідентифікації, оцінювання та класифікації кіберризиків можуть бути застосовані для вдосконалення внутрішньої системи управління ризиками підприємства, зокрема під час організації платіжних операцій, оброблення фінансових даних та роботи з електронними документами.

Запропоновані практичні заходи щодо мінімізації кіберризиків можуть бути використані при розробленні або актуалізації внутрішніх регламентів, політик інформаційної безпеки та процедур контролю доступу у фінансових підрозділах підприємства. Крім того, результати дослідження можуть бути використані в процесі проведення внутрішнього аудиту, оцінювання ефективності діючих заходів кіберзахисту та під час навчання персоналу щодо протидії сучасним кіберзагрозам.

Структура роботи. Кваліфікаційна бакалаврська робота складається зі змісту, вступу, 3 розділів, 9 підрозділів, в яких викладено теоретичні основи, результати аналізу та практичні рекомендації для покращення кібербезпеки підприємства, висновків, списку використаних джерел. Робота містить таблиці, графіки, додатки.

Ключові слова: *кіберризики, кібербезпека, фінансові процеси, управління ризиками, методи оцінювання, моделі оцінювання, фінансовий департамент, вразливості, загрози, ТОВ «Спектр-Агро».*

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДИЧНІ ОСНОВИ ОЦІНЮВАННЯ КІБЕРРИЗИКІВ У ФІНАНСОВІЙ ДІЯЛЬНОСТІ ПІДПРИЄМСТВА

1.1. Сутність, класифікація та сучасні підходи до розуміння кіберризиків у фінансових процесах

У сучасному світі, де суспільство все швидше переходить у цифрову сферу, поняття «кіберризик» набирає особливого значення. Воно охоплює широкий спектр проблем, включаючи не тільки технічні аспекти, але й соціальні, економічні та юридичні ризики, що виникають у кіберпросторі. З юридичної точки зору, кіберризик можна визначити як імовірність виникнення негативних правових наслідків у результаті небезпечних дій або подій у цифровому середовищі. Водночас в українському законодавстві, зокрема Законі України «Про основні засади забезпечення кібербезпеки України», відсутнє чітке визначення терміна «кіберризик». Замість цього, використовуються поняття, що описують конкретні види ризиків: «кіберінцидент», «кібератака», «кібершпигунство» та «кібертероризм». Подібна ситуація спостерігається у Конвенції про кіберзлочинність (Будапештській конвенції), де також відсутній термін «кіберризик», і акцент робиться на криміналізації злочинів, пов'язаних з комп'ютерними системами та даними. Деякі стратегічні документи, наприклад, «Стратегія кібербезпеки України», підкреслюють необхідність методик оцінки та страхування кіберризиків. Однак, термін «кіберризик» не має чіткого нормативного визначення [10,с.1;34,с.12]. Внаслідок цього, виникає необхідність більш детального роз'яснення сутності поняття «кіберризик». Ця концепція формується на стику трьох ключових областей:

1. технологічної (наявність слабких місць в інформаційних системах);
2. соціальної (існування зловмисників, які можуть використати ці слабкості);
3. правової (недостатність або прогалини у державному регулюванні).

Кіберризик доцільно визначати як імовірність реалізації певної кіберзагрози, що може спричинити негативні наслідки – порушення конфіденційності чи цілісності даних, спотворення інформаційних ресурсів, фінансові втрати або інші шкідливі ефекти для діяльності підприємства.

Водночас важливо чітко розмежовувати поняття «кіберзагроза» та «кіберризик».

Кіберзагроза – це потенційна дія, подія або явище, яке може завдати шкоди інформаційним системам, даним або бізнес-процесам; вона описує джерело та характер можливої небезпеки, наприклад фішинг, шкідливе програмне забезпечення чи інсайдерську активність.

Кіберризик є ширшим поняттям. Він відображає не лише наявність загрози, а й імовірність її реалізації та масштаб можливих наслідків для організації. Тобто кіберзагроза відповідає на запитання що може статися, тоді як кіберризик – наскільки це ймовірно та якими будуть наслідки для фінансових процесів, безперервності роботи та дотримання регуляторних вимог.

Саме тому аналіз загроз є лише початковим етапом побудови системи кіберзахисту, тоді як управління ризиками включає їхню оцінку, ранжування за критичністю та вибір оптимальних заходів з їхнього зменшення чи контролю.

У фінансовій сфері кіберризики становлять особливу загрозу, оскільки можуть порушувати точність облікової інформації, безпеку фінансових операцій та бізнес-процесів. За висновками С.М. Адаменка [1, с.10], загрози кіберпростору слід розглядати як невід’ємний елемент загальної системи захисту інформації у фінансовій сфері. Їхній вплив може проявлятися у зміні фінансових показників, погіршенні платоспроможності та підриві репутаційної стійкості компанії.

Іноземні експерти розглядають кіберризики ширше – як сукупність різноманітних загроз і вразливостей, що можуть спричинити порушення функціонування цифрових систем. У звіті World Economic Forum підкреслюється, що зростання кіберзагроз та посилення кібернерівності

формують одні з найбільш значущих викликів для глобальної економіки та бізнесу у найближчі роки [50, с.3]. Світовий банк зазначає, що в країнах, які швидко цифровізуються, темпи впровадження технологій часто випереджають інвестиції у кіберстійкість, що підвищує їхню вразливість, а одним із найбільш уражених секторів глобально є фінансовий [49, с.27].

У наукових джерелах виділяють кілька підходів до класифікації кіберризиків, узагальнені у таблиці 1.1.

Таблиця 1.1

Класифікація кіберризиків

<i>Критерії</i>	<i>Група ризиків</i>	<i>Приклади</i>
За джерелом виникнення	Внутрішні	Помилки персоналу, порушення доступів
	Зовнішні	Хакерські атаки, шкідливе ПЗ
За типом впливу	Фінансові	Крадіжки коштів, фальсифікація платежів
	Операційні	Зупинка систем, DDoS-атаки
	Репутаційні	Витоки даних
	Регуляторні	Порушення законодавства
За об'єктом впливу	Транзакційні системи	Несанкціоновані перекази
	Бухгалтерські системи	Підміна даних
	Персональні дані	Витоки інформації
	Інфраструктура	Зупинка серверів, атаки на мережу
За мотивацією зловмисника	Фінансова	Вимагання, крадіжка коштів, шахрайські транзакції
	Шпигунська	Викрадення конфіденційних даних, промисловий шпionаж
	Деструктивна	Саботаж, видалення або шифрування даних
	Ідеологічна/хактивізм	Атаки з політичних або соціальних мотивів
За технікою атаки	Соціальна інженерія	Фішинг, вішинг, компрометація облікових даних
	Технічні атаки	Експлуатація вразливостей, SQL-ін'єкції, експлойти
	Мережеві атаки	DDoS-атаки, перехоплення трафіку, MITM
	Шкідливе ПЗ	Рансомвар, трояни, програми-кейлогери

Джерело: розроблено автором на основі [1,2,4,8,9,13,14,16,17,21,25]

Сучасні системи штучного інтелекту створюють нову категорію кіберзагроз, оскільки здатні автоматизувати фішингові операції, генерувати

правдоподібні повідомлення та значно ускладнювати виявлення соціальної інженерії. Додаткову небезпеку становлять алгоритмічні помилки та упередження моделей, які можуть спричинити хибні рішення в автоматизованих фінансових процесах або маніпуляцію даними. Крім того, використання ШІ підвищує ризик зловживань, коли моделі застосовуються зловмисниками для аналізу вразливостей, підбору паролів або творення шкідливого коду.

Найпоширенішим критерієм класифікації є поділ кіберризиків за джерелом їх виникнення – на внутрішні та зовнішні [2, с.14, 8, с.21]. До внутрішніх відносять ризики, що виникають через прорахунки працівників, порушення правил доступу, недбалість або навмисні дії персоналу. Зовнішні ризики охоплюють кібератаки, зараження шкідливим програмним забезпеченням, фішингові інциденти, а також атаки, спрямовані на постачальників чи елементи цифрової інфраструктури [5, с.35].

З огляду на характер наслідків кіберризиків поділяють на фінансові, операційні, репутаційні та регуляторні [12, с.15; 23, с.28]. Фінансові ризики пов'язані з втратою коштів або незаконними транзакціями, операційні – з порушенням безперервної роботи бізнес-процесів. Репутаційні ризики виникають у разі витоку важливої інформації або розголошення фактів кібератак, тоді як регуляторні стосуються можливого недотримання вимог законодавства у сфері кібербезпеки [9, с.2; 10, с.1; 33, с.5-6; 53, с.3-4].

Ще один підхід ґрунтується на визначенні об'єкта впливу кіберзагроз: виділяють ризики, що стосуються транзакційних систем, систем обліку, персональних даних та інфраструктурних інформаційних ресурсів [6, с.31; 28, с.43]. Для кожної з цих категорій характерні свої типові атаки – від підміни транзакцій і шифрування ERP до витоків даних і компрометації мережевих ресурсів. Такий підхід дозволяє точніше визначати критичність кожного ресурсного сегмента та формувати адресні заходи захисту відповідно до специфіки потенційних загроз.

У сучасних системах управління ризиками кіберризиками розглядаються як важлива частина загальної корпоративної системи Enterprise Risk Management (ERM). Це означає, що їх слід аналізувати не лише з технічного боку, а також з урахуванням того, як вони можуть впливати на фінансові результати, стратегічні цілі та репутацію підприємства [15, с.21; 35, с.42; 49, с.12]. Сучасні підходи до розуміння кіберризиків у фінансових процесах можна узагальнити та поділити на напрями, що зображено на рисунку 1.1.



Рисунок 1.1 – Підходи до оцінювання кіберризиків

Джерело: розроблено автором [7, с.24; 30, розд.2-3; 33, с.32].

Процесний підхід спрямований на оцінювання кіберризиків через аналіз ключових бізнес-процесів компанії, зокрема тих, що стосуються платежів, бухгалтерського обліку, документообігу та функціонування інформаційних систем. У цьому випадку ризики розглядаються в контексті їхнього впливу на конкретні етапи діяльності підприємства [7, с.24; 15, с.32].

Стандартизований підхід, включаючи міжнародні стандарти ISO та NIST, зокрема ISO/IEC 27001 та ISO/IEC 27005, визначає чіткі правила оцінювання ризиків інформаційної безпеки і побудови систем їх управління. [18, розд.6;19, розд.7-8]. У США особливу популярність здобули NIST

Cybersecurity Framework, а також керівні документи NIST SP 800-30 і NIST SP 800-53, які описують детальні методики аналізу ризиків і впровадження відповідних заходів контролю. [30, розд. 2-3; 31, розд. 3; 32, розд. 2].

Методи моделювання загроз спрямовані на передбачення й аналіз можливих атак, інструментів, якими можуть скористатися кіберзлочинці, та наслідків для компаній. У цьому контексті міжнародні організації, такі як ENISA, Microsoft, IBM, Palo Alto Networks та інші, регулярно інтегрують ці моделі у свої щорічні аналітичні доповіді щодо кіберзагроз. Завдяки цьому формується актуальне розуміння ризиків і динаміки їх розвитку [16; 17; 20; 36; 37; 41; 51; 52].

Економічний підхід зосереджений на аналізі фінансових наслідків кіберінцидентів: оцінці потенційних втрат, витрат на відновлення інфраструктури, збитків від простоїв у роботі та розмірів коштів для виконання нормативних вимог. Цей метод сприяє підприємствам у раціональному обґрунтуванні витрат на кіберзахист та визначенні економічної ефективності реалізованих заходів [33, с.42; 49, розд.1; 50, розд.3-4].

Сучасна практика оцінювання кіберризиків включає поділ методів на якісні та кількісні. Якісні підходи ґрунтуються на думках експертів і застосовуються в умовах обмеженості даних чи складності їх формалізації. До них належать методи експертного аналізу та матриці ризиків, які дають змогу порівняти ймовірність виникнення інцидентів із потенційним впливом і швидко визначити ключові пріоритети для глибшого дослідження.

Кількісні методи дозволяють оцінювати ризики у фінансовому вираженні, забезпечуючи глибше розуміння потенційних загроз. Серед найбільш поширених підходів виділяються моделі SLE (Single Loss Expectancy) та ALE (Annual Loss Expectancy), які допомагають розрахувати одноразові втрати та очікувані річні збитки відповідно. Більш деталізований аналіз пропонує модель FAIR, яка дозволяє дослідити як прямі, так і непрямі втрати, враховуючи ключові фактори ризику. Метод Монте-Карло, у свою чергу, забезпечує моделювання великої кількості можливих сценаріїв і визначення

спектру потенційних втрат з урахуванням невизначеностей. Поєднання якісних та кількісних підходів дозволяє створити збалансоване розуміння рівня кіберризиків і сприяє прийняттю обґрунтованих управлінських рішень в межах фінансових процесів.

Еволюція кіберзагроз від простих вірусів і примітивних атак 1990-х призвела до виникнення масштабних, добре організованих кампаній із фінансовою мотивацією, в яких часто використовуються елементи промислового шпигунства. Сучасний ландшафт кіберризиків формується цільовими фішинговими атаками, загрозами на ланцюги постачання та програмами-вимагачами, що активно застосовують автоматизацію та штучний інтелект для обходу систем захисту. У відповідь на це організації все частіше впроваджують комплексні ризик-орієнтовані програми кіберстійкості, які поєднують технології, процеси та ефективні управлінські підходи.

Отже, кіберризики у фінансовій діяльності підприємств представляють собою складне та багатогранне явище, яке виникає через поєднання технічних вразливостей, організаційних недоліків, людського фактора і вимог регуляторного середовища. Вони охоплюють не лише ймовірність перебоїв у роботі інформаційних систем або зовнішніх атак, а й можуть значно впливати на стабільність ключових фінансових процесів. Це зачіпає такі аспекти, як достовірність бухгалтерських даних, безперебійність платіжних операцій, дотримання нормативних стандартів і збереження репутації компанії. Тому кіберризики доцільно аналізувати як інтегральну частину системи корпоративного управління, включно з бюджетуванням, контролем доступу, аудитом і визначенням зон відповідальності співробітників.

Сучасні міжнародні підходи та дослідження висвітлюють, що фінансові підрозділи компаній стикаються з широким спектром взаємопов'язаних ризиків. Їхній перелік охоплює технічні загрози (компрометація ІТ-інфраструктури, фішинг, шкідливе ПЗ), організаційні недоліки (прогалини в контролі, помилки персоналу), зовнішні фактори (ризики постачальників, контрагентів чи хмарних платформ) і вимоги регуляторів (аудит, фінансовий моніторинг). У цій сфері

навіть незначний інцидент може зашкодити обороту коштів, виконанню контрактів, складанню звітності, податковим розрахункам і стійкості бізнесу загалом, роблячи фінансову сферу надзвичайно важливою з точки зору кіберзахисту.

Додаткова складність полягає у вартості фінансових даних – банківських реквізитів, бухгалтерських проводок, первинної документації, звітності чи доступу до систем дистанційного банкінгу. Вони є одночасно цінними активами підприємства і головними об'єктами кіберзлочинців. Усі випадки несанкціонованого втручання у ці дані можуть призвести як до прямих втрат (затримки платежів, штрафні санкції та спотворення фінансових показників), так і до непрямих негативних наслідків (втрата довіри партнерів, судові розгляди та репутаційні ризики).

З огляду на це, кіберризики у фінансових процесах слід визначати як ймовірність реалізації кіберзагроз, які можуть порушити конфіденційність, цілісність або доступність фінансової інформації, спричинити викривлення облікових даних, здійснення несанкціонованих операцій чи тимчасову зупинку критично важливих систем. Такі сценарії здатні спричиняти юридичні, економічні й репутаційні втрати. Подібне трактування узгоджується із загальновизнаними міжнародними підходами до управління ризиками та формує основу для детального аналізу, моделювання і вибору ефективних заходів для мінімізації кіберзагроз у фінансовій діяльності компанії.

1.2. Теоретичні основи систем управління кіберризиками та міжнародні стандарти їх оцінювання

Система управління кіберризиками (CRMS) представляє собою скоординовану структурну основу, яка об'єднує політики, процеси, ролі та контрольні механізми для виявлення, оцінки (кількісної та якісної), пріоритизації та управління ризиками, спричиненими кіберзагрозами. Ця система інтегрована у загальнокорпоративну систему управління ризиками

(ERM, Enterprise Risk Management), що дозволяє забезпечити узгодженість рішень із кібербезпеки з фінансовими, операційними та стратегічними цілями підприємства.

Сучасні дослідники відзначають, що ефективна CRMS повинна знаходити оптимальний баланс між рівнем захисту системи й економічною доцільністю інвестицій у безпеку. Це питання особливо актуальне для фінансових підрозділів, які прагнуть мінімізувати витрати без шкоди для ефективності захисту.

Основу функціонування CRMS складають ключові принципи: системний підхід, орієнтація на ризики, безперервність і адаптивність, а також відповідність прийнятому рівню ризик-апетиту. Завдяки цьому забезпечується координація управлінських рішень, оперативна реакція на нові виклики та формування культури безпеки, що сприяє розумінню кожним співробітником своєї ролі у забезпеченні стійкості організації.

У наукових і міжнародних джерелах CRMS часто розглядають через її структурні компоненти, детальний перелік яких представлено у таблиці 1.2.

Таблиця 1.2

Основні елементи системи управління кіберризиками

<i>Елемент CRMS</i>	<i>Зміст</i>
Політики та стандарти безпеки	Набір правил, процедур, регламентів щодо захисту активів
Ідентифікація активів	Каталогізація інформаційних ресурсів та визначення власників
Оцінювання ризиків	Класифікація загроз, вразливостей, впливів і ймовірностей
Контрольні заходи	Технічні, організаційні та процесні механізми мінімізації ризиків
Моніторинг і аудит	Постійне відстеження ефективності контролів, аудит, KRI/KPI
Реагування та відновлення	Інцидент-менеджмент, план безперервності, резервування
Постійне вдосконалення	Оновлення політик/контролів, навчання персоналу, аналіз інцидентів

Джерело: розроблено автором на основі [18, розд. 4-10; 19, розд. 7-8]

CRMS ґрунтується на кількох ключових принципах:

1.Процесний підхід у CRMS:

CRMS функціонує як постійний циклічний процес, у рамках якого діяльність з управління ризиками регулярно оновлюється та вдосконалюється. Це передбачає, що оцінювання ризиків, запровадження відповідних заходів контролю та аналіз їхньої ефективності виконуються не як одноразові дії, а повторюються системно на всіх етапах життєвого циклу системи безпеки. Такий підхід базується на моделі PDCA (Plan-Do-Check-Act), яка є основою міжнародного стандарту ISO 27001 і забезпечує безперервний процес управління інформаційною безпекою. Враховуючи особливості фінансового департаменту підприємства, на основі цієї моделі розроблено адаптовану таблицю 1.3, що пояснює практичну реалізацію кожного етапу PDCA та перелік ключових артефактів, притаманних фінансовим процесам.

Таблиця 1.3

Інтерпретація PDCA-циклу для фінансових процесів підприємства

<i>Етап</i>	<i>Практичний зміст для фіндепартаменту</i>	<i>Основні артефакти</i>
P - Plan	Визначення фінансових активів (клієнт-банк, ERP, ЕЦП), ролей, ризик-апетиту; формування критеріїв $P \times I$	Реєстр активів, профіль ризиків, матриця доступів
D - Do	Впровадження контролів: MFA, SoD, сегментація, підтвердження реквізитів, резервне копіювання	Налаштовані контролі, регламенти, журнали подій
C - Check	Верифікація: KRI/KPI, аналіз інцидентів, аудит доступів, перевірка відповідності процедур	Звіти аудиту, KRI/KPI, звіти моніторингу
A - Act	Корекція політик, навчання, оновлення контролів; адаптація заходів до нових загроз	Оновлені політики, оновлені SoD/доступи, план удосконалення

Джерело: розроблено автором на основі [18, розд.4-10]

Логіка PDCA в рамках ISMS передбачає циклічний підхід підприємства до управління ризиками. Це включає планування контексту, критеріїв та процедур для ризик-менеджменту, впровадження організаційних і технічних контролів, перевірку їх ефективності через моніторинг, вимірювання та аудит, а

також удосконалення політик і контролів на основі аналізу інцидентів і результатів перевірок [18,розд.4-10].

Поєднання підходів DevSecOps, Zero Trust і безперервного моніторингу перетворює цикл PDCA із просто формального документа на ефективний адаптивний механізм, здатний оперативно реагувати на зміну загроз.

2. Ризик-орієнтоване мислення:

На відміну від традиційного підходу, де головна увага приділялася переважно загрозам, система керування ризиками кібербезпеки (CRMS) акцентує увагу на саме ризиках – взаємозв'язку між вразливостями, ймовірністю атаки та потенційними наслідками. Недолік загрозо-центричного підходу полягає у можливому нераціональному перерозподілі бюджетів, коли ресурси направляються на другорядні ризики. Натомість модель ризик-орієнтованої логіки пропонує зосередити увагу на найвпливовіших сценаріях. Це допомагає сфокусувати ресурси підприємства на великих ризиках, замість того щоб розпорошувати зусилля на маловажливі загрози. Для фінансових департаментів це критично важливо, оскільки навіть один успішний інцидент може мати значні економічні наслідки.

3. Системність і комплексність CRMS:

CRMS створюється як цілісна конструкція, що охоплює всі ключові аспекти організації:

- технології: IT-інфраструктура, системи контролю доступу, засоби моніторингу;
- процеси: політики, процедури та стандартизовані регламенти;
- персонал: навчання працівників, контроль доступу та дотримання вимог безпеки;
- управління: визначення політик, розподіл відповідальності, проведення аудиту та систематичний контроль.

Комплексність висуває чіткий акцент на тому, що кіберзахист не можна забезпечити лише технологіями. Відповідні процеси та людський фактор є не менш важливими складовими системи.

4. Ролі та відповідальність у CRMS:

Ефективність CRMS залежить від чіткої організації ролей і зон відповідальності в структурі організації. Ключовою фігурою є керівник із інформаційної безпеки (CISO). Його завдання включають розробку політики кіберзахисту, організацію аналізу ризиків та впровадження заходів контролю. CISO наглядає за узгодженістю між IT-відділом, внутрішнім аудитом, топменеджментом і бізнес-процесами, забезпечуючи відповідність міжнародним стандартам і власним політикам компанії. IT-директор (CIO/CTO) відіграє ключову роль у реалізації технічного компонента кіберзахисту. Він відповідає за архітектуру інформаційних систем, впровадження рішень з контролю доступу та моніторингу, а також за оперативне реагування на інциденти. CIO забезпечує технічну підтримку ініціатив CISO та контролює їх ефективне застосування в робочих умовах організації.

Керівник фінансового департаменту (CFO) відіграє ключову роль у фінансових процесах підприємства, керуючи активами, мінімізуючи ризики фінансових операцій та визначаючи бюджети кіберзахисту спільно з CISO. Бізнес-власники процесів відповідають за ризики у своїх відділах, дотримання політик і контроль доступу, гарантуючи практичний підхід до управління ризиками. Внутрішній аудит перевіряє ефективність контролів, аналізує ризики та надає рекомендації для їх зниження, забезпечуючи прозорість. Топ-менеджмент і власники підприємства визначають стратегію, затверджують політику кібербезпеки та контролюють ресурси й ефективність системи. Data Protection Officer (DPO) та архітектор Zero Trust відповідають за захист даних і доступи в середовищах з високими ризиками, забезпечуючи відповідність регуляторним нормам і впроваджуючи сучасні механізми безпеки. Злагоджена робота цих ролей створює результативну систему кіберризиків, здатну оперативно реагувати на загрози та забезпечувати стабільність бізнесу.

5. Міжнародні стандарти CRMS: ISO та NIST

Ефективна система управління кіберризиками базується на дотриманні міжнародних стандартів, які визначають єдині вимоги до політик, процесів та

контролів безпеки. Серед ключових нормативних документів, на які спирається CRMS, варто виділити ISO/IEC 27001, що встановлює вимоги до побудови системи управління інформаційною безпекою, та ISO/IEC 27005, який описує методологію оцінювання ризиків. У практиці також широко застосовуються стандарти NIST: NIST CSF 2.0 – рамкова модель організації кіберзахисту, NIST SP 800-30 – методичні рекомендації щодо проведення аналізу ризиків, та NIST SP 800-53 – комплексний каталог технічних і організаційних контролів. Разом ці документи формують структурну основу CRMS, визначаючи її процеси, вимоги до контролів та підхід до вимірювання ефективності.

На практиці ISO/IEC 27001/27005 виконують роль керівного каркаса (політики, ролі, PDCA), тоді як NIST CSF/SP 800-30/SP 800-53 використовують для прикладного дизайну контролів і сценарного аналізу ризиків; у поєднанні вони знімають методичний розрив між «що робити» та «як реалізувати».

6. Моніторинг, аналітика та безперервне вдосконалення:

Система CRMS працює на основі постійного збору даних, їх аналізу та безперервного нагляду. Вона спрямована на те, щоб збирати інформацію про інциденти, аналізувати рівні вразливостей, відстежувати ефективність контролів (KPI/KRI), прогнозувати можливі сценарії атак.

Сучасні системи аналізу (SIEM/XDR) та елементи III допомагають виявляти аномалії й прискорюють реагування. Безперервне вдосконалення включає перегляд політик, оновлення інфраструктури та адаптацію CRMS до нових технологічних і регуляторних змін.

Кіберзагрози постійно змінюються, тому CRMS повинна регулярно оновлюватись – перегляд політик, модернізація інфраструктури, підвищення кваліфікації персоналу, адаптація до нових законодавчих вимог.

Міжнародні стандарти оцінювання системи управління кіберризиками формують універсальну рамку, що дозволяє організаціям у різних країнах дотримуватися єдиного підходу до виявлення, аналізу та оброблення кіберризиків. Найбільш поширеними є стандарти сімейства ISO/IEC, зокрема ISO/IEC 27001 та ISO/IEC 27005, які визначають вимоги до побудови системи

інформаційної безпеки та методологію ризик-менеджменту. Поряд із ними NIST Cybersecurity Framework та документи NIST SP 800-30 і SP 800-53 пропонують деталізовані інструменти для моделювання загроз, оцінювання впливу інцидентів та впровадження контрольних заходів. Завдяки цим стандартам підприємства отримують узгоджені підходи до формування політик безпеки, проведення аудиту, побудови процесів моніторингу та управління інцидентами, що суттєво підвищує їхню кіберстійкість у глобальному цифровому середовищі.

ISO/IEC 27001:2022 – міжнародний стандарт, що встановлює вимоги до системи управління інформаційною безпекою (ISMS – Information Security Management System). Він визначає ключові компоненти ISMS, зокрема політики безпеки, процеси внутрішнього аудиту, порядок реагування на інциденти та механізми постійного вдосконалення [18,розд.5-10].

ISO/IEC 27005:2022 є міжнародним стандартом, який надає детальні методичні рекомендації для організацій у сфері оцінювання та управління ризиками інформаційної безпеки. На відміну від нормативних документів, що встановлюють жорсткі технічні вимоги, цей стандарт акцентується на організації процесу роботи з ризиками: від ідентифікації критичних активів та потенційних загроз до визначення найефективніших заходів реагування. Він сприяє формуванню в організаціях послідовного і систематизованого підходу до управління ризиками, що забезпечує прогнозованість, структурованість і відповідність загальній політиці безпеки [19,розд.7].

У практиці фіндепартаменту зручно оцінювати ризик як добуток імовірності та впливу за формулою 1.1

$$R = P \times I \quad (1.1)$$

де P – імовірність того, що інцидент або загроза реалізується;

I – величина можливих наслідків або збитків.

Матриця ризиків (Risk Matrix) у стандарті ISO/IEC 27005 є одним із ключових інструментів, який використовується для системної оцінки рівня загроз в інформаційній безпеці. В основі її побудови лежить напівкількісний

підхід, коли ризик визначають як поєднання двох параметрів – ймовірності інциденту та масштабу його можливих наслідків. Обидва показники оцінюють за шкалою від 1 до 5, що дозволяє стандартизувати оцінювання та порівняти різні сценарії ризиків між собою (табл.1.4).

Завдяки матриці ризику не лише вимірюються чисельно, але й візуально структуруються, що значно спрощує їх інтерпретацію. Комбінація оцінок Р та І дозволяє віднести конкретний ризик до однієї з категорій: від низького (зелена зона) до критичного (червона зона). Такий підхід допомагає підприємству швидко визначити, які загрози потребують негайного реагування, а які можуть бути прийняті або контрольовані з мінімальними ресурсами.

Таблиця 1.4

Матриця ризиків ($P \times I$, шкала 1-5)

Ймовірність / Вплив	1–Низький	2–Помірний	3–Середній	4 – Високий	5 –Критичний
5 – Дуже висока	Середній	Середній	Високий	Дуже високий	Критичний
4 – Висока	Помірний	Середній	Високий	Дуже високий	Дуже високий
3 – Середня	Низький	Помірний	Середній	Високий	Дуже високий
2 – Низька	Низький	Низький	Помірний	Середній	Високий
1 – Дуже низька	Низький	Низький	Низький	Помірний	Середній

Джерело: розроблено автором на основі [19, розд.7-8]

Примітка автора: кольорове зонування не використовується, але рівні “критичний/дуже високий/високий” застосовуються як пріоритети для фінансових процесів.

Фреймворк (framework) – готова схема роботи, яка показує що потрібно робити та в якій послідовності, але не диктує конкретних технічних рішень. Він допомагає навести порядок у процесах, зробити їх передбачуваними та такими, що легко оцінювати й покращувати.

У сфері кіберризиків найвідомішим є NIST Cybersecurity Framework (NIST Cybersecurity Framework 2.0 – це повна, офіційна назва версії,

опублікованої NIST у 2024 році). Його можна уявити як “дорожню карту” кібербезпеки [32,секц.2].

Оновлена версія NIST CSF 2.0 увела окрему функцію Govern, яка забезпечує зв'язок між стратегією організації та операційними процесами безпеки, закриваючи прогалину між «що потрібно робити» і «хто за це відповідає». Такий акцент сприяє узгодженню CRMS із корпоративним управлінням і наглядом.

У фінансовому департаменті доцільно застосовувати CSF 2.0 як рамку узгодження ролей, політик і контрольних дій. Нижче наведено приклади практичних кроків у розрізі шести функцій, орієнтованих на платіжні операції, бухгалтерський облік і роботу з конфіденційними фінансовими даними.

Govern (GV) – управління:

1. Затвердження ризик-апетиту для фінансових процесів на рівні правління/CFO з прив'язкою до RTO/RPO, порогів втрат і лімітів на простої платіжного контуру.
2. Ролі й відповідальність – матриця RACI для ініціювання платежів, узгодження, візування, банківських відносин, інцидент-менеджменту.
3. Політики доступу та сегментації – дисципліна мінімальних привілеїв, розділення обов'язків (SoD) між ініціатором, узгоджувачем і відправником платежів.
4. TPRM – вимоги до безпеки у договорах із банками, хмарними бухсервісами та провайдерами ЕЦП (SLA, право аудиту, повідомлення про інцидент, тест відмовостійкості).
5. Метрики наглядового рівня – щомісячний звіт CFO по KRI/KPI.

Identify (ідентифікація):

1. Реєстр активів фіндепартаменту – клієнт-банк, ERP/облік, реєстр ЕЦП/токенів, шаблони платіжних доручень, довідники контрагентів, журнали погодження.
2. Картування даних – класифікація фінданих (IBAN, договори, первинка, ЗКП/ЗЕД) і визначення власників.

3. Реєстр ризиків – сценарії BEC/фішингу, підміни реквізитів, злам акаунта, збої інтеграцій; первинна оцінка PхI, позначення контролів та власників.
4. Залежності – перелік критичних інтеграцій (банки, СЕА/податкові шлюзи, хмарні сервіси).

Protect (захист):

1. Доступ і автентифікація – MFA для клієнт-банку та обліку; окремі обліковки для ініціації/узгодження/відправки; денай-лист для географій/ASN.
2. Захист даних – шифрування резервних копій, DLP-правила для IBAN/ЄДРПОУ у пошті; watermark/штампи на платіжних PDF.
3. SoD та «чотири очі» – обов’язкове подвійне погодження платежів вище порога; ліміти і «step-up»-верифікація для змін реквізитів контрагента.
4. Процедури зміни реквізитів – out-of-band перевірка (телефон за довідником, а не з листа), журнал перевірок, шаблони підтверджень.
5. Навчання – щоквартальні тренінги/фішинг-симуляції з індивідуальними зворотними зв’язками.

Detect (виявлення):

1. Моніторинг подій – кореляція входів у клієнт-банк/ERP, сповіщення про логіни з нових пристроїв/локацій, аномалії часу та сум.
2. Сигнатури BEC – виявлення листів із «терміновою зміною реквізитів», доменів-двійників, невідповідності доменного підпису (DMARC/DKIM/SPF).
3. Вразливості – трекінг критичних CVE на робочих станціях фіндепартаменту та серверах ERP, SLA усунення.
4. KRI виявлення – частка платежів з ручною зміною реквізитів; кількість підозрілих запитів від «керівника»; кількість відхилених листів без DMARC.

Respond (реагування):

1. Плейбук інцидентів платежів – стоп-процедура (призупинити відправлення, заморозити чергу), внутрішні повідомлення (CFO, CISO, IT, юристи), зовнішні контакти (банк, контрагент).
2. Комунікаційний чек-лист – шаблон листа/дзвінка банку, фіксація часу звернення, ID-інциденту, службова записка.

3. Чорний список – оперативне внесення доменів-двійників/IBAN-шахраїв, блокування правил маршрутизації.
4. Збір артефактів – збереження логів, платіжних доручень, e-mail-заголовків, скріншотів для розслідування/страховика.
5. Пост-мортем – аналіз причин, оновлення контролів, додатковий тренінг команди, звіт у наглядовий комітет.

Recover (відновлення):

1. RTO/RPO для платіжного контуру – перевірка відновлення клієнт-банку/ERP із резервів; тест відпрацювання черги платежів.
2. Альтернативні канали – узгоджені з банком резервні канали відправлення платіжок (наприклад, відділення/окремий веб-канал) на час інциденту.
3. Перевірка цілісності – звірка контрагентів/реквізитів після інциденту; контроль повторної відправки/відкату.
4. Комунікація з контрагентами – типові повідомлення про затримки, запити на підтвердження реквізитів, оновлення статусу.
5. Уроки і профілактика – оновлення процедур SoD, лімітів, шаблонів перевірок; планова перевірка резервних копій і вправи з відновлення.

Документ NIST SP 800-30 (NIST SP 800-30 Rev.1 – оновлений, покращений та актуальний варіант, який слід використовувати сьогодні) – це один із ключових документів Національного інституту стандартів і технологій США (NIST), який описує, як правильно проводити оцінку ризиків інформаційної безпеки в організації. У цьому документі подано покрокову методику, яка допомагає визначати, які загрози існують, наскільки вразливими є системи, з якою ймовірністю інцидент може статися та яких збитків він може завдати.

На відміну від нормативних стандартів, NIST SP 800-30 не встановлює жорстких правил, а надає практичні рекомендації, як будувати процес аналізу ризиків. У ньому описано такі етапи: визначення активів, ідентифікація загроз і вразливостей, оцінка ймовірності та впливу, класифікація рівнів ризику та вибір методів їх подальшої обробки.

NIST SP 800-30 сприяє тому, щоб організація могла систематично й аргументовано підходити до управління кіберризиками, охоплюючи як технічні, так і організаційні аспекти, а також враховуючи реальні сценарії потенційних атак [30,секц.2-3].

NIST SP 800-53 Rev.5 (загальна назва стандарту NIST SP 800-53) – це базовий каталог контролів безпеки та приватності для інформаційних систем і організацій. Його мета – дати уніфікований набір заходів (політики, процеси, технічні та організаційні контролі), щоб захищати операції, активи й персональні дані від широкого спектра ризиків: від кібератак і помилок людей до збоїв інфраструктури та інцидентів конфіденційності. Актуальна редакція опублікована у вересні 2020 року (з оновленнями від 10.12.2020) і доступна безкоштовно на сайті NIST. Офіційна сторінка публікації також зазначає наявність мапінгів до NIST CSF, NIST Privacy Framework та ISO/IEC 27001:2022, що спрощує узгодження програм безпеки між фреймворками.

Редакція Rev.5 об'єднала безпеку й приватність в єдиний каталог контролів, додала нові сімейства – PT (PII Processing & Transparency) та SR (Supply Chain Risk Management) – і перейшла на орієнтацію на результат у формулюваннях контролів; каталог офіційно публікується також у машиночитних форматах OSCAL (JSON/XML/YAML) для автоматизації та мапінгів. Крім того, 27.08.2025 NIST опублікував мінорний реліз 5.2.0 (точкові доповнення/правки до низки контролів і посилань).

Ключові риси Rev.5 (у чому відмінність від попередніх версій):

1. Єдиний каталог безпеки й приватності. Контролі приватності інтегровані в основний перелік, більше немає окремого додатка – це підкреслює нерозривний зв'язок безпеки та приватності в реальних системах.
2. Нові сімейства контролів. Додано контрольні сімейства PT (PII Processing and Transparency) та SR (Supply Chain Risk Management), що відображає сучасні виклики – обробку персональних даних і ризики ланцюгів постачання.

3. Орієнтація на результат: формулювання контролів сфокусовані на цільовому ефекті, а не тільки на кроках виконання, що полегшує адаптацію під контекст організації.
4. 20 сімейств контролів. Каталог охоплює 20 доменів (AC, AT, AU, CA, CM, CP, IA, IR, MA, MP, PE, PL, PM, PS, PT, RA, SA, SC, SI, SR), що дає повний набір важелів управління ризиками в різних середовищах (on-prem, хмара, IoT, критична інфраструктура тощо).
5. Підтримка автоматизації. Каталог доступний у OSCAL (JSON/XML/YAML) і у вигляді таблиць/списків базлайнів (спільно з SP 800-53B), що полегшує імпорт у GRC-системи та побудову контрольних «базових профілів» за рівнями Low/Moderate/High.

Документ використовують федеральні агентства США та підрядники у межах FISMA, але його так само беруть за основу в приватному секторі, щоб структурувати програми безпеки, провести гар-аналіз, підібрати релевантні контроли та узгодити їх із ризик-апетитом і нормативними вимогами. Rev.5 сумісний із RMF/800-37 і слугує «конструктором» контролів, з якого формується організаційний набір захисту під конкретні ризики та середовище експлуатації [31,розд.1-3].

Підходи ISO та NIST до управління ризиками мають спільну мету – забезпечити системний контроль над загрозами, однак різняться акцентами. ISO зосереджується на створенні цілісної системи менеджменту та циклічному процесі (PDCA), тоді як NIST надає більш деталізовані технічні рекомендації та конкретні контроли для практичної реалізації захисту на рівні систем і процесів.

COBIT (Control Objectives for Information and Related Technologies) – фреймворк ISACA для IT-governance, що узгоджує IT з бізнес-цілями, задає ролі/відповідальність і метрики ефективності на рівні всієї організації [21, EDM01-EDM05; APO01].

На відміну від ISO/IEC 27001/27005 (процес ISMS) та NIST (каталоги контролів і сценарний аналіз), COBIT працює на рівні управління – формує цілі керування, політики та показники, які «зшивають» процеси безпеки end-to-end.

Для фінансових процесів це корисно, бо спрощує мапінг контролів, підтримує оцінку зрілості та інтегрується з ISO/NIST/ITIL. COBIT доцільно застосовувати як «парасольку» над CRMS.

Основні характеристики підходів систематизовано в таблиці 1.5.

Таблиця 1.5

Порівняння підходів ISO, NIST, OCTAVE

<i>Підхід</i>	<i>Практична користь для фіндепартаменту</i>	<i>Джерела даних усередині компанії</i>	<i>Основний артефакт</i>
ISO/IEC 27001–27005	Дозволяє формально визначити активи, встановити критерії ризику та узгодити політики безпеки з фінансовими процесами	Реєстр активів (ERP, клієнт-банк), матриця доступів, внутрішні регламенти, аудиторські матеріали	Профіль ризиків фіндепу та план їх оброблення
NIST CSF / SP 800-30 / SP 800-53	Дає практичні орієнтири: які саме контролі потрібні для захисту платежів, обліку й доступів; допомагає структурувати сценарії атак	Журнали подій, історія інцидентів, логіни у клієнт-банк, договори з банками й хмарними сервісами	Мапінг функцій CSF на фінпроцеси та перелік контрольних заходів
OCTAVE	Дозволяє швидко визначити критичні активи та операційні загрози фіндепартаменту через участь бізнес-користувачів	Інтерв'ю з фінансистами, карти процесів, перелік документів та точок прийняття рішень	Три етапи: перелік ключових активів – сценарії загроз – пріоритетний список заходів

Джерело: розроблено автором на основі [18,19,30,32]

Важливим елементом CRMS є управління ризиками третіх сторін (TPRM). Воно охоплює попередню перевірку постачальників, фіксацію вимог до безпеки в договірних документах (SLA/OLA із правом аудиту, умовами інцидент-репортування), постійний моніторинг виконання зобов'язань і заздалегідь визначені сценарії виходу зі співпраці. Така практика зменшує як концентраційні ризики, так і ланцюгові ризики, що є типовими для хмарних сервісів та критичних ІКТ-провайдерів. У хмарному контексті TPRM також має

чіткий фінансовий вимір: до SLA/OLA доцільно включати вимірювані метрики надійності провайдера, вимоги до своєчасного повідомлення про інциденти та право на доступ до облікових логів (журналів подій), а також фінансові тригери розірвання договору у разі невиконання узгоджених показників.

У підсумку розділ окреслює CRMS як цілісну конструкцію, у якій політики, процеси, ролі та контрольні заходи замикаються у безперервний цикл PDCA. Ризик-орієнтована логіка дозволяє спрямовувати ресурси на сценарії з найбільшим очікуваним фінансовим ефектом, тоді як комплексність CRMS забезпечує узгодженість технологічних рішень, процедур, людського фактора й управлінських рішень. Ролі учасників (CISO, CIO/CTO, CFO, бізнес-власники процесів, внутрішній аудит і топ-менеджмент, а також DPO та архітектор Zero Trust) структуровано за зонами відповідальності, що забезпечує трасованість рішень від ризику до контролю та метрики ефективності.

Міжнародні стандарти ISO/IEC 27001-27005 формують керівний каркас і процесну дисципліну, тоді як NIST (CSF 2.0, SP 800-30, SP 800-53) надають практичні інструменти сценарного аналізу та деталізують контрольні заходи – у поєднанні це знімає розрив між “що робити” і “як реалізувати”. Водночас нові умови (використання ШІ, домінування хмарних сервісів, ризику ланцюга постачання ПЗ) вимагають адаптивного оцінювання, постійного моніторингу KPI/KRI та впровадження Zero Trust у фінансово критичні процеси (платіжні операції, облік, клієнт-банкінг). У подальших розділах ця рамка слугуватиме основою для вибору методів оцінки і побудови системи показників для фіндепартаменту ТОВ «Спектр-Агро».

1.3. Методичні підходи та моделі оцінки кіберризиків, придатні для фінансових департаментів підприємств

Українські наукові та практичні дослідження засвідчують, що кіберризик у фінансових процесах формуються під впливом кількох груп

чинників – технічних, організаційно-процесних та людських. Саме тому їх слід аналізувати не ізольовано, а як складову частину корпоративної системи управління ризиками (ERM/CRMS) [1, с.16; 11, с.31; 14, с.10-22]. Такий системний підхід закріплений і в нормативно-практичних документах: рекомендаціях Мінцифри України, аналітичних звітах ДССЗІ та міжнародних стандартах ISO і NIST, які наголошують на потребі комплексного та безперервного ризик-менеджменту [14,с.10-22; 27,с.5-12].

Для методичного підґрунтя доцільно спиратися на узгоджену рамку міжнародних стандартів. З одного боку, ISO/IEC 27005 задає процесну логіку управління ризиками інформаційної безпеки в контексті ISMS (цілі, критерії, процедури та PDCA-цикл). З іншого боку, документи NIST деталізують сценарний аналіз (SP 800-30) і надають каталог контрольних заходів (SP 800-53) для практичної реалізації захисту; у зв'язці це полегшує перехід від ідентифікації ризику до вибору та впровадження релевантних контролів [18,розд.4-10;19, розд.7-8;30,секц.2-3]. Таким чином, ці стандарти взаємодоповнюють один одного – ISO визначає логіку та структуру процесу, а NIST забезпечує глибину й практичні інструменти для проведення оцінювання.

Міжнародні аналітичні звіти (ENISA, WEF, Світовий банк) послідовно підкреслюють, що наслідки кіберінцидентів мають вимірюваний фінансовий ефект, а тому організаціям доцільно переходити до кількісних підходів до оцінювання ризиків, здатних враховувати невизначеність і «товсті хвости» розподілів втрат для рідкісних, але дорогих подій [16,розд.20;15,с.40-55;46,с.5-12; 47,с.30-45;49,с.15-35; 50, с.5-12]. За спостереженнями ENISA, упродовж 2024 -2025 рр. зберігалася висока інтенсивність рандсомвар-активності, відбувалася комодифікація фішингу через Phishing-as-a-Service, а переважна частка інцидентів була зумовлена масовими низьковартісними DDoS-кампаніями (до 80% у вибірці інцидентів, зафіксованих у відповідних оглядах). WEF фіксує поглиблення «кібернерівності»: частка організацій, що підтримують мінімально життєздатний рівень кіберстійкості, скоротилася приблизно на 30%, на тлі дефіциту понад 4 млн фахівців із кібербезпеки.

Світовий банк показує, що в країнах, що розвиваються, близько 36% розкритих кіберінцидентів припадає на державний сектор, тоді як фінансові установи стабільно входять до найуразливіших, водночас системні інвестиції в кіберстійкість корелюють із кращими макро - та галузевими результатами.

Вибір конкретної методики оцінювання має відштовхуватися від чотирьох практичних критеріїв: наявності даних, терміновості ухвалення рішень, потреби у грошовій інтерпретації результатів та рівня зрілості ISMS/CRMS. У такій оптиці методи виконують спільне завдання: системно виявляти релевантні загрози, аналізувати їхній вплив на інформаційні активи та прогнозувати можливі наслідки для бізнес-процесів. У практиці доцільно комбінувати якісні, напівкількісні та кількісні підходи: перші – для швидкої пріоритизації за браку даних; другі – для структурованого ранжування з урахуванням ваг чинників; треті – для фінансово обґрунтованих рішень щодо контролів і бюджетів. Власне, ISO/IEC 27005 і NIST SP 800-30 і передбачають таку інтеграцію методів у єдиний процес ризик-менеджменту (ідентифікація – аналіз – оцінка – оброблення – моніторинг), що забезпечує і методичну послідовність, і керованість впровадження [18,розд.4-10;19,розд.7-8;30,секц.2-3].

Якісні методи оцінювання кіберризиків використовують тоді, коли немає достатніх статистичних даних, процеси важко формалізувати або потрібно оперативно отримати загальне уявлення про рівень загроз. У вітчизняних роботах (та практиках аудиту) використовують експертні техніки, зокрема SWIFT, Delphi та Peer Review, які базуються на колективній оцінці фахівців щодо можливих загроз і слабких місць системи, а також матриці ризиків $P \times I$ (5×5) для ранжування сценаріїв у «зелену/жовту/червону» зони [1,с.60-75;14,с.30-40;19, розд.7-8;секц.3]. Сильні сторони – швидкість і залучення бізнес-експертів; обмеження – суб'єктивність і нечутливість до «товстих хвостів» рідкісних, але дорогих подій [1,с.60-75;11,с.35-50; 15,с.40-55;20,с.6-12].

SWIFT – це швидкий метод експертної оцінки ризиків, коли група фахівців у форматі структурованої дискусії визначає можливі загрози, слабкі місця та потенційні наслідки для системи.

Delphi – це метод послідовного опитування експертів, у якому їхні думки збирають анонімно та узгоджують у кілька етапів, щоб отримати найбільш об'єктивну спільну оцінку ризиків.

Peer Review – це експертна перевірка, коли незалежні спеціалісти оцінюють процеси, рішення або систему безпеки, щоб виявити недоліки та запропонувати покращення.

NIST SP 800-30 прямо допускає використання якісних оцінок на різних «ярусах» управління ризиком (організація – процес – система), а ISO/IEC 27005 радить починати з якісного профілю ризиків і уточнювати його за потреби напівкількісними /кількісними інструментами.

До якісних методів відноситься ще методика оцінювання кіберризиків OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), яка розроблена Університетом Карнегі-Меллона для організацій, яким потрібно проаналізувати свої інформаційні активи та визначити найбільш критичні загрози. На відміну від технічно орієнтованих моделей, OCTAVE робить акцент на бізнес-контексті – ключову роль у процесі відіграють співробітники, які знають операційні процеси, а не лише IT-фахівці.

Методика складається з трьох логічних етапів:

1. Визначення критичних активів і бізнес-цілей – організація встановлює, що саме потрібно захищати.
2. Ідентифікація загроз, слабких місць і ризикових сценаріїв – формується перелік потенційних інцидентів та умов, які можуть їх спричинити.
3. Розроблення пріоритетних заходів – для найкритичніших ризиків визначаються стратегії реагування та підвищення стійкості.

OCTAVE корисна тим, що поєднує організаційний, процесний і технічний аналіз, дозволяючи отримати повну картину ризиків та визначити, де саме підприємство має найбільшу вразливість у своїй роботі. Має такі переваги

– самокерованість і фокус на операційній специфіці, але водночас має і обмеження – переважно якісний характер і потреба доповнення кількісними оцінками для бюджету [4,розд.1-3;1,с.60-75;11,с.35-50;15,с.40-55].

Перевага якісних методів в оперативності та гнучкості, а недолік в суб'єктивності оцінок та обмеженості у випадках, коли потрібні точні фінансові виміри.

Напівкількісні методи оцінювання кіберризиків поєднують у собі якісний підхід із числовими шкалами, що дозволяє надавати більш структуровану та зіставну оцінку ризикам. Завдяки переведенню експертних суджень у цифрові показники підприємство може точніше ранжувати загрози та визначати їхню пріоритетність.

Одним із найбільш уживаних інструментів є системи оцінювання ймовірності та наслідків за шкалою від 1 до 10. Такий підхід зберігає простоту якісного аналізу, але водночас дає змогу деталізувати відмінності між ризиками та точніше визначати ті з них, що становлять найбільшу загрозу для підприємства [26,с.45-60]. Він широко застосовується в ISO/IEC 27005.

У межах методу вагомих коефіцієнтів кожному фактору ризику – технологічному, організаційному чи людському – присвоюється певна вага, яка відображає його важливість для загальної оцінки. Після цього фактори оцінюються за шкалою, а підсумковий рівень ризику визначають як суму добутків ваг і відповідних оцінок, згідно з формулою 1.2:

$$R = \sum(W_i \times S_i), \quad (1.2)$$

де W_i – ваговий коефіцієнт фактора;

S_i – бальна оцінка цього фактора.

Такий метод підходить для узгодження ризик-апетиту та орієнтовного перерозподілу ресурсів захисту, однак їх точність залежить від узгодженості шкал між підрозділами [19, розд.7-8; 26, с.45-60].

Кількісні методи допомагають оцінити кіберризики у грошовому вимірі, що особливо корисно для фінансових департаментів при плануванні бюджету

на кібербезпеку. Модель ALE (Annual Loss Expectancy) дозволяє оцінити потенційні щорічні збитки від кіберінцидентів, показуючи масштаб загроз і обґрунтовуючи витрати на захист інформаційних систем. [15,с.40-55;20,с.4-12].

Основою моделі є визначення очікуваного річного збитку, який розраховується як добуток одноразових втрат та частоти виникнення інцидентів, згідно з формулою 1.3:

$$ALE = SLE \times ARO, \quad (1.3)$$

де SLE (Single Loss Expectancy) – передбачуваний збиток від одного кіберінциденту;

ARO (Annualized Rate of Occurrence) – очікувана кількість таких інцидентів протягом року.

Для обчислення SLE використовується формула 1.4:

$$SLE = AV \times EF, \quad (1.4)$$

де AV – вартість активу, який може бути пошкоджено або втрачено;

EF – частка збитків від інциденту, виражена у відсотках.

У підсумку модель ALE дозволяє компанії оцінити, якою може бути річна фінансова шкода у разі реалізації певного ризику, і порівняти її з витратами на впровадження заходів безпеки. Це робить модель корисним інструментом для стратегічного планування та обґрунтування інвестицій у кіберзахист, але водночас вона має обмеження у вигляді чутливості до якості параметрів ARO/EF та ігнорування форми розподілу втрат [15,с.40-55;20,с.4-12]. Приклад застосування методу ALE наведено у таблиці 1.6.

Таблиця 1.6

Приклад оцінювання за методом ALE

Актив	Вартість (AV)	Коефіцієнт втрати (EF)	$SLE=AV \times EF$	Частота інцидентів за рік (ARO)	$ALE = SLE \times ARO$
Платіжний сервер	500 000 грн	0,30	150 000 грн	0,20	30 000 грн/рік
База даних клієнтів	800 000 грн	0,25	200 000 грн	0,10	20 000 грн/рік

Джерело: розроблено автором на основі [20, с.4-12]

Методологія FAIR (Factor Analysis of Information Risk) – міжнародний підхід до оцінювання кіберризиків, що визначає фінансові наслідки кіберінцидентів і широко застосовується у фінансовій сфері завдяки точності та структурованості. [20,с.4-12;22,розд.2-4;48,с.30-45]. У практиці її часто комбінують з attack-trees для моделювання атак і кількісного аналізу на рівні вузлів, що зручно для складних фінансових бізнес-процесів із численними інтеграціями. У FAIR ризик розраховується як добуток частоти події на величину можливих втрат за формулою 1.5.

$$\text{Risk} = \text{LEF} \times \text{LM}, \quad (1.5)$$

де LEF (Loss Event Frequency) описує, як часто може відбутися подія;

LM (Loss Magnitude) показує, якими будуть її фінансові наслідки.

Структура LEF деталізується через (формула 1.6):

$$\text{LEF} = \text{TEF} \times V, \quad (1.6)$$

де TEF – частота появи загроз;

V – ймовірність того, що атака буде успішною.

Величина втрат визначається як сума двох компонентів (формула 1.7):

$$\text{LM} = \text{PL} + \text{SL}, \quad (1.7)$$

де PL – прямі збитки (наприклад, відновлення систем чи втрата даних);

SL – непрямі втрати, що можуть проявлятися у простоях, репутаційних ризиках або штрафах.

Таблиця 1.7 містить модель FAIR, яка показує зв'язок між частотою подій і розміром можливих втрат, а також пояснює її складові у контексті фінансової діяльності підприємства.

Таблиця 1.7

Узагальнена структура оцінювання ризику за моделлю FAIR

Компонент	Сутність у контексті фінансових процесів	Приклади даних
TEF – частота загроз	Як часто виникає подія, що може призвести до атаки	Фішинг-спроби, спроби зміни реквізитів
V – вразливість	Ймовірність того, що загроза буде	Наявність MFA, якість паролів,

	успішною	SoD
LEF – частота подій втрат	Результат $TEF \times V$ – скільки інцидентів може статися	Кількість реальних інцидентів за рік
PL – прямі збитки	Прямі витрати на відновлення систем або втрату коштів	Збитки від несанкціонованих платежів
SL – непрямі збитки	Репутаційні втрати, затримки роботи, штрафи	Затримка платежів, зриви операцій
LM – загальний масштаб збитків	PL + SL – повний вплив на фіндепартамент	Загальний розрахунок втрат

Джерело: розроблено автором на основі [22, розд.2-4]

Завдяки такій структурі FAIR дає змогу не лише визначити рівень ризику, а й зрозуміти, які чинники найбільше впливають на можливі збитки.

Для урахування невизначеностей у частотах/збитках використовують метод Монте-Карло – тисячі ітерацій формують розподіл можливих втрат і метрики VaR/TVaR (оцінки «хвостових» ризиків) [20, с.4-12;22, розд.2-4;46,с.5-12;47,с.30-45]. Це особливо важливо для фінансово значущих сценаріїв (зупинки платежів, компрометація бухгалтерського ядра, витоки клієнтських БД) і для обґрунтування страхування/самострахування. Коли потрібна швидка орієнтація керівництва, то використовуємо матрицю $P \times I$; коли потрібна конкретна сума в гривнях для планування бюджету, то застосовуємо ALE; а коли важливо врахувати рідкісні, але дорогі події й чутливість сценаріїв, то обираємо FAIR або моделювання Монте-Карло з метриками VaR/TVaR.

Кількісні моделі є найпереконливішими для обґрунтування інвестицій у кіберзахист.

Комбіновані моделі оцінювання кіберризиків поєднують елементи якісного та кількісного аналізу, що дозволяє отримати більш повну та збалансовану картину ризиків. Такий підхід дає змогу спочатку швидко окреслити потенційні загрози на основі експертних суджень, а потім доповнити цю інформацію числовими розрахунками, що забезпечує точніші висновки та обґрунтовані управлінські рішення. Він використовується в ISO/IEC 27005 та NIST SP 800-30, адже дозволяє охопити як структурну сторону ризику, так і фінансову.

Порівняльна характеристика моделей оцінювання кіберризиків у таблиці 1.8 дозволяє наочно побачити відмінності між підходами за їх призначенням, точністю та сферою застосування. Завдяки такому зіставленню легко визначити, які методи є найбільш придатними для аналізу конкретних кіберзагроз та прийняття обґрунтованих управлінських рішень.

Таблиця 1.8

Порівняльна характеристика моделей оцінювання кіберризиків

<i>Модель/Метод</i>	<i>Тип оцінювання</i>	<i>Основні переваги</i>	<i>Основні недоліки</i>
Матриця ризику (ISO/IEC 27005)	Якісний/ напівкількісний	Проста у використанні, наочне представлення ризиків, підходить для початкового аналізу	Значна суб'єктивність, нечіткість меж між рівнями ризику
ALE (Annual Loss Expectancy)	Кількісний	Дає можливість визначити очікувані фінансові втрати та обґрунтувати бюджет на кіберзахист	Потребує достовірних статистичних даних щодо частоти інцидентів
FAIR (Factor Analysis of Information Risk)	Кількісний	Висока точність, урахування прямих та непрямих втрат, структурний аналіз факторів ризику	Складність збору параметрів, потребує експертних знань
OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)	Якісний/ комбінований	Орієнтація на бізнес-процеси, акцент на критичних активах, залучення персоналу, добра структуризація загроз і сценаріїв	Переважно якісний характер, потребує значного часу та участі групи експертів
NIST SP 800-30	Комбінований	Сценарний аналіз, детальний опис загроз і вразливостей, комплексний підхід	Вимагає значних ресурсів та участі експертів
NIST CSF 2.0	Комбінований	Системний підхід, охоплює всі аспекти кіберзахисту,	Не містить конкретних методів

		гнучкість застосування	розрахунку ризику
ISO/IEC 27005	Напівкількісний	Чітка методологія управління ризиками, міжнародний стандарт	Потребує адаптації під специфіку підприємства

Джерело: розроблено автором на основі [4, розд.1-3; 15 с.40-55; 19, розд.7-8; 22, розд.2-4; 30; 31; 32]

Контрольні заходи являють собою скоординований набір організаційних, технічних та процесних інструментів, спрямованих на зниження ймовірності виникнення кіберзагроз або мінімізацію їхніх наслідків. До цих заходів входять політики та регламенти, управління доступом, навчання персоналу, технічний моніторинг, реагування на інциденти, резервне копіювання та відновлення, проведення аудиту, а також постійне вдосконалення.

Для оцінки ефективності роботи механізмів безпеки використовуються метрики – числові показники, які дозволяють визначити, наскільки добре функціонує система безпеки і де можуть виникати проблеми. Метрики поділяються на два основні типи: KPI (Key Performance Indicators) – показники результативності процесів і контрольних механізмів, такі як швидкість виявлення та реагування на інциденти, рівень покриття систем засобами захисту, чи дотримання SLA; і KRI (Key Risk Indicators) – індикатори ризику, які сигналізують про зростання загроз або уразливостей, наприклад, накопичення критичних CVE понад допустимий рівень SLA, аномальну активність доступу чи частоту помилок користувачів. Система KPI/KRI дає змогу відстежувати поточний стан безпеки, ефективніше розподіляти ресурси для інвестицій у захист, керувати ризиками на основі реальних даних, а також узгоджувати рівень захисту з ризик-апетитом і стратегічними завданнями бізнесу [18,розд. 9-10;31; 35, с.120-140].

На основі висвітленого матеріалу можна дійти висновку, що ефективно оцінювання кіберризиків у фінансових департаментах потребує використання методичних підходів, що базуються на інтеграції декількох моделей і методик. Це обумовлено тим, що природа кіберризиків є багатогранною, формуючись під впливом широкого спектра взаємопов'язаних чинників, які включають

технічні аспекти, організаційні особливості та поведінкові елементи людського фактора. Міжнародні стандарти ISO/IEC 27005 і NIST SP 800-30 виступають фундаментом для побудови цілісного та системного підходу до управління ризиками. Перший із них забезпечує чітку логічну структуру процесного підходу до управління ризиками, тоді як другий деталізує практичні методи сценарного аналізу, самооцінки й інструментів визначення як ймовірності ризиків, так і потенційних наслідків їх реалізації. Синергетичне застосування цих стандартів сприяє гармонізації процедур оцінювання, дозволяє точніше ідентифікувати ризики та забезпечує перехід від загальних теоретичних формулювань до вибору конкретних заходів управління та контролю. Такий підхід не тільки підвищує точність оцінювання кіберризиків, а й дає змогу гнучко адаптувати запобіжні заходи до специфічних умов діяльності фінансових структур.

Аналіз показує, що в реальних умовах фінансових процесів неможливо обмежитися одним методом оцінки ризиків. Якісні моделі (SWIFT, Delphi, Peer Review, OCTAVE) дозволяють швидко ідентифікувати загрози та вразливості, особливо в ситуаціях, коли відсутні достовірні статистичні дані. Напівкількісні підходи забезпечують структуроване ранжування ризиків та врахування різної ваги факторів. Кількісні методики, зокрема ALE та FAIR, надають змогу оцінити ризики у фінансовому вимірі, що є критичним для обґрунтування витрат на кіберзахист у фінансових підрозділах підприємств. Методика FAIR у поєднанні зі сценаріями моделювання на основі Монте-Карло здатна враховувати високий рівень невизначеності та масштаб потенційних фінансових втрат, що має критичне значення, особливо при аналізі малоймовірних інцидентів із дуже значними наслідками. Це дозволяє формувати більш адаптивну та життєздатну модель управління ризиками в умовах фінансової нестабільності.

Отже, найбільш раціональний та дієвий підхід у даному контексті полягає в інтеграції різних методологій, що охоплюють як поглиблений якісний аналіз, так і детальну фінансову оцінку. Такий рівень комбінованого аналізу дає

можливість отримати всебічне уявлення про потенційні загрози та вразливості, дозволяючи ефективно збалансувати фінансові витрати на заходи безпеки та оптимальний рівень захисту підприємства. Більше того, він створює базу для прийняття зважених управлінських рішень, які зможуть адекватно враховувати як економічні аспекти діяльності організації, так і її загальну цифрову стійкість. Зрештою інтегроване застосування взаємодоповнюючих методик дає змогу сформувати цілісну систему управління ризиками, здатну оперативно і точно виявляти, аналізувати та зменшувати кіберзагрози, що можуть впливати на фінансові процеси підприємства.

Висновок до розділу 1

В першому розділі роботи сформовано теоретико-методичні основи оцінювання кіберризиків у фінансовій діяльності підприємства. Встановлено, що кіберризики є комплексним явищем, яке виникає під впливом технічних вразливостей, людського фактора, організаційних недоліків і регуляторного середовища та здатне спричиняти значні фінансові, операційні й репутаційні втрати.

Обґрунтовано необхідність розмежування понять «кіберзагроза» і «кіберризик», що дозволяє перейти від суто технічного підходу до ризик-орієнтованого управління фінансовими процесами, а також узагальнено основні класифікації кіберризиків за джерелами виникнення, типами впливу, об'єктами атак і техніками реалізації, що дає змогу системно оцінювати критичність загроз для фінансового департаменту підприємства.

Проаналізовано теоретичні засади побудови системи управління кіберризиками (CRMS), інтегрованої в загальнокорпоративну систему ERM, і визначено, що ефективна CRMS базується на процесному підході, циклі PDCA, чіткому розподілі ролей і застосуванні міжнародних стандартів ISO/IEC та NIST, які забезпечують методологічну узгодженість і практичну реалізованість заходів кіберзахисту.

Узагальнено методичні підходи до оцінювання кіберризиків – від якісних і напівкількісних методів до кількісних моделей ALE, FAIR і моделювання Монте-Карло; доведено доцільність їх комбінування залежно від управлінських потреб і рівня зрілості системи ризик-менеджменту, а отримані висновки є методологічною основою для подальшого прикладного аналізу кіберризиків у фінансовому департаменті підприємства.

Сформований у розділі теоретико-методичний підхід дозволяє забезпечити системність і послідовність подальших етапів дослідження та створює базу для ідентифікації, оцінювання й пріоритизації кіберризиків з урахуванням специфіки фінансових процесів, що дає змогу перейти до їх практичного аналізу та розроблення ефективних заходів мінімізації.

РОЗДІЛ 2. АНАЛІТИКО-ДОСЛІДНИЦЬКА ДІАГНОСТИКА КІБЕРРИЗИКІВ У РОБОТІ ФІНАНСОВОГО ДЕПАРТАМЕНТУ ТОВ «СПЕКТР-АГРО»

2.1. Характеристика підприємства ТОВ «Спектр-Агро» та фінансового департаменту як об'єкта дослідження

ТОВ «Спектр-Агро» – одна з найпомітніших компаній українського аграрного ринку, яка працює з 2009 року та спеціалізується на дистрибуції насіння, засобів захисту рослин, добрив і сільськогосподарської техніки провідних виробників. Компанія сформувала широку мережу регіональних представництв та забезпечує стабільну роботу з клієнтами по всій Україні. Головний офіс розташований у місті Обухів Київської області. За час діяльності підприємство вибудувало стійкі партнерські відносини з кількома тисячами агровиробників – від малих фермерських господарств до великих агрохолдингів.

Фінансові результати діяльності підприємства упродовж останніх років свідчать про позитивну динаміку розвитку, що підтверджується зростанням доходу, прибутку та показників рентабельності (табл. 2.1).

Таблиця 2.1

Динаміка основних фінансових показників ТОВ «Спектр-Агро»
за 2023-2025 рр.

Рік	Дохід, млн грн	Чистий прибуток, млн грн	Рентабельність, %
2023	5 200	210	4,0
2024	6 100	260	4,3
2025	7 300	340	4,7

Джерело: узагальнено автором на основі фінансової звітності підприємства

Як видно з таблиці, у 2023-2025 рр. ТОВ «Спектр-Агро» демонструє стабільне зростання доходів і чистого прибутку. Важливим показником є рентабельність, яка збільшилася з 4,0% до 4,7%, що вказує на підвищення ефективності використання ресурсів і зміцнення фінансового стану компанії.

Динаміку зміни чистого прибутку наочно відображено на рис. 2.1, що підтверджує стійку тенденцію до його зростання протягом аналізованого періоду.

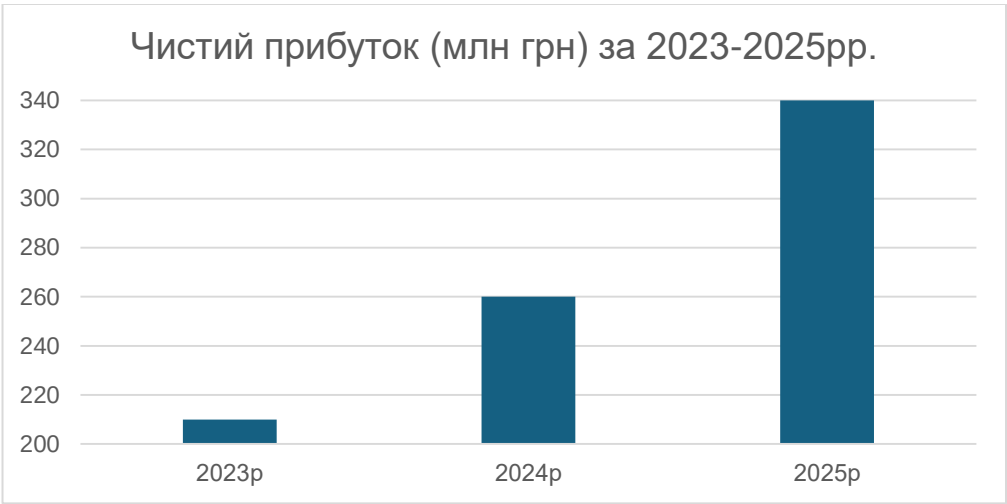


Рисунок 2.1 – Діаграма чистого прибутку (млн грн) за 2023-2025рр.

Джерело: розроблено автором на основі фінансових звітів ТОВ «Спектр-Агро»

«Спектр-Агро», не маючи власних земель чи виробничих потужностей, зосереджує діяльність на сервісі та логістиці. Компанія поєднує дистрибуцію ресурсів із технічним супроводом, консультаціями та фінансовими рішеннями для клієнтів. Це спричиняє великий обсяг електронних операцій, інтеграцій з

банками та державними сервісами, через що фінансовий департамент стає ключовим центром кіберризиків. Згідно з міжнародними стандартами викладеними в Розділі 1 (ISO/IEC 27005, NIST CSF 2.0, PDCA/ISMS), саме він визначений як основний об'єкт для кібероцінювання.

Специфіка галузі зумовлює суттєві сезонні коливання робочого навантаження. У періоди посівних і збиральних кампаній значно зростають обсяги замовлень, відвантажень, погоджень документів і проведення платіжних операцій. Такі пікові періоди супроводжуються підвищенням терміновості виконання завдань, що підвищує ризик помилок співробітників і створює сприятливі умови для здійснення соціально-інженерних атак. Саме в ці моменти активізуються фішингові розсилки та ВЕС-сценарії, спрямовані на викрадення платіжних рішень або зміну реквізитів. Ця ситуація підтверджує принципи, розглянуті в Розділі 1, які підкреслюють важливість оцінки ризиків не просто як переліку загроз, а як взаємозалежності подій із певною ймовірністю та можливим впливом на конкретні бізнес-процеси й активи.

Окрім основних напрямів діяльності, товариство пропонує клієнтам широкий спектр додаткових сервісів – від налаштування й обслуговування техніки до розробки технологічних карт і агрономічного супроводу. Функціонують також партнерські програми фінансування та інші дотичні послуги. Кожен із цих напрямів генерує окремі інформаційні потоки, створює нові точки взаємодії із зовнішніми системами та підвищує вимоги до контролю доступів, управління ідентичностями та забезпечення цілісності даних. Відтак зростає потреба у чіткому структуруванні ризиків та застосуванні системних підходів до їх оцінювання, визначених у методологічній рамці Розділу 1.

Фінансовий департамент у цій моделі є середовищем, де концентруються найважливіші дані підприємства – операційні, комерційні та логістичні. У його структурі функціонують такі підрозділи:

1. Бухгалтерія – первинні документи, податкова звітність, робота з державними е-сервісами.

2. Казначейство – платіжний календар, клієнт-банк, валютні операції, step-up-верифікація змін реквізитів і лімітів.
3. Контроль дебіторської заборгованості (Credit Control) – кредитні ліміти, моніторинг прострочок, акти звірок.
4. Фінансове планування та аналіз (FP&A) – бюджет/факт, прогнозування, аналіз маржинальності та грошових потоків.
5. Внутрішній контроль і комплаєнс – політики доступів, реалізація принципу SoD, аудит операцій.

У контексті підходів, викладених у Розділі 1, така структура відповідає ризик-орієнтованому підходу CRMS, у межах якого технічні, процесні та людські фактори розглядаються у взаємозв'язку з інформаційними активами та їх бізнес-наслідками.

Фінансовий департамент працює в умовах цифрового середовища, що включає ERP (облік, закупівлі, склади), CRM (дані контрагентів, історія, кредитні умови), клієнт-банк, електронний документообіг, BI-аналітику та API-інтеграції з банками й службами. Відповідно до ISO/IEC 27005, всі активи ідентифікуються, класифікуються й додаються до реєстру для оцінки ризиків за моделлю $P \times I$ (ймовірність $\times$ вплив). У таблиці 2.2 наведено узагальнені результати. Критичність активів визначається за шкалою загроз і впливу (1-5), після чого їх відносять до категорій: «критичний», «дуже високий», «високий» або «середньо високий». Методологія забезпечує системне ранжування ризиків і ефективну пріоритетизацію захисту фінансових процесів.

Таблиця 2.2

Основні цифрові активи фінансового департаменту ТОВ «Спектр-Агро»
та рівень їх критичності

<i>Категорія активу</i>	<i>Приклади даних</i>	<i>Відповідальний підрозділ</i>	<i>Рівень критичності</i>	<i>Потенційні кіберризики</i>

Фінансові транзакції	Платіжні доручення, виписки банку, шаблони платежів	Казначейство	Критичний	ВЕС-атаки, фішинг, порушення безпеки облікового запису клієнт-банку
Податкова документація	Податкові накладні, ПН/РК, декларації	Бухгалтерія	Дуже високий	Злам КЕП, підміна документів, блокування ЕДО
Довідники контрагентів	ІВАН, ЄДРПОУ, адреси, умови договорів	CRM Юридичний відділ	Високий	Підміна реквізитів, шкідливі зміни умов
Аналітичні моделі і бюджети	Прогнози, моделі cash-flow, плани/факт	FP&A	Середньо-високий	Витік звітності, порушення цілісності даних
Електронні ключі та доступи	КЕП керівника, бухгалтерії, паролі до ERP/CRM	Керівники процесів + ІТ	Критичний	Несанкціоновані платежі, підміна документів

Продовження таблиці 2.2

Інтеграційні дані	API з банками, податковими шлюзами, логістикою	ІТ+ Фіндепартамент	Високий	Атаки MITM, збої синхронізації
Електронна пошта	Листи контрагентів, рахунки, підтвердження реквізитів	Усі фінансові підрозділи	Дуже високий	Фішинг, ВЕС, шкідливі вкладення

Джерело: розроблено автором на основі [19, розд. 7, 8]

Фінансовий департамент ТОВ «Спектр-Агро» працює в умовах інтенсивного обміну даними між внутрішніми системами (ERP, CRM), зовнішніми сервісами (банки, державні податкові шлюзи) та каналами корпоративної комунікації (електронна пошта, ЕДО). Кожен із цих інформаційних потоків є критичним, оскільки містить чутливі фінансові дані,

впливає на безперервність бізнес–процесів та є потенційною точкою кіберризиків.

Нижче подано розгорнутий опис кожного каналу:

1. Потік ERP – бухгалтерія

Взаємодія між ERP-системою та бухгалтерією формує основу фінансового обліку підприємства. Саме в ERP створюються первинні документи, відображаються товарні рухи та облік закупівель. Бухгалтерія використовує ці дані для формування проводок, контролю господарських операцій, підготовки податкових документів та регламентованої звітності. Таким чином, ERP акумулює первинну інформацію, а бухгалтерія забезпечує її формальне відображення у фінансових результатах підприємства.

2. Потік ERP/CRM – казначейство

ERP і CRM виступають джерелами критичних довідкових даних – реквізитів контрагентів, історії співпраці, кредитних лімітів та умов договорів. Казначейство використовує ці відомості під час формування та погодження платежів, перевірки IBAN, контролю дебіторської заборгованості та дотримання умов розрахунків. Основні ризики цього потоку пов'язані з можливістю підміни реквізитів у CRM, несанкціонованим коригуванням лімітів або фішинговими, ВЕС-атаками під час погодження платіжних документів.

3. Потік казначейство – банк (клієнт-банк)

Цей канал забезпечує виконання всіх платіжних операцій підприємства. Казначейство формує та підписує платіжні доручення, завантажує банківські виписки, використовує шаблони платежів та проводить додатковий контроль реквізитів перед відправленням коштів. Через критичність цього процесу застосовуються ключові механізми захисту – багатофакторна автентифікація, КЕП, токени, принцип SoD та обмеження доступу до операцій із коштами. Уразливості включають ризики компрометації облікових записів, зміну платіжних доручень, втручання у шаблони або створення підроблених транзакцій.

4. Потік бухгалтерія – державні податкові сервіси

У цьому напрямі відбувається реєстрація податкових накладних, подання звітності та обмін документами з державними електронними сервісами. Усі операції виконуються з використанням КЕП, що забезпечує юридичну силу документів. Основні ризики пов'язані з компрометацією електронного підпису, несанкціонованим доступом до податкових сервісів, підміною чи пошкодженням документів, а також технічними збоями, які можуть спричинити несвоєчасну реєстрацію ПН/РК або блокування звітності.

5. Потік Credit Control – CRM

Цей потік забезпечує доступ Credit Control до інформації про договори, кредитні ліміти, історію оплат та стан дебіторської заборгованості. На основі даних CRM формується оцінка платіжної дисципліни контрагентів та приймаються рішення щодо можливості відвантажень або надання відтермінування. Ключові загрози включають несанкціоновані зміни лімітів, маніпуляції даними про оплату, некоректні акти звірки та підміну договірних умов, що може безпосередньо вплинути на фінансовий результат підприємства.

6. Електронна пошта як канал фінансових комунікацій

Електронна пошта залишається базовим каналом взаємодії з контрагентами, банками та внутрішніми підрозділами. Через e-mail надходять рахунки, підтвердження реквізитів, договори, акти, запити на погодження платежів. Саме ця точка часто використовується для атак через фішинг, шкідливі вкладення, домени-двійники або ВЕС-схеми, коли зловмисники видають себе за керівництво або партнерів. Тому канал потребує посиленого контролю автентичності відправників і додаткових процедур перевірки змін реквізитів.

Оскільки кожен із розглянутих інформаційних потоків фінансового департаменту містить критичні дані та використовується для виконання фінансово значущих операцій, вони потребують посилених механізмів контролю. Саме у цих процесах – під час перевірки реквізитів, внесення змін до довідників, погодження платежів, підписання документів КЕП та обміну інформацією з зовнішніми сервісами і виникає найбільша концентрація ризиків.

Тут найчастіше проявляються помилки персоналу, спроби підміни даних, компрометація облікових записів або технічні збої, що створюють реальні загрози для безперервності фінансових операцій. Для мінімізації цих ризиків у фінансовому контурі застосовується комплекс контрольних заходів. До них належать: розподіл обов'язків у платіжному процесі, багатофакторна автентифікація, підтвердження змін реквізитів через незалежні канали зв'язку, моніторинг аномальної активності, засоби запобігання витоку даних (DLP), а також встановлення показників відновлення та системи KPI/KRI для оцінювання стабільності процесів. Такі механізми дозволяють зменшити ймовірність помилок і зловмисних дій на кожній із точок переходу інформації, забезпечуючи відповідність фінансових процесів принципам управління ризиками, описаним у Розділі 1.

У межах фінансових процесів підприємства ключову роль відіграють контрольні механізми, які забезпечують достовірність операцій, цілісність даних та своєчасне виявлення відхилень. Основними точками контролю, що підтримують безпечне функціонування платіжного контуру, є такі:

По-перше, у платіжному процесі застосовується принцип розподілу обов'язків (SoD), згідно з яким створення, погодження та відправлення платежів виконують різні посадові особи. Це зменшує ризик помилок і навмисних маніпуляцій та забезпечує додатковий рівень перевірки («чотири очі»).

По-друге, зміни банківських реквізитів перевіряються через альтернативний канал зв'язку. Будь-яке коригування IBAN чи контактних даних верифікується телефонним дзвінком за офіційними номерами контрагента, що унеможлиблює використання підроблених повідомлень і знижує ризик ВЕС-сценаріїв.

По-третє, робота з клієнт-банком і ERP супроводжується застосуванням багатофакторної автентифікації та контролем параметрів доступу (пристрої, IP-адреси, геолокація). Це гарантує легітимність користувача та середовища виконання операцій.

Наступним елементом є моніторинг аномальної активності – фіксація входів із незнайомих пристроїв, виконання операцій у нетиповий час або ініціювання платежів на нестандартні суми. Такі індикатори дозволяють своєчасно реагувати на потенційні загрози.

Окреме місце займають DLP-механізми, що запобігають передачі конфіденційних фінансових даних у листуванні та корпоративних чатах, мінімізуючи ризики витоку реквізитів і чутливої інформації.

Крім того, важливою складовою є визначення показників відновлення (RTO/RPO) для платіжного контуру та регулярні навчальні тренування з відновлення безперервності роботи, що забезпечують готовність до інцидентів і технічних збоїв.

Завершальним елементом системи контролю є використання показників KPI та KRI, які дають змогу оцінювати ефективність фінансових процесів та виявляти тенденції зростання ризиків. До ключових індикаторів належать: час погодження платіжних операцій, частота ручних змін реквізитів у довідниках та операційних системах, а також рівень дотримання SLA щодо усунення критичних вразливостей на робочих станціях співробітників фінансового департаменту. Такі метрики забезпечують об'єктивний моніторинг стану безпеки та дозволяють оперативно реагувати на відхилення в роботі платіжного контуру.

Фінансові процеси ТОВ «Спектр-Агро» потребують функціонування системи управління кіберризиками, побудованої відповідно до вимог ISO/IEC 27001, ISO/IEC 27005 та рекомендаціями NIST CSF 2.0. Основою цієї системи є цикл PDCA, який забезпечує послідовне планування заходів безпеки, їх впровадження, перевірку ефективності та подальше вдосконалення.

На етапі Plan визначаються інформаційні активи, формуються критерії оцінювання ризику та встановлюється рівень прийнятного ризику. Етап Do передбачає реалізацію ключових контролів – розподіл обов'язків, багатофакторну автентифікацію (MFA), сегментацію доступів та застосування технічних і організаційних засобів захисту. У межах Check здійснюються

моніторинг роботи контролів, внутрішній аудит та аналіз показників KPI/KRI. Етап Act включає оновлення політик, коригування процесів та підвищення компетентності персоналу відповідно до результатів оцінювання ризиків і змін у зовнішньому середовищі.

Для дієвості PDCA-циклу необхідна чітка організація відповідальності, яка закріплює, хто саме планує, впроваджує, контролює та вдосконалює заходи безпеки у фінансових процесах. У цьому контексті розподіл ролей формує прозору систему підзвітності та забезпечує узгодженість дій усіх учасників. Розподіл ролей забезпечує прозорість відповідальності, у межах якої CFO відповідає за фінансові активи та управлінські рішення щодо їх захисту; CISO формує методологію й координує політику кібербезпеки; керівники фінансових підрозділів забезпечують дотримання вимог у своїх процесах; IT-підрозділ підтримує технічну інфраструктуру та моніторинг подій; внутрішній аудит перевіряє дієвість контролів і надає рекомендації щодо поліпшення. Такий підхід створює цілісну та безперервну систему управління ризиками у фінансовій діяльності підприємства.

Узгодженість ролей і процесів підсилює стійкість фінансового контуру, однак навіть за наявності сформованої системи відповідальності фінансовий департамент залишається найбільш чутливою ланкою організації. Саме тут зосереджені ключові цифрові активи підприємства, такі як: платіжні шаблони, довідники контрагентів, кваліфіковані електронні підписи та доступи до системи клієнт-банк. Будь-яке втручання в ці активи може миттєво перерости у прямі фінансові втрати, що робить цей підрозділ найбільш ризиковою ділянкою бізнесу.

Крім того, фінансові операції напряму впливають на ліквідність підприємства, виконання договірних зобов'язань і дотримання регуляторних вимог. Тому для оцінювання ризиків у цій сфері доцільно застосовувати кількісні методики, такі як ALE чи FAIR (розглянуті у Розділі 1), які дозволяють оцінити потенційні збитки у грошовому вимірі та обґрунтовано визначити пріоритети захисту.

Підсумовуючи наведене, слід зазначити, що фінансовий департамент ТОВ «Спектр-Агро» закономірно визначено центральним об'єктом кібероцінювання, оскільки він концентрує найкритичніші цифрові активи та забезпечує виконання фінансово значущих операцій. Проаналізовано інформаційні потоки між ERP, CRM, клієнт-банком, державними е-сервісами та корпоративною поштою, що формують основні точки ризику для безперервності процесів і цілісності даних. На основі підходів Розділу 1 окреслено необхідні контрольні механізми (SoD, MFA, out-of-band-верифікація реквізитів, DLP, моніторинг аномалій, KPI/KRI, RTO/RPO) та підтверджено доцільність побудови CRMS за логікою PDCA з чітким розподілом ролей (CFO, CISO, керівники фінпідрозділів, IT, внутрішній аудит). З огляду на прямий вплив фінансових операцій на ліквідність і договірні зобов'язання, подальше оцінювання ризиків має спиратися на кількісні методики (зокрема ALE і FAIR), що дозволяють у грошовому вимірі визначити пріоритети захисту та обґрунтувати інвестиції у кібербезпеку.

2.2. Аналіз поточного стану кіберзагроз і вразливостей фінансових процесів підприємства за останні два роки

Для фінансового департаменту ТОВ «Спектр-Агро» у 2024-2025 рр. найбільш характерними стали загрози, властиві підприємствам аграрного сектору з великим документообігом, сезонними піками навантаження та активною взаємодією з банками, логістичними провайдерами та державними сервісами. Сезонність та підвищений обсяг платіжних операцій у періоди посівної й збору врожаю створюють сприятливі умови для зловмисників, які намагаються використати стресові та прискорені робочі процеси компанії.

Для підприємства найбільш критичними залишаються сценарії Business Email Compromise (BEC), що орієнтовані на зміну банківських реквізитів, перехоплення комунікацій із контрагентами та надсилання підроблених рахунків. Особливо високими такі ризики є у періоди сезонного навантаження,

коли співробітники казначейства опрацьовують значні обсяги платежів, а толерантність до «термінових» запитів зростає. Для компанії це створює реальну небезпеку фінансових втрат через несанкціоновані перекази коштів на підроблені рахунки.

Посилює цю проблему й те, що сучасні інструменти штучного інтелекту зробили подібні атаки значно складнішими для виявлення. Поширення ШІ-інструментів призвело до появи фішингових листів, які майже повністю імітують стиль партнерів та постачальників «Спектр Агро». Це стосується передусім підроблених рахунків, накладних чи запитів на зміну IBAN, що надходять у форматах PDF та XLSM із правдоподібними метаданими. Оскільки компанія працює з великою кількістю контрагентів, ризик потрапляння таких документів у процес погодження значно зріс.

Через активне використання клієнт-банк-систем і високий обсяг облікових записів у ERP-/CRM-системах, товариство залишається вразливим до атак, спрямованих на викрадення сесій, паролів та зловживання MFA-повідомленнями. Повторне використання паролів або підтвердження push-запитів «на автоматі» під тиском термінових операцій створюють умови для непомітного втручання в платіжні шаблони й довідники контрагентів.

Фінансові процеси підприємства щоденно залежать від обміну даними між ERP, CRM, банківськими сервісами та державними шлюзами.

Збої або затримки цих інтеграцій у пікові періоди можуть спричинити дублювання платежів, помилки в бюджетуванні та порушення податкових строків. Ризики посилює недостатня прозорість маршрутизації інтеграцій і відсутність повної інвентаризації технічних залежностей.

ТОВ «Спектр-Агро» використовує значну кількість КЕП у бухгалтерії та казначействі, що створює додатковий клас ризиків: неконтрольоване зберігання ключів, застосування КЕП на незареєстрованих робочих станціях, фішингові кампанії під виглядом «оновлення сертифікатів» та підміна ланцюга підписання документів. Через юридичну значущість КЕП такі інциденти можуть призвести до прямих фінансових збитків та юридичних спорів.

Загалом ці тенденції відповідають світовій практиці, де домінують атаки соціальної інженерії, компрометація облікових записів та маніпуляції даними, у той час як масові DDoS часто виступають інструментом відволікання на тлі цільових шахрайських дій.

Проаналізувавши інформаційні потоки «Спектр-Агро» (ERP-бухгалтерія, CRM - казначейство, клієнт-банк, державні сервіси, Credit Control, корпоративна пошта), можна окреслити найактуальніші загрози, що безпосередньо стосуються роботи фінансового департаменту. Кожен із цих каналів має власну специфіку ризиків, які формуються як технічними, так і організаційними чинниками.

Першою критичною ланкою виступає взаємодія між ERP-системою та бухгалтерським обліком. Тут існують ризики несанкціонованого коригування первинних документів, впровадження шкідливих макросів або появи помилок через нестабільну роботу інтеграцій. Такі інциденти здатні спричинити викривлення бухгалтерських даних, формування некоректної звітності та виникнення податкових ризиків, а також можуть призвести до дублювання операцій чи повторного проведення транзакцій.

Наступним стратегічним каналом є обмін даними між ERP/CRM і казначейством, який безпосередньо впливає на точність та безпеку платіжних операцій. У цьому напрямі найсуттєвішими загрозами є підміна банківських реквізитів, неконтрольовані зміни у довідниках контрагентів, коригування кредитних лімітів та здійснення «ручних» винятків у платіжному процесі. Реалізація таких ризиків може спричинити прямі фінансові втрати, порушення платіжної дисципліни та відхилення від затвердженого платіжного календаря ТОВ «Спектр-Агро».

Ще більш критичною точкою є взаємодія казначейства з банківськими сервісами, адже саме тут відбувається фактичний рух коштів. У сегменті роботи з клієнт-банк-системами найпоширеніші ризики пов'язані з компрометацією токенів та засобів автентифікації, непомітним коригуванням реквізитів одержувача під час формування платежів, а також із фішинговими

спробами під виглядом «оновлення безпеки». Через те, що цей канал забезпечує виконання фінансових операцій у реальному часі, він є однією з найпривабливіших цілей для злоумисників.

Паралельно з цим значну групу ризиків формує взаємодія бухгалтерії з державними податковими сервісами. Стабільність цього каналу має критичне значення, оскільки робота бухгалтерії залежить від своєчасності обміну документами з державними шлюзами. Компрометація КЕП, технічні збої або затримки можуть спричинити несвоєчасну реєстрацію податкових накладних, порушення строків подання звітності та потенційні штрафні санкції

Окремим важливим напрямом є взаємодія підрозділу Credit Control з CRM-системою, що визначає коректність управління дебіторською заборгованістю. Тут ризики зосереджені навколо можливих маніпуляцій кредитними лімітами, підробки актів звірки або некоректного внесення даних щодо історії оплат. Наслідком таких дій можуть бути хибні управлінські рішення щодо відвантажень та зростання простроченої дебіторської заборгованості.

Завершальною, але не менш критичною ланкою є корпоративна електронна пошта, яка є ключовим каналом комунікації фінансового департаменту й водночас основною точкою входу для соціально-інженерних атак (зокрема ВЕС, шкідливі вкладення, домени-двійники). Їхня мета – підміна реквізитів, перехоплення фінансового листування та втручання в ланцюги погодження документів, що створює значні ризики для цілісності фінансових процесів.

Аналіз роботи фінансового контуру підприємства дає змогу виокремити кілька груп вразливостей, які впливають на рівень кіберстійкості. Вони охоплюють організаційні, процесні, технічні аспекти та ризики, пов'язані з поведінкою працівників.

До організаційних недоліків належать недоопрацьовані процедури та прогалини у правилах безпеки, що створюють сприятливі умови для реалізації загроз. Серед ключових проблем можна зазначити такі як: відсутність

обов'язкового незалежного каналу підтвердження змін реквізитів контрагента (out-of-band-верифікації); неповне ведення журналу перевірок IBAN, що ускладнює подальший аудит операцій; нечіткий розподіл ролей і відповідальності (RACI) щодо оновлення довідників; різний рівень обізнаності співробітників у сфері кібербезпеки, що впливає на якість виконання контрольних процедур.

У процесах фінансового департаменту простежуються регулярні відхилення від встановлених процедур, зокрема застосування «ручних» винятків у платіжному циклі, обмін фінансовими документами через месенджери без формального контролю метаданих, недостатня періодичність перевірки розподілу обов'язків (SoD-рев'ю) та схильність персоналу обходити окремі контролі в умовах сезонного навантаження та браку часу.

Технічні вразливості проявляються у недостатньо чіткій сегментації доступів у бізнес-системах, відсутності централізованого аналізу логів, неповній інвентаризації інтеграцій та використанні КЕП на пристроях без підтвердженої безпечності.

Людський фактор залишається одним із головних джерел кіберризиків, оскільки працівники часто потрапляють на фішингові повідомлення, поспішають під час погодження платежів та використовують слабкі або повторювані паролі. Крім того, значна частина інцидентів виникає через неуважність до ознак шахрайства в електронних листах, зокрема нетипових формулювань чи сумнівних доменів.

Ураховуючи суттєвий вплив людського чинника на рівень безпеки фінансових процесів, виникає потреба у системній оцінці ризиків, що й було реалізовано за допомогою напівкількісного підходу. Для первинного ранжування кіберризиків у фінансових процесах застосовано матрицю $P \times I$ (ймовірність $\times$ вплив) за шкалою 1-5, відповідно до методичного підходу, викладеного у Розділі 1. Нижче подано узагальнений результат оцінювання, який відповідає критичності активів ТОВ «Спектр-Агро», визначених у розділі 2.1.

1. Зміна IBAN контрагента внаслідок ВЕС-атаки або фішингу оцінюється як критичний ризик ($P=4-5$; $I=5$), оскільки такі інциденти трапляються часто й призводять до прямих фінансових втрат та суттєвих репутаційних і юридичних наслідків.
2. Компрометація робочого облікового запису казначейства чи бухгалтерії має дуже високий рівень ризику ($P=3-4$; $I=5$), що зумовлено втомою від MFA-запитів, повторним використанням паролів та ймовірністю непомітного коригування шаблонів платежів.
3. Втрати або незаконне використання КЕП класифікуються як дуже високий ризик ($P=3$; $I=5$), оскільки електронний підпис надає юридичну силу будь-якій дії та створює можливість несанкціонованого оформлення фінансових документів.
4. Порухення роботи інтеграцій ERP із банком або державними сервісами становлять дуже високий або високий ризик ($P=3-4$; $I=4$), адже можуть спричинити затримки платежів, появу дублюючих операцій і порушення регламентованих строків.
5. Несанкціоновані зміни у CRM/ERP (довідники, кредитні ліміти) визначені як високий ризик ($P=3$; $I=4$), оскільки такі втручання здатні впливати на кредитну політику та формувати опосередковані фінансові збитки.
6. Шкідливі вкладення у форматах PDF або XLSM, отримані через електронну пошту, несуть високий рівень ризику ($P=4$; $I=3-4$), адже можуть призвести до зараження робочих станцій, викрадення сесій чи доступу до чутливих фінансових даних.

Матриця $P \times I$ дозволила визначити ризики, які мають найбільший вплив на безперервність і безпеку фінансових операцій. Однак для прийняття управлінських рішень такої оцінки недостатньо, тому наступним етапом є деталізація ключових сценаріїв за методикою NIST SP 800-30, що дає змогу проаналізувати логіку атаки, чинники успішності та можливі наслідки для ТОВ «Спектр-Агро».

У контексті отриманих результатів першочергової уваги потребує Сценарій А, що стосується підміни банківських реквізитів у результаті ВЕС-атаки, оскільки саме цей тип інцидентів демонструє найвищий рівень імовірності та потенційного фінансового впливу. У цьому сценарії загроза походить від зовнішнього зловмисника, який перехоплює електронне листування та видає себе за контрагента, використовуючи домени-двійники або підроблені рахунки. Основні вразливості для «Спектр Агро» – це відсутність обов’язкової out-of-band перевірки реквізитів, неповне ведення журналу IBAN-підтверджень та відсутність посиленої верифікації для нетипових змін. Наслідками таких атак можуть бути прямі фінансові втрати та репутаційні ризики. Попри наявні контролі (SoD, подвійне погодження, SPF/DKIM/DMARC, DLP), ризик залишається високим у сезон пікового навантаження, коли зростає ймовірність помилкового погодження. Попри високу критичність Сценарію А, він не є єдиною загрозою для фінансового департаменту.

Наступним суттєвим ризиком, який демонструє значну ймовірність реалізації, є Сценарій В – компрометація облікового запису працівника казначейства, що може стати точкою входу для маніпуляцій платіжними операціями та змінами у фінансових системах. Загроза виникає через фішинг та «втому MFA», що спонукає працівника підтверджувати сторонні запити. Слабкими місцями є повторне використання паролів, відсутність прив’язки акаунта до конкретного пристрою та недостатність мережевих обмежень. Це створює можливість прихованої зміни шаблонів платежів, проведення транзакцій поза лімітами та маніпуляцій у довідникових даних. Хоча впроваджено посилений MFA, політику паролів, роботу лише з авторизованих станцій та гео/ASN-фільтри, залишковий ризик залишається середньо-високим без централізованої кореляції подій у XDR/SIEM. Однак низка критичних загроз пов’язана не лише з доступами до систем, а й з інструментами, що мають юридичну силу.

Саме тому наступним кроком є аналіз Сценарію С – втрати або компрометації КЕП працівників фінансового департаменту. Для «Спектр-Агро» ризик, пов'язаний із кваліфікованими електронними підписами, є одним із найчутливіших, адже КЕП використовується для підписання платежів, податкових документів та юридично значущих матеріалів. Загрози виникають у двох основних формах: отримання зловмисником доступу через фішингові розсилки («оновлення сертифіката») або фізична втрата носія. Вразливості включають використання ключів на неперевірених пристроях та відсутність повного обліку їх життєвого циклу. Потенційний вплив – це можливість підписання сторонніх або фальсифікованих документів від імені компанії. Контрзаходи передбачають реєстр видачі та блокування КЕП, облік робочих станцій, шифрування носіїв, двоетапний контроль для критичних операцій та політику заборони використання особистих пристроїв. Без регулярних аудитів залишковий ризик залишається суттєвим.

Розгляд ключових сценаріїв А, В та С дав змогу визначити, у яких точках фінансового контуру ТОВ «Спектр-Агро» виникають найбільш критичні загрози та фактори, які впливають на їхню успішність. Однак для забезпечення сталого та передбачуваного управління ризиками недостатньо лише ідентифікувати потенційні інциденти, а необхідно мати механізм постійного контролю їх динаміки.

Саме тому наступним кроком є формування системи KRI та KPI, що у фазі Check циклу PDCA дає змогу в реальному часі відстежувати динаміку ризику та оцінювати ефективність запроваджених контролів. У фінансових процесах ці показники виступають інструментами постійного моніторингу, які своєчасно виявляють небезпечні тенденції та показують, наскільки дієвими є заходи безпеки. У межах системи управління ризиками розрізняють два типи метрик: KRI (сигналізують про потенційні загрози) та KPI (відображають фактичну результативність контролів).

Основні KRI для фінансового контуру ТОВ «Спектр -Агро»:

1. частка платежів із ручною зміною реквізитів (індикатор можливих підмін IBAN);
2. кількість листів, що не пройшли SPF/DKIM/DMARC (ознака ризику BEC-атак);
3. входи у клієнт-банк із нових пристроїв або незвичних мереж (сигнал можливої компрометації);
4. кількість критичних вразливостей на робочих станціях фінансових співробітників, не усунених у строк.

Ключові KPI ефективності контролів:

1. частка операцій із незалежною перевіркою банківських реквізитів;
2. час виявлення та блокування BEC-сценарію;
3. регулярність SoD-рев'ю у платіжному процесі та частка усунених порушень;
4. відсоток співробітників, що успішно пройшли антифішингове навчання.

Завдяки цим показникам фінансовий департамент отримує «систему раннього попередження» і переходить від реактивного до проактивного управління ризиками, де тенденції фіксуються до того, як вони вплинуть на платіжні чи облікові процеси, а стабільність операцій підтримується на заданому рівні.

На наступному етапі доцільно узагальнити типові зв'язки між загрозами, вразливостями, наслідками та контрольними заходами. Для цього застосовано матричний підхід, що систематизує ключові сценарії та дозволяє визначити пріоритетні зони посилення.

У межах аналізу ключових сценаріїв було сформовано узагальнену матрицю, яка демонструє логіку розвитку ризику— від джерела загрози до вразливого етапу процесу, очікуваних наслідків та відповідних заходів їх мінімізації. Особливо показовим є блок електронних комунікацій та змін реквізитів — BEC і фішингові атаки виникають тоді, коли реквізити не проходять незалежної перевірки, що створює ризик підміни IBAN і шахрайських платежів. Протидіяти цьому допомагають SoD, подвійне погодження, автентифікація відправників і DLP-політики.

Не менш важливою складовою кіберстійкості є контроль за доступами у фінансових системах. Компрометація робочих облікових записів часто виникає через слабкі або повторювані паролі та перевантаження користувачів MFA-запитами. Зменшити такий ризик допомагають посилені правила автентифікації, застосування географічних і мережевих фільтрів, а також використання поведінкової аналітики, що виявляє нетипові дії.

Окремої уваги потребує й безпечне використання кваліфікованих електронних підписів. Запобігти підписанню фіктивних чи підроблених документів дозволяють ведення реєстру ключів, перевірка пристроїв, на яких ці ключі застосовуються, а також додаткове підтвердження операцій, що мають юридичне значення.

Стабільність інтеграцій ERP/CRM з банками та держсервісами є критичною: збої призводять до дублювання платежів, затримок і облікових помилок; ризики зменшують інвентаризація інтеграцій, контроль цілісності даних і резервні канали.

Також існує ризик несанкціонованих внутрішніх змін у CRM/ERP, якщо логування недостатнє, а доступи надмірні. Зменшити його дозволяють детальна історія змін, чітке розмежування ролей і регулярний перегляд прав користувачів.

У сукупності матриця дозволяє структуровано бачити ризикові сценарії й визначати, які елементи управління потребують першочергової модернізації, закладаючи основу для наступного підрозділу з побудови комплексної системи контролю.

Проведений аналіз показав, що у 2024-2025 рр. фінансові процеси ТОВ «Спектр Агро» перебувають під впливом широкого спектра взаємопов'язаних кіберзагроз. Найбільш критичними серед них є сценарії, пов'язані з підміною реквізитів у результаті ВЕС-та фішингових атак, компрометацією робочих облікових записів та кваліфікованих електронних підписів, а також збої у взаємодії між ERP, CRM, клієнт-банком та державними сервісами. Формування ризикового профілю демонструє, що вразливості мають переважно

організаційно-процесний характер – недосконалі процедури перевірок, обмеження SoD, недостатня фіксація змін, та суттєво підсилюються технічними чинниками, такими як недоліки сегментації доступів, відсутність глибокої кореляційної аналітики чи повної інвентаризації інтеграцій. Важливу роль відіграє і людський фактор, який особливо загострюється в періоди сезонних навантажень. Застосування напівкількісної моделі ISO/IEC 27005 (P×I) підтвердило, що сценарії підміни IBAN, компрометації облікових записів та КЕП мають критичний або дуже високий рівень ризику, тоді як інтеграційні збої та внутрішні маніпуляції у CRM/ERP оцінюються як ризики високого рівня. Сукупність отриманих результатів формує обґрунтовану методологічну основу для подальшої кількісної оцінки ризиків у наступному розділі та визначення пріоритетних напрямів посилення кіберстійкості фінансового контуру підприємства.

2.3. Практичне застосування методик оцінки кіберризиків на фактичних даних ТОВ «Спектр-Агро»

Метою цього підрозділу є демонстрація практичної процедури оцінювання кіберризиків фінансових процесів ТОВ «Спектр-Агро» на основі узагальнених внутрішніх показників. Аналіз виконується поетапно:

1. спершу за напівкількісною матрицею $P \times I$ визначаються найбільш ризикові сценарії;
2. далі застосовується кількісна модель ALE (Annual Loss Expectancy) для грошової оцінки очікуваних наслідків;
3. на завершення, на прикладі найкритичнішого сценарію демонструється підхід FAIR, який розділяє частоту настання подій та структуру можливих втрат, уточнюючи управлінські пріоритети.

Для проведення аналізу використано агреговані показники за 2024-2025 роки, які не розкривають комерційно чутливої інформації про діяльність

підприємства. До розгляду включено такі характеристики фінансових операцій та інцидентів інформаційної безпеки:

1. Платіжна активність. У середньому за місяць опрацьовувалося від 2 900 до 3 700 вихідних платежів, при цьому діапазон середньої суми однієї операції становив 48 000-62 000 грн, а максимальні разові платежі коливалися у межах 900 000-1 600 000 грн.
2. Коригування реквізитів. Частка платежів, у яких здійснювалися ручні зміни платіжних реквізитів, перебувала на рівні 0,8-1,4%. Питома вага нових контрагентів у загальній структурі становила приблизно 3-6% на місяць.
3. Спроби фішингових і ВЕС-атак. Кількість виявлених інцидентів соціальної інженерії коливалася у межах 6-14 випадків на місяць, із яких 0-2 переходили до етапу погодження, але блокувалися чинними контрольними механізмами. Успішні інциденти траплялися поодинокі.
4. Компрометація облікових записів. Середньомісячна кількість спроб несанкціонованого доступу, включно з атаками типу MFA fatigue, становила 4-11 подій. Успішні випадки характерні як 0 або 1 на квартал, і зазвичай не призводили до фінансових втрат завдяки принципу розподілу обов'язків (SoD) та багатофакторній автентифікації.
5. Події, пов'язані з КЕП. Порушення, пов'язані з кваліфікованими електронними підписами (втрата носія, підозрілі операції підписання), фіксувалися з періодичністю 0-2 на квартал. Прямих фінансових збитків не виявлено, однак такі випадки потребували додаткових перевірок і підтверджень.
6. Стабільність інтеграцій із зовнішніми сервісами. У взаємодії ERP-системи з банківськими сервісами та державними шлюзами реєструвалися короткочасні збої з частотою 2-5 разів на квартал, тривалістю від 25 до 90 хвилин, що спричиняло помітний вплив насамперед у періоди пікового навантаження.

З урахуванням специфіки діяльності фінансового департаменту, характеру основних інформаційних потоків підприємства (ERP, CRM, клієнт-банк, державні електронні сервіси, корпоративна електронна пошта), а також

виявлених типових вразливостей, описаних у попередніх підрозділах, було визначено шість ключових сценаріїв кіберризиків, найбільш релевантних для подальшої оцінки. До них належать:

1. А. Спроби ВЕС/фішингу, спрямовані на підміну реквізитів IBAN у рахунках або листуванні з подальшим ризиком погодження неправомірного платежу.
2. В. Компрометація корпоративного облікового запису працівників казначейства чи бухгалтерії, що створює можливість несанкціонованого втручання у платіжні шаблони або довідникові дані.
3. С. Використання або зловживання КЕП, коли електронний підпис застосовується сторонньою чи неуповноваженою особою для підтвердження документів або податкових накладних.
4. D. Порушення роботи інтеграцій між ERP-системою, банківськими сервісами та державними шлюзами, особливо у періоди пікового навантаження, що може призводити до дублювання або затримки платежів та недотримання строків.
5. Е. Несанкціоновані коригування довідникової інформації у ERP/CRM, зокрема даних контрагентів або кредитних лімітів, наслідком чого можуть бути опосередковані фінансові втрати.
6. F. Надходження шкідливих вкладень у форматах PDF/XLSM, які можуть стати джерелом зараження робочої станції, викрадення сесій та ініціювання шахрайських операцій.

Для кожного зі сценаріїв було проведено напівкількісне оцінювання ризику шляхом визначення ймовірності (Р) та ступеня впливу (І) за п'ятибальною шкалою, із подальшим коротким обґрунтуванням отриманих значень. Після цього три сценарії з найвищими показниками критичності були відібрані для подальшого кількісного аналізу методом ALE, що дозволило здійснити фінансову оцінку можливих наслідків їх реалізації.

Для первинного ранжування кіберризиків фінансових процесів було застосовано напівкількісний підхід, що передбачає оцінювання рівнів ймовірності (Р) та впливу (І) кожного сценарію за п'ятибальною шкалою. На

основі отриманих показників сформовано матрицю ризиків, яка наведена в таблиці 2.3 та відображає відносне розміщення розглянутих сценаріїв.

Таблиця 2.3

Матриця ризиків($P \times I$) для сценаріїв А-Е (шкала 1-5)

Примітка: P –імовірність (1–5), I –вплив (1–5), $R=P \times I$ –індекс пріоритетності.

Код	Сценарій	Короткий опис	P (1–5)	I (1–5)	$R=P \times I$	Коротке обґрунтування	Пріоритет
А	ВЕС/фішинг – підміна IBAN	Підміна IBAN у рахунках і листуванні з ризиком погодження неправомірного платежу	5	5	25	Часті спроби у пікові періоди; у разі успіху – прямі фінансові втрати та репутаційні наслідки	Високий
В	Компрометація облікового запису	Доступ до акаунта (казначейство/бухгалтерія) з можливістю змін шаблонів/довідників	4	5	20	Імовірність зростає через «втому МФА»; вплив високий через пряме втручання у платіжні процеси	Високий
Д	Збої інтеграцій ERP-банк-держсервіси	Затримки/дублювання платежів, порушення строків у пік навантаження	4	4	16	Регулярні короткі збої; у сезон наслідки відчутні для строків і операційної безперервності	Високий

Продовження таблиці 2.3

Е	Шкідливі вкладення (PDF/XLSM)	Ризик зараження робочих станцій, викрадення сесій, шахрайські дії	4	4	16	Спроби трапляються; вплив залежить від швидкості виявлення та стримуючих контролів	Середньо-високий
С	Використан-	Підписання	3	5	15	Рідші	Середньо

	ня/ зловживання КЕП	документів/ ПН неуповнова- женою особою				інциденти, але у разі реалізації наслідки юридично значущі	-високий
Е	Несанкціо- новані зміни у довідниках ERP/CRM	Зміни даних контрагентів/ кредитних лімітів з непрямими втратами	3	4	12	Непрямий вплив через хибні рішення/пом илки в операціях, що акумулю- ються	Середній

Джерело: розроблено автором

За підсумками матриці $P \times I$ сценарії А, В та D мають найвищі значення індексу R і, відповідно, відібрані для кількісної оцінки за методикою ALE , а також подальшої деталізації елементів частоти/збитків у логіці FAIR.

Інтерпретація результатів:

Сценарій А (ВЕС/зміна реквізитів IBAN), $P=5$, $I=5$. Належить до групи найвищої критичності, оскільки у разі реалізації безпосередньо створює ризик значних прямих фінансових втрат, а також супроводжується відчутними репутаційними наслідками для підприємства.

Сценарій В (компрометація облікового запису), $P=4$, $I=5$. Рівень імовірності зростає у періоди підвищеного операційного навантаження, зокрема через ефект «втоми від MFA». Потенційний вплив зберігається на високому рівні, адже несанкціонований доступ може призвести до маніпуляцій із платіжними документами та критичними даними.

Сценарій D (збої інтеграцій), $P=4$, $I=4$. Основну загрозу становлять порушення строків виконання операцій, можливість дублювання платежів та операційні втрати, що найбільш помітні в сезонні піки навантаження.

Сценарії F та E. Попри нижче розташування в матриці, залишаються релевантними для контролю: F пов'язаний із ризиком зараження робочих станцій та подальшим втручанням у фінансові процеси, тоді як E відображає небезпеку спотворення довідникової інформації, що впливає на коректність облікових і платіжних операцій.

Отримані оцінки дозволяють виокремити А, В та D, як пріоритетні сценарії для подальшого поглибленого аналізу з використанням ALE і FAIR, що дає змогу кількісно обґрунтувати очікувані втрати та визначити першочергові заходи мінімізації ризиків. У подальшому викладі зосередимося саме на цих трьох сценаріях.

Відповідно до обраної методики, для А, В та D виконано кількісну оцінку за моделлю ALE (Annual Loss Expectancy). Розрахунки проведено за формулою $ALE = SLE \times ARO$, де $SLE = AV \times EF$ (див. формули 1.3, 1.4), з урахуванням особливостей фінансових операцій підприємства. Зведені результати подано у таблиці 2.4, яка демонструє співвідношення параметрів AV, EF, SLE, ARO та підсумкові значення ALE для кожного сценарію (див. табл. 2.4).

Таблиця 2.4

Розрахунок ALE для пріоритетних сценаріїв

Сценарій	Короткий опис	AV (грн)	EF	SLE = AV × EF, грн	ARO (подій / рік)	ALE = SLE × ARO (грн/рік)	Чинні ключові конт-ролі	Висновок
А	ВЕС – підміна ІВА N у платіжці	400 000	0,35	140 000	0,40	56 000	SoD, подвійне погодження, out-of-band верифікація змін реквізитів, DLP, DMARC	Найвищий пріоритет; навіть за невеликої ARO очікуваний збиток суттєвий

Продовження таблиці 2.4

B	Компрометація акаунта казначейства/бухгалтерії	250 000	0,30	75 000	0,80	60 000	MFA, гео/ASN-фільтри, доступ лише з корпоративних станцій, журнали аномалій	Пріоритет високий; частота вища, ніж у А
D	Збій інтеграцій ERP-банк/держсервіси (пік)	180 000	0,25	45 000	1,60	72 000	RTO/RPO, ретрайчерг, дубльканал, моніторинг API	Найбільший ALE через вищу частоту; критично в піки

Джерело: розроблено автором

Отримані значення ALE можуть бути використані як основа для планування бюджету на заходи кібербезпеки та оцінки їх економічної доцільності.

Нижче наведено обґрунтування використаних параметрів для кожного з трьох пріоритетних сценаріїв.

Сценарій А – BEC / підміна реквізитів IBAN.

Основний ризик стосується вихідних платежів, середня сума яких зазвичай становить близько 55 000 грн. Найуразливішою категорією є великі перекази понад 300 000 грн. З огляду на це AV прийнято як «середній масштаб потенційної втрати» 400 000 грн. Частка можливих безповоротних втрат (EF) оцінена на рівні 0,35, що враховує як ймовірність негайного списання коштів, так і можливість часткового повернення банком у разі швидкого виявлення інциденту. Очікувана частота подібних випадків (ARO) становить приблизно 0,4 на рік, що відповідає одному суттєвому інциденту орієнтовно раз на 2,5 року за чинних механізмів контролю.

Сценарій В – компрометація робочого акаунта.

У цьому сценарії шкода пов'язана передусім із ризиком зміни платіжних шаблонів, довідкових даних або створення разових несанкціонованих платежів. Виходячи з цього, AV визначено як 250 000 грн – умовна оцінка можливого впливу на платіжний контур за одноразову подію. Частка втрати (EF) прийнята на рівні 0,30, оскільки на практиці ризик суттєво зменшується через застосування багаторівневих контролів (SoD, ліміти, подвійне погодження). Щодо частоти (ARO), зафіксована періодичність імовірних інцидентів дозволяє застосувати орієнтир 0,8 на рік, що відповідає приблизно одному інциденту на 15 місяців.

Сценарій D – збої інтеграцій між ERP, банківськими сервісами та державними шлюзами.

У цьому випадку шкода виникає внаслідок операційних затримок, дублювання транзакцій або зриву строків реєстраційних дій. Вартісний еквівалент впливу одного інциденту AV оцінено на рівні 180 000 грн, що відповідає типовим втратам продуктивності та витратам на усунення наслідків. Параметр EF становить 0,25, оскільки не кожен збій призводить до фінансових наслідків – частина збоїв має короткостроковий або технічно компенсований характер. ARO прийнято рівним 1,6 на рік, що відповідає приблизно одному значущому інциденту раз на 7-8 місяців.

Ключове спостереження – попри те, що A (BEC) часто сприймається як найбільш загрозливий сценарій, у межах цього аналізу найвищий річний очікуваний збиток (ALE) формує D (інтеграції) за рахунок вищої частоти (ARO). Це типовий результат кількісної оцінки, коли частота подій здатна «переважити» тяжкість одиничного інциденту.

Для ілюстрації підходу FAIR розглянемо сценарій A та розкладемо його на ключові складові (спрощено):

1. TEF (Threat Event Frequency) – орієнтовна частота релевантних подій (цільові звернення щодо зміни IBAN, які доходять до етапу погодження) – близько 3 подій на рік.

2. V (Vulnerability) – імовірність успішної реалізації однієї такої події за наявності чинних контролів (SoD, out-of-band-перевірка, навчання персоналу) – приблизно 0,12.
3. LEF (Loss Event Frequency) – очікувана частота інцидентів втрат–
 $LEF = TEF \times V = 3 \times 0,12 = 0,36$ події/рік, що співвідноситься за порядком величини з ARO у розрахунках ALE.
4. PL (Primary Loss) – прямі фінансові втрати на один успішний випадок, у межах 130 000 - 220 000 грн (типові орієнтири мін/мода/макс; модальне значення – близько 160 000 грн).
5. SL (Secondary Loss) – непрямі витрати (операційні, репутаційні, правові): орієнтовно 40 000 -120 000 грн (мода – приблизно 70 000 грн).
6. LM (Loss Magnitude) – сукупний масштаб втрат за подію: $LM = PL + SL$ близько 200 000 - 340 000 грн (мода – близько 230 000 грн).
7. Очікуваний річний ризик за FAIR: $Risk = LEF \times LM = 0,36 \times 230\,000 \text{ грн} =$ близько 82 800 грн/рік.

Варто зазначити, що різниця між оцінками, отриманими за методами ALE та FAIR, зумовлена відмінностями у підходах до розрахунку: модель ALE використовує середні оцінки втрат і частоти подій, тоді як FAIR враховує більш деталізовану структуру збитків, включаючи непрямі (secondary) наслідки та модальні значення втрат.

Оскільки підхід FAIR дозволяє розвести в моделі частоту подій та масштаб збитків, чітко окреслюючи точки впливу контролів (зокрема, зниження V завдяки посиленню out-of-band-перевірок та дисципліни погоджень), логічним наступним кроком є узгодження цих висновків із кількісними оцінками за ALE. Далі подано розподіл очікуваних річних збитків (ALE) для пріоритетних сценаріїв А, В та D, візуалізація якого дає змогу встановити послідовність управлінських дій і обґрунтувати розподіл ресурсів (див. рис. 2.1).

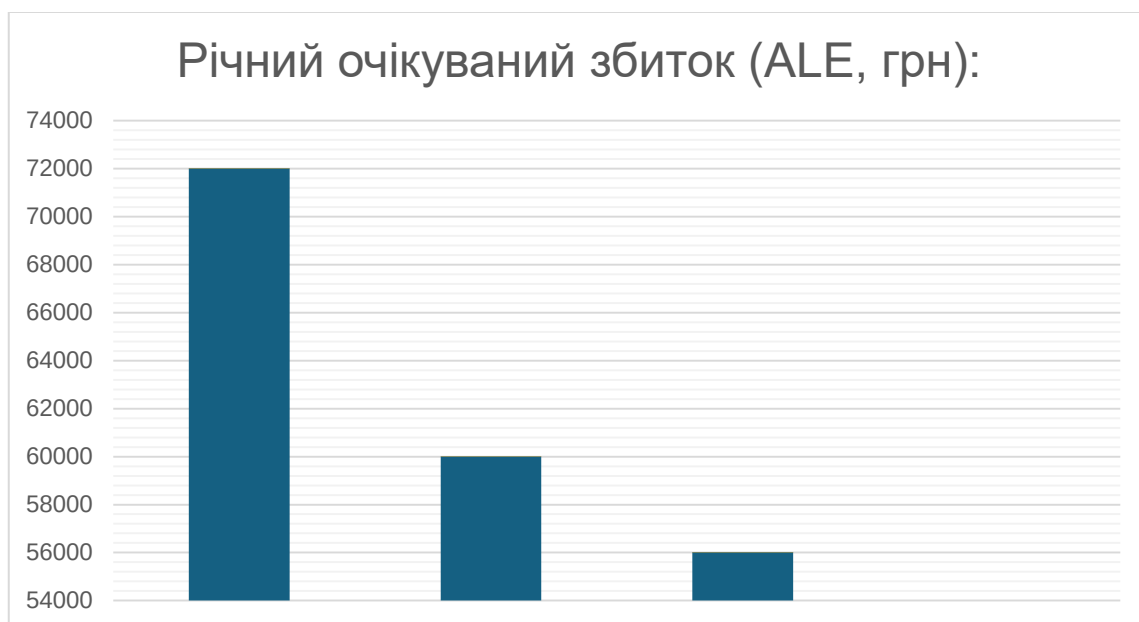


Рисунок 2.1 – Діаграма пріоритетів за ALE

Джерело: розроблено автором

Найбільший очікуваний річний вплив демонструє сценарій D (збої інтеграцій), що зумовлює необхідність посилення механізмів стійкості інтеграційних потоків (удосконалення ретрай-логіки, використання резервних каналів, налаштування оперативних алертів, формалізація дій у пікові періоди). Сценарій B (компрометація облікового запису) зберігає високий пріоритет через ризик прямого втручання у платіжні та довідникові процеси; доцільно зміцнити гігієну MFA, скоротити тривалість сесій, обмежити пристрої/локації доступу і проводити регулярні SoD-рев'ю. Сценарій A (BEC/зміна IBAN) потребує додаткових гарантій достовірності платіжної інформації (обов'язкові out-of-band-перевірки змін реквізитів, стандартизовані шаблони підтверджень, «step-up»-валідація для нетипових платежів).

Зведені результати демонструють, що хоча всі три сценарії належать до високопріоритетних, саме D, B та A формують ключовий внесок у сумарний річний ризик і вимагають першочергового управлінського реагування.

Зіставлення FAIR і ALE дозволило виділити критичні сценарії та їхній внесок у сукупний ризик. Наступним кроком є оцінювання того, наскільки змінною є ця ієрархія під впливом ключових параметрів, тому для цього виконаємо перевірку чутливості та визначимо пріоритетні управлінські кроки.

Аналіз чутливості параметрів (what-if):

Сценарій А (BEC). За умови зростання ARO із 0,40 до 0,80 (наприклад, через сезонне підвищення навантаження або зниження дисципліни перевірок) очікуваний річний збиток ALE(A) подвоюється приблизно до 112 000 грн/рік, що виводить цей сценарій на перше місце за критичністю, випереджаючи В та D.

Сценарій D (інтеграції). Запровадження резервного каналу обміну та оптимізація ретраїв дозволяють знизити ARO з 1,60 до 0,70, унаслідок чого ALE(D) зменшується з 72 000 близько до 31 500 грн/рік. Це забезпечує найвищу віддачу на інвестиції серед розглянутих коригувань.

Сценарій В (акаунт). Зменшення EF із 0,30 до 0,20 (за рахунок жорсткіших лімітів, принципу «чотирьох очей» та оперативних сповіщень) знижує ALE(B) з 60 000 близько до 40 000 грн/рік.

Управлінські пріоритети на 6 -12 місяців:

1. Стійкість інтеграцій (D). Налаштувати черги ретраїв, передбачити дублюючі канали для ключових потоків (платежі/ПН), проводити квартальні тести відновлення, оновити SLA із провайдерами з чіткими метриками доступності та часу реакції.
2. Дисципліна доступів (B). Максимально мінімізувати привілеї, обмежити пристрої/локації для доступу, упровадити заходи протидії MFA-fatigue (номерні підтвердження, частотні ліміти запитів), скоротити час життя сесій.
3. Out-of-band-перевірки (A). Зробити обов'язковою альтернативну перевірку для будь-яких змін реквізитів IBAN/контактів; вести журнал підтверджень, застосовувати типові шаблони та проводити додаткову step-up-валідацію для нетипових сум або нових одержувачів.
4. Антифішинг і безпека контенту (F). Проводити щоквартальні навчання та фішинг-симуляції, блокувати макроси за замовчуванням, використати «пісочницю» (sandbox) для перевірки вкладень.
5. SoD-рев'ю та аудит журналів (E, B). Запровадити щомісячний огляд платіжного контуру: контроль розподілу обов'язків, аналіз журналів доступу/змін.

Встановити цілі KPI/KRI: частка платежів із ручною зміною реквізитів – < 0,5%; кількість критичних CVE понад SLA – 0.

6. Регулярні вправи з відновлення (D). Перевіряти RTO/RPO у практичних сценаріях («відкат», повторна відправка, звірка), із фіксацією уроків та корекцією процедур.

З огляду на це, можна зробити висновок, що результати чутливості підтверджують пріоритетність інвестицій у стійкість інтеграцій (D), зміцнення керування доступами (B) та підсилення out-of-band-перевірок (A), оскільки саме ці дії забезпечують найвагоміше зниження очікуваного річного збитку та ризику операційних збоїв.

Наведені оцінки сформовано на основі агрегованих внутрішніх показників і експертних припущень щодо параметрів AV/EF/ARO (для моделі ALE) та TEF/V/PL/SL (для підходу FAIR). Для коректного виробничого використання потрібні регулярна калібрація цих параметрів на підставі журналів подій і перегляд сезонних ефектів. Рекомендовані KPI/KRI для безперервного нагляду: частка платежів із ручною зміною реквізитів (ціль – < 0,5%), частка нетипових сум із «step-up» – валідацією, час відновлення інтеграції (RTO), допустима втрата даних (RPO) та дотримання SLA щодо усунення критичних уразливостей на робочих станціях фінансового департаменту. Значення KPI/KRI переглядаються щоквартально в межах PDCA-циклу, з урахуванням сезонності та результатів тестів відновлення/інцидентів.

У розділі проведено практичну оцінку кіберризиків фінансових процесів ТОВ «Спектр-Агро» із послідовним застосуванням трьох підходів: $P \times I$ для первинного ранжування, ALE для грошової оцінки та FAIR для розділення частоти подій і структури втрат. Така логіка дозволила перейти від загальної карти загроз до конкретних управлінських рішень.

Матриця $P \times I$ визначила трійку пріоритетів: A (BEC/підміна IBAN), B (компрометація облікового запису), D (збої інтеграцій). Розрахунки ALE показали, що найбільший очікуваний річний збиток формує D за рахунок вищої

ARO, далі – B, тоді як A має нижчий річний ефект попри високу тяжкість одиначної події. Аналіз FAIR для сценарію A вказав практичні точки впливу – зниження V через out-of-band-перевірки та дисципліну погоджень, а також зменшення SL завдяки стандартизації реагування.

Перевірка чутливості підтвердила, що найбільше скорочення очікуваних втрат забезпечують: підвищення стійкості інтеграцій (ретрай-черги, дубль-канали, моніторинг API), зміцнення керування доступами (SoD, MFA, ліміти, алерти) і підсилення платіжних перевірок поза електронною поштою (out-of-band, step-up). Запропоновані кроки зменшують очікуваний річний збиток і підвищують кіберстійкість фінансового контуру, а регулярна калібрація параметрів і моніторинг KPI/KRI забезпечують безперервне удосконалення в логіці ISMS/CRMS.

Висновок до розділу 2

У розділі 2 виконано аналітико-дослідницьку оцінку кіберризиків фінансових процесів ТОВ «Спектр-Агро», що дозволило сформувати цілісне уявлення про стан кіберстійкості фінансового департаменту підприємства. Аналіз проведено на основі методологічних підходів ISO/IEC 27005, NIST CSF 2.0 та циклу PDCA, що забезпечило системність і практичну спрямованість дослідження.

У підрозділі 2.1 фінансовий департамент обґрунтовано визначено як центральний об'єкт кібероцінювання, оскільки в його межах концентруються найбільш критичні цифрові активи підприємства – платіжні операції, довідники контрагентів, КЕП та доступи до ERP, CRM і клієнт-банку. Проаналізовано структуру фінансових підрозділів, основні інформаційні потоки та галузеву специфіку діяльності компанії, що характеризується сезонними піками навантаження. Напівкількісне ранжування активів за моделлю RхI дозволило виокремити активи з критичним і дуже високим рівнем впливу та визначити пріоритети їх захисту.

У підрозділі 2.2 проаналізовано актуальні кіберзагрози й вразливості фінансових процесів у 2024-2025 рр. Встановлено, що ключовими ризиками є ВЕС-атаки та фішинг із підміною реквізитів, компрометація облікових записів і КЕП, а також збої інтеграцій між ERP, банківськими й державними сервісами. Показано, що вразливості мають комплексний характер і поєднують організаційно-процесні недоліки, технічні обмеження та вплив людського чинника, який посилюється в умовах сезонного навантаження. Оцінка за моделлю ISO/IEC 27005 ($P \times I$) підтвердила критичний або дуже високий рівень ризику для сценаріїв підміни IBAN, компрометації акаунтів і КЕП, а також високий рівень ризику для збоїв інтеграцій і внутрішніх змін у CRM/ERP.

У підрозділі 2.3 продемонстровано практичне застосування методик оцінки ризиків шляхом поєднання підходів $P \times I$, ALE та FAIR. Кількісні розрахунки показали, що найбільший очікуваний річний збиток формують збої інтеграцій через їхню вищу частоту, тоді як ВЕС-атаки характеризуються максимальною тяжкістю одиничного інциденту. Аналіз чутливості параметрів підтвердив доцільність пріоритетних інвестицій у підвищення стійкості інтеграцій, посилення керування доступами та обов'язкові out-of-band-перевірки змін реквізитів як заходи з найвищим ефектом зменшення ризику.

Отже, результати розділу 2 сформуvalи обґрунтований ризиковий профіль фінансового департаменту ТОВ «Спектр-Агро» та довели ефективність комбінованого використання напівкількісних і кількісних методик оцінювання кіберризиків. Отримані висновки створюють основу для розроблення у наступному розділі практичних рекомендацій щодо підвищення рівня кіберстійкості фінансових процесів підприємства.

РОЗДІЛ 3. КОНСТРУКТИВНІ ШЛЯХИ ПІДВИЩЕННЯ КІБЕРБЕЗПЕКИ ФІНАНСОВОГО ДЕПАРТАМЕНТУ ТОВ «СПЕКТР-АГРО»

3.1. Обґрунтування стратегічних напрямів удосконалення системи управління кіберризиками

Ефективне управління кіберризиками у фінансовому департаменті ТОВ «Спектр-Агро» є критично важливим елементом забезпечення безперервності бізнес-процесів, достовірності фінансових даних та виконання договірних і регуляторних зобов'язань підприємства. Результати аналітичного розділу показали, що найбільш небезпечними для фінансового контуру є сценарії підміни банківських реквізитів (BEC), компрометації облікових записів, порушення роботи інтеграцій та зловживання КЕП. Враховуючи ці висновки, стратегічні напрями вдосконалення системи кібербезпеки мають формуватися як комплексна, ризик-орієнтована програма, що поєднує організаційні, технічні, процесні та аналітичні рішення.

Потреба у формуванні стратегічних напрямів удосконалення CRMS впливає з трьох ключових факторів:

1. Цифрова інтегрованість фінансових процесів, що базується на взаємодії ERP, CRM, клієнт-банку та державних електронних сервісів, створює множинні точки кіберризиків.
2. Організаційно-процесні вразливості, включно з недостатньою формалізацією перевірок реквізитів, нерегулярним аудитом доступів та переобтяженням персоналу у сезонні піки, що підвищує ймовірність людських помилок.
3. Домінування соціальної інженерії та атак на цілі фінансових операцій, що підтверджено аналізом інцидентів 2024-2025 років і узгоджується з глобальними тенденціями.

У цьому контексті стратегічні напрями покликані не лише зміцнити технічні контролю, а й забезпечити узгодженість ролей, стандартів та процесів

відповідно до вимог ISO/IEC 27001, ISO/IEC 27005, NIST CSF 2.0 та NIST SP 800-30, що розглядалися у першому розділі.

Аналіз показав, що наявні заходи кіберзахисту ТОВ «Спектр-Агро» носять переважно оперативний характер – акцент зміщено на реагування на інциденти або усунення технічних неполадок. Водночас методики ISO/IEC 27005 та NIST SP 800-30 вимагають системності у визначенні активів, моделюванні сценаріїв атак, оцінюванні ймовірностей і впливів та побудові циклічного ризик-менеджменту.

Для фінансового департаменту перехід до ризик-орієнтованої моделі означає:

1. чітке визначення контурів критичних активів (ERP, клієнт-банк, КЕП, довідники контрагентів);
2. проведення регулярного аналізу сценаріїв атаки на основі NIST SP 800-30;
3. застосування кількісних підходів ALE та FAIR для бюджетування заходів безпеки;
4. планове оновлення політик і процедур на основі фактичних KRI/KPI.

Це дозволить перевести систему безпеки з «реактивної» моделі у «проактивну», де критичні ризики прогнозуються, а не фіксуються постфактум. Водночас підвищення зрілості процесів ризик-менеджменту потребує не лише технічних рішень, а й чіткої координації управлінських функцій та узгодження політик безпеки з бізнес-цілями підприємства. Саме тому наступним стратегічним кроком є формування прозорої системи ролей, відповідальності та наглядових механізмів.

Оновлена редакція NIST CSF 2.0 акцентує на тому, що надійна кібербезпека потребує не лише технічних рішень, а й чіткого стратегічного управління та координації дій усіх залучених підрозділів. Аналіз роботи фінансового департаменту показав, що низка процесних прогалин, зокрема неповна фіксація процедур підтвердження IBAN чи нерегулярний перегляд розподілу обов'язків (SoD), свідчать про потребу у більш структурованій організації управлінських функцій.

У цьому контексті визначені стратегічні кроки розвитку системи включають:

1. визначення допустимого рівня ризику для фінансових процесів, зокрема граничних обсягів потенційних втрат, максимально припустимих простоїв та ключових параметрів відновлення (RTO/RPO);
2. побудову матриці RACI для чіткого розподілу ролей під час виконання основних фінансових операцій;
3. формалізацію меж відповідальності між CFO, CISO, CIO, керівниками операційних підрозділів і внутрішнім аудитом;
4. запровадження практики щомісячної звітності CFO щодо ключових індикаторів ризику (KRI) та результатів аналізу журналів змін.

Завдяки цьому управлінські процеси стають прозорішими, ризики більш контрольованими, а діяльність фінансового департаменту узгодженою та передбачуваною на рівні всієї організації.

Разом із формалізацією ролей та управлінських процедур важливим є й підсилення практичних механізмів захисту саме тих процесів, які залишаються найбільш вразливими згідно з результатами проведеної оцінки ризиків. Оскільки основні інциденти та потенційні збитки у фінансовому департаменті виникають на стику електронної комунікації, обміну фінансовими документами та виконання платіжних операцій, наступним стратегічним напрямом стає зосередження уваги на підвищенні стійкості цих критичних потоків.

Проведений аналіз засвідчив, що ризик А – підміна банківських реквізитів у результаті ВЕС-атаки є найбільш загрозливим за масштабом можливих наслідків (I=5). Водночас сценарій В – компрометація робочого облікового запису співробітника демонструє підвищену імовірність реалізації (P=3-4), особливо в умовах високого навантаження та соціально-інженерних атак. Такі результати підкреслюють необхідність упровадження комплексних стратегічних заходів, які б суттєво зменшили вразливість платіжних та комунікаційних процесів.

До першочергових кроків у цьому напрямі належать:

1. запровадження обов'язкової незалежної (out-of-band) перевірки будь-яких змін банківських реквізитів;
2. посилення захисту електронної пошти за рахунок застосування DMARC, DKIM, SPF, анти-BEC фільтрів та технологій аналізу вкладень у безпечному середовищі (sandbox);
3. використання механізмів «step-up authentication» для платежів та автоматичного виявлення нетипових сум або поведінкових аномалій;
4. регулярне проведення фішинг-симуляцій та індивідуально орієнтованих навчальних програм для співробітників фінансового підрозділу.

Оскільки саме фінансовий департамент найчастіше стає ціллю цілеспрямованих атак, зміцнення стійкості цих процесів є визначальним фактором підвищення загального рівня кіберзахисту підприємства.

Утім, захист електронних комунікацій та платіжного контуру охоплює лише один із критичних сегментів фінансової діяльності. Не менш важливою складовою кіберстійкості є забезпечення надійної роботи технологічних інтеграцій, які поєднують ERP, CRM, клієнт-банківські сервіси та державні шлюзи. Саме від їхньої безперебійності залежить коректність бухгалтерських операцій, своєчасність платежів та дотримання регуляторних строків.

За результатами проведених розрахунків за моделлю ALE встановлено, що сценарій D – збої інтеграцій між ERP, CRM, клієнт-банком та державними сервісами, формує найбільший очікуваний річний збиток (72 000 грн). Це означає, що саме цей напрям потребує пріоритетної уваги у середньостроковому плануванні кіберзахисту. Аналіз операційної діяльності підтверджує наявність технічних вразливостей: періодичні збої взаємодії з банківською інфраструктурою та державними електронними платформами вже неодноразово призводили до затримок, повторних транзакцій або порушення строків подання фінансових документів.

З огляду на це, стратегічний розвиток системи має включати такі кроки:

1. Створення формалізованої архітектури інтеграцій, що передбачає повну інвентаризацію API, точок обміну даними та залежностей між ними.
2. Упровадження механізмів автоматичного відновлення та стійкості, зокрема ретраїв, контролю черг оброблення запитів і використання резервних каналів передачі даних.
3. Визначення чітких SLA щодо доступності інтеграційних сервісів і максимально допустимого часу їхнього відновлення, що дозволить структурувати очікування та відповідальність постачальників.
4. Регулярне проведення тестувань на відмовостійкість (disaster recovery drills), які допоможуть оцінити реальну готовність систем до аварійних ситуацій та скоротити час реагування.

Забезпечення високої стійкості інтеграційних потоків є фундаментом безперебійної роботи платіжних, бухгалтерських та облікових операцій. Відтак саме від якості цих процесів безпосередньо залежить загальна фінансова стабільність і операційна надійність підприємства.

Підвищення стійкості інтеграційних потоків забезпечує надійну основу для безперебійної роботи фінансових систем, однак не менш важливим елементом захисту залишається контроль за інструментами, що мають юридичну силу. Наступним критичним аспектом кіберстійкості фінансового департаменту є належна організація роботи з кваліфікованими електронними підписами, оскільки саме вони підтверджують легітимність фінансових транзакцій і офіційних документів. Це потребує стандартизованого та централізованого підходу.

Сценарій С, пов'язаний зі зловживанням КЕП, є одним із найбільш ризикових, адже електронний підпис прирівнюється до власноручного підпису та надає юридичну силу фінансовим та податковим операціям. Тому на стратегічному рівні підприємству важливо впровадити єдину, контрольовану модель управління КЕП, яка охоплюватиме весь життєвий цикл підписів.

До ключових елементів такої моделі належать:

1. формування централізованого реєстру видачі, зберігання, передачі та відкликання електронних підписів;
2. обмеження використання КЕП виключно перевіреними та авторизованими пристроями;
3. застосування апаратних токенів або захищених контейнерів для мінімізації ризику копіювання ключів;
4. автоматизований контроль коректності підписувачів у бізнес-процесах ERP та системах обробки фінансових документів;
5. упровадження додаткового рівня підтвердження для документів і транзакцій, що мають особливу юридичну вагу.

Реалізація такої моделі дозволяє суттєво зменшити юридичні та операційні ризики, а також унеможливорює випадки несанкціонованого підписання документів сторонніми або неповноважними особами.

Підвищення контролю над життєвим циклом електронних підписів значно зменшує юридичні та операційні ризики, однак для підтримання стійкості фінансових процесів цього недостатньо. Безперервність безпеки вимагає не лише впровадження окремих заходів, а й постійного спостереження за їхньою дієвістю. Саме тому наступним ключовим елементом розвитку системи управління кіберризиками є створення ефективного механізму моніторингу, здатного своєчасно фіксувати зміни ризикового профілю та забезпечувати аналітичну підтримку управлінських рішень.

Як було встановлено у розділі 2, окремі ризики демонструють суттєву динамічність і можуть різко посилюватися залежно від сезонності чи змін операційного навантаження. Наприклад, збільшення кількості шкідливих вкладень ($P = 4$) або підвищена частка платежів із ручною зміною реквізитів чітко корелюють із періодами пікового обсягу робіт. Це вимагає переходу до систематичного моніторингу, який охоплюватиме:

1. оперативне відстеження ключових індикаторів ризику, що сигналізують про зміни у загрозовому середовищі;

2. оцінювання ефективності існуючих контрольних механізмів, з визначенням їхньої відповідності поточним умовам;
3. підтримку управлінських рішень на основі реальних даних, а не припущень;
4. планове вдосконалення системи CRMS у межах PDCA-циклу (Plan-Do-Check-Act) із щоквартальним переглядом результатів.

Індикатори ризику (KRI), релевантні для фінансового департаменту, такі як частка платежів із ручним коригуванням реквізитів або кількість листів, відхилених за DMARC, мають використовуватися як «ранні сигнали». Вони дозволяють визначати, коли слід посилити контролю, провести додаткові перевірки або змінити окремі процедури. Завдяки цьому система управління ризиками стає не статичною, а адаптивною, здатною швидко реагувати на зміни у внутрішньому та зовнішньому середовищі.

Побудова системи показників і регулярний перегляд результативності контролів дозволяють фінансовому департаменту оперативно реагувати на зміни у ризиковому середовищі. Проте для ефективного управління кіберризиками недостатньо лише відстежувати їхню динаміку, важливо також мати можливість обґрунтовано планувати витрати на кіберзахист та раціонально розподіляти ресурси між різними напрямками. Саме тут вагоме значення набувають кількісні моделі оцінювання, які забезпечують прозорість та економічну аргументованість управлінських рішень.

Ключова стратегічна перевага використання методологій ALE та FAIR, результати яких наведено у розділі 2, полягає у здатності перетворити кіберризики з абстрактних загроз на вимірювані фінансові показники. Наприклад, зниження частоти інцидентів у сценарії D шляхом впровадження резервного каналу може зменшити очікувані річні збитки майже вдвічі, що наочно демонструє економічний ефект від конкретних заходів.

Застосування таких моделей дозволяє:

1. визначати пріоритетність заходів безпеки на основі співвідношення їхньої вартості та очікуваного результату;

2. обґрунтовувати необхідність інвестицій перед керівництвом на основі розрахунків, а не припущень;
3. оцінювати окупність впроваджених рішень (ROI) та прогнозувати їхній довгостроковий ефект;
4. планувати модернізацію CRMS у середньостроковій перспективі (6-12 місяців) із прив'язкою до конкретних фінансових показників.

Таким чином, кількісні моделі перестають бути допоміжним інструментом технічних фахівців і перетворюються на основу стратегічного планування, що забезпечує прозорість, передбачуваність та економічну доцільність усіх рішень у сфері кібербезпеки.

Узагальнюючи результати дослідження, слід зазначити, що обґрунтування стратегічних напрямів удосконалення системи управління кіберризиками у фінансовому департаменті ТОВ «Спектр-Агро» є ключовою передумовою підвищення кіберстійкості підприємства. Проведений аналіз підтвердив, що саме фінансовий контур залишається найбільш вразливою частиною організаційної структури через високу концентрацію критичних активів, значну інтенсивність транзакційних операцій і залежність від зовнішніх цифрових сервісів.

Установлено, що найбільшу небезпеку становлять ризики, пов'язані з підміною банківських реквізитів, компрометацією робочих облікових записів, збоєм інтеграцій між ключовими системами та зловживанням кваліфікованими електронними підписами. Саме ці сценарії формують основу стратегічних рішень і визначають необхідність переходу до системного, передбачуваного й стандартизованого підходу до кіберзахисту.

Відповідно до міжнародних стандартів ISO/IEC 27001, ISO/IEC 27005 та NIST CSF 2.0, ефективна система управління кіберризиками має ґрунтуватися на ризик-орієнтованості, формальності процедур і безперервності циклу PDCA. Це передбачає чітке визначення критичних активів, регулярне моделювання сценаріїв атак, застосування кількісних методів оцінювання (ALE, FAIR),

створення системи індикаторів KPI/KRI та впровадження прозорого механізму розподілу ролей і відповідальності.

Особливе значення мають стратегічні заходи, спрямовані на посилення захисту електронних комунікацій, підвищення стійкості інтеграційних потоків ERP-CRM-клієнт-банк, контроль за життєвим циклом електронних підписів та формування культури безпеки серед співробітників. Запропоновані напрями дозволяють зменшити вплив людського фактора, посилити надійність платіжного контуру та забезпечити юридичну захищеність фінансових операцій.

Отже, стратегічне удосконалення системи управління кіберризиками повинно розглядатися як інтегрована програма, що поєднує організаційні, технічні та аналітичні рішення. Її реалізація забезпечить перехід від реактивного реагування на інциденти до проактивного попередження кіберзагроз, сприятиме підвищенню рівня кіберстійкості фінансових процесів і зміцнить загальну безпеку діяльності ТОВ «Спектр-Агро».

3.2. Розроблення комплексу організаційних та технічних заходів щодо мінімізації кіберризиків фінансового департаменту

Побудова ефективної системи управління кіберризиками фінансового департаменту ТОВ «Спектр-Агро» потребує впровадження комплексного набору організаційних і технічних заходів, здатних мінімізувати ймовірність реалізації найбільш критичних сценаріїв. Проведений аналіз показав, що значна частина ризиків виникає на перетині технологічних процесів і людського фактора, а отже, заходи з кібербезпеки повинні одночасно охоплювати процедури, регламенти, інфраструктуру, політики доступів та навчання персоналу.

В основу запропонованого комплексу заходів покладено результати кількісної та якісної оцінки ризиків ($P \times I$, ALE, FAIR), методологічні підходи

ISO/IEC 27001-27005, рекомендації NIST CSF 2.0, а також специфіку фінансових процесів підприємства. Це дозволяє сформувати цілісну систему захисту, у якій кожен елемент слугує посиленням попереднього, забезпечуючи багаторівневу й адаптивну модель безпеки.

Після визначення стратегічних пріоритетів та ключових напрямів розвитку системи управління кіберризиками постає необхідність перейти від концептуального рівня до конкретних практичних рішень. Оскільки виявлені загрози формуються на стику технічних, організаційних та людських факторів, подальший етап удосконалення передбачає комплексний підхід, який одночасно охоплює процедури, політики, доступи, поведінку персоналу й технологічні механізми захисту. У цьому контексті першочергового значення набувають організаційні заходи, що забезпечують чіткість процесів, прозорість відповідальності та належний рівень управлінського контролю.

Для ефективної роботи фінансового департаменту критично важливо мати чітко визначені та формалізовані правила, які регулюють обробку фінансової інформації та виконання платіжних операцій. Ураховуючи виявлені слабкі місця, необхідно:

1. запровадити стандартизовану процедуру перевірки банківських реквізитів, яка включатиме обов'язкову незалежну out-of-band верифікацію при будь-якій зміні IBAN чи інших критичних даних;
2. встановити політику “Zero Tolerance to Manual Overrides”, що мінімізує використання ручних правок у платіжних документах, інтеграційних налаштуваннях і довідниках;
3. документувати кожен винятковий випадок у фінансових процесах та погоджувати його на рівні CFO або CISO;
4. розробити деталізований регламент реагування на інциденти, який охоплюватиме дії у разі BEC-атак, підозрілих платежів, збоїв інтеграцій чи ознак компрометації КЕП, а також визначатиме канали комунікації та механізми ескалації.

Упровадження таких правил гарантує контрольованість та аудитованість фінансових операцій і значно знижує ризик помилок або несанкціонованих втручань.

Щоб мінімізувати внутрішні ризики та запобігти можливим зловживанням, необхідно поглибити розмежування функцій і відповідальностей:

1. відділити ролі ініціатора, погоджувача та виконавця платежів, уникнувши будь-якого суміщення цих функцій однією особою;
2. сформувати RACI-матрицю для всіх ключових фінансових операцій – від зміни реквізитів і оновлення довідників до управління КЕП та доступу в клієнт-банк;
3. здійснювати щомісячний SoD-рев'ю, з автоматичним виявленням конфліктів доступів і відхилень;
4. вести повний журнал прав доступу, у якому фіксуються всі зміни ролей, привілеїв і підстави їх надання.

Регулярний аудит доступів дозволяє вчасно виявляти непропорційні чи невинновдані права доступу та підвищує прозорість внутрішніх процесів.

Оскільки переважна частина інцидентів у фінансовому департаменті пов'язана із соціально-інженерними атаками, людськими помилками та фішинговими листами, важливо системно зміцнювати обізнаність співробітників:

1. проводити регулярні фішинг-симуляції з урахуванням реальних сценаріїв атак, спрямованих на співробітників ТОВ «Спектр-Агро»;
2. організувати навчання, адаптоване до конкретних ролей: для казначейства, бухгалтерії, Credit Control та інших підрозділів;
3. включити модуль з кібергігієни до програми адаптації нових працівників, що охоплюватиме правила роботи з реквізитами, документами та КЕП;
4. розробити корпоративний гайдлайн із безпеки фінансових операцій, який міститиме приклади ВЕС-атак, ознаки підроблених документів і рекомендації щодо безпечної комунікації.

Системне підвищення рівня обізнаності персоналу зменшує вразливість до атак соціальної інженерії та значно посилює загальну кіберстійкість фінансового департаменту.

Узгоджені політики, прозорий розподіл ролей і системне навчання персоналу створюють керований контур фінансових процесів. Водночас, щоб ці правила працювали на практиці та витримували тиск реальних загроз, потрібні надійні технологічні «опори» – контроль доступів, захист каналів комунікації, стійкі інтеграції та безпечне використання електронних підписів. Саме поєднання організаційних і технічних механізмів дає той рівень кіберстійкості, який очікує бізнес.

З огляду на підвищену ймовірність сценаріїв, пов'язаних із захопленням облікових записів, пріоритетом є «ущільнення» контуру доступу до фінансових систем:

1. Увімкнути підсилену багатофакторну автентифікацію для клієнт-банку та ERP (наприклад, number matching, FIDO2-ключі або апаратні токени) – це ускладнює компрометацію навіть у разі витоку пароля.
2. Дозволити роботу лише з керованих корпоративних пристроїв, зареєстрованих у домені/MDM – так виключаються невідомі або скомпрометовані середовища.
3. Застосовувати географічні та ASN-фільтри, щоб відсікати нетипові підключення та трафік із ризикових автономних систем.
4. Скоротити час життя сесій у фінансових системах і вмикати ре-автентифікацію для критичних дій.
5. Автоматично блокувати облікові записи у разі виявлення аномальної поведінки (серії помилкових MFA, нетипова активність у позаробочий час, раптові зміни середовища доступу).

У сукупності ці кроки суттєво зменшують шанс успішної компрометації через фішинг, повторне використання паролів чи викрадення сесій.

Проте навіть за умов посиленого контролю доступів одним із найвразливіших каналів залишається корпоративна електронна пошта, яка

часто стає першим етапом реалізації атак. Саме тому наступним важливим напрямом є підвищення її «імунітету» до підробок, маніпуляцій і шкідливого вмісту:

1. Активувати DMARC, DKIM та SPF із суворими політиками (відхилення/карантин), аби запобігти підробці домену відправника.
2. Установити спеціалізовані anti-BEC фільтри, що виявляють домени-двійники, підміни реквізитів і маніпуляції у ланцюжках листування.
3. Запровадити sandbox-перевірку вкладень (PDF, XLSM тощо), щоб ізолювати й проаналізувати потенційно небезпечні файли до доставки адресатові.
4. Автоматично маркувати зовнішні листи й повідомлення з ознаками ризику, аби користувач завчасно бачив попередження та діяв обережніше.

Таке налаштування дає змогу блокувати переважну більшість фішингових і шахрайських повідомлень ще до того, як вони досягають співробітників фінансового підрозділу. Проте навіть надійний захист електронної пошти не усуває ризиків, що виникають у процесах, де задіяні зовнішні сервіси та взаємодія між кількома інформаційними системами підприємства. Саме тому наступним важливим елементом технічної безпеки є забезпечення стабільності та відмовостійкості інтеграційних потоків.

Безперервність платіжних і облікових процесів напряму залежить від надійності інтеграцій між внутрішніми системами та зовнішніми сервісами. Щоб зменшити операційні ризики потрібно:

1. Реалізувати механізми повторних спроб (retry), черги обробки та автоматичне дублювання запитів у разі короткочасних збоїв.
2. Створити резервні канали обміну даними з банками та державними платформами, аби уникнути простою під час інцидентів на стороні провайдера.
3. Централізувати логування API-викликів та інтеграційних помилок, з їх подальшою кореляцією у SIEM/XDR для швидкого розслідування.
4. Проводити регулярні DR-тести для перевірки досяжності цілей RTO/RPO і готовності команд до відновлення.

Посилені інтеграції знижують імовірність збоїв у пікові періоди, запобігають дублюванню платежів і допомагають дотримуватися регуляторних строків.

Однак технологічна стійкість є лише одним із компонентів захисту фінансових процесів. Не менш критичним елементом залишається контроль за інструментами, що мають юридичну силу та використовуються у щоденній роботі – кваліфікованими електронними підписами. Саме тому наступним напрямом удосконалення є вибудова системи їхнього безпечного управління.

Кваліфіковані електронні підписи надають юридичну силу фінансовим діям, тому їхній захист має бути максимально строгим:

1. Перевести КЕП на апаратні носії або захищені контейнери, щоб унеможливити копіювання ключів.
2. Вести єдиний реєстр видачі, передавання та блокування КЕП із повною історією життєвого циклу.
3. Дозволити використання КЕП лише на авторизованих робочих станціях, що пройшли перевірку безпеки.
4. Додати другий фактор підтвердження (second-factor approval) для підписання документів підвищеної важливості.

Такі практики мінімізують ризики несанкціонованого підписання та зловживань, а також спрощують аудит і розслідування інцидентів.

Наступним напрямом є впровадження процесних інструментів, які автоматизують контроль і мінімізують можливість обходу технічних та організаційних бар'єрів.

Запровадження додаткових рівнів перевірки для транзакцій підвищеної ризиковості, зокрема альтернативного підтвердження через незалежний канал зв'язку, автоматичного виявлення нетипових сум, нових контрагентів чи зміни IBAN, а також аналізу поведінкових особливостей користувачів – створює багаторівневий бар'єр, що суттєво ускладнює проведення шахрайських операцій. Такі механізми дозволяють виявляти аномалії ще до етапу

погодження платежу, тим самим істотно зменшуючи ймовірність успішного проходження підроблених транзакцій.

Разом із тим, навіть найефективніші такі процедури не забезпечать повного контролю без системної прозорості змін усередині фінансових систем. Саме тому наступним елементом процесного вдосконалення є автоматизація журналів змін та їхнє регулярне аналітичне опрацювання.

Для підвищення контрольованості та своєчасного виявлення потенційних інцидентів у фінансових системах необхідно впровадити такі механізми:

1. автоматичне фіксування всіх змін у ERP та CRM, включно з редагуванням реквізитів, лімітів, довідників та фінансових параметрів;
2. створення дашбордів для оперативного аналізу змін, що дозволить швидко виявляти нетипові дії або потенційні ознаки компрометації;
3. регулярний перегляд журналів на основі ключових індикаторів ризику (KRI), що дозволяє визначати відхилення від норми й вчасно реагувати на підозрілу активність;
4. інтеграцію логів до систем SIEM/XDR, які забезпечують кореляцію подій, автоматичне виявлення аномалій та прискорене розслідування інцидентів.

Систематизована аналітика змін не лише посилює контроль за критично важливими фінансовими операціями, а й забезпечує раннє виявлення потенційних точок компрометації, що значно підвищує прозорість і надійність роботи фінансового департаменту. Однак для того, щоб ця аналітика перетворювалася на дієві управлінські рішення, необхідно доповнити її системою кількісних показників, яка дозволить оцінювати стан кібербезпеки в динаміці та коригувати політики відповідно до реальних тенденцій.

Для того щоб система управління кіберризиками працювала у відповідності до циклу PDCA та реагувала на зміни у ризиковому профілі, необхідно:

1. встановити цільові порогові значення KPI та KRI, наприклад частку ручних змін реквізитів на рівні менше 0,5%;

2. створити інтерактивний дашборд ризиків для CFO, який забезпечуватиме оперативну видимість ситуації у фінансовому контурі;
3. проводити квартальні огляди ефективності контролів, оцінюючи їх відповідність поточним загрозам та інцидентам;
4. налаштувати автоматичні сповіщення про перевищення встановлених порогів KRI, щоб забезпечити своєчасне реагування та коригування процесів.

Упровадження такої системи гарантує постійний моніторинг стану безпеки, своєчасне виявлення тенденцій зростання ризиків та швидке коригування контрольних заходів, що робить CRMS фінансового департаменту по-справжньому адаптивною та ефективною.

У межах розроблення комплексу організаційних і технічних заходів було сформовано цілісну модель підвищення кіберстійкості фінансового департаменту ТОВ «Спектр-Агро». Проведений аналіз довів, що ефективність системи забезпечується лише при узгодженій роботі процесних, організаційних та технологічних рішень, інтегрованих у єдину керовану структуру.

Ключовим результатом цього підрозділу є формування багаторівневої структури контролю, яка охоплює регламенти роботи фінансових підрозділів, чіткий розподіл обов'язків, підвищення культури безпеки персоналу, захист каналів комунікації, стійкість інтеграцій, контроль за життєвим циклом КЕП та безперервний моніторинг стану ризиків. Такий підхід дозволяє зменшити ймовірність реалізації найкритичніших загроз, від підміни реквізитів і компрометації облікових записів до збоїв у роботі інтеграційних сервісів та зловживання електронними підписами.

Запропоновані заходи не лише закривають наявні вразливості, виявлені у фінансових процесах, але й створюють основу для поступового переходу до проактивної моделі захисту, у якій ризики прогнозуються та контролюються на етапі їх формування. Систематизація процедур, посилення контролю доступів, автоматизація перевірок та інтеграція KPI/KRI забезпечують стабільне функціонування CRMS і дозволяють оперативно реагувати на зміни у загрозовому середовищі.

Таким чином, реалізація комплексу заходів, розглянутих у цьому підрозділі, формує фундаментально новий рівень кіберзахисту фінансового департаменту – цілісний, структурований і керований. Він не лише підвищує стійкість до поточних загроз, але й забезпечує адаптивність системи у довгостроковій перспективі, сприяючи фінансовій стабільності та безперервності бізнес-процесів ТОВ «Спектр-Агро».

3.3. Прогнозування ефективності запропонованих рішень та оцінювання їх впливу на рівень кіберзахищеності підприємства

Ефективність заходів підвищення кіберстійкості визначається не фактом упровадження, а вимірюваним ефектом через зниження ризиків і зростання надійності фінансових процесів. Сформований у підрозділах 3.1-3.2 комплекс організаційних, технічних і процесних рішень створює цілісну систему, здатну трансформувати ризиковий профіль фінансового департаменту ТОВ «Спектр-Агро». Для об'єктивної оцінки очікуваних результатів застосовано прогнозування впливу на ключові параметри кібербезпеки.

Прогнозування ґрунтується на трьох групах показників:

1. зменшення ймовірності реалізації критичних сценаріїв,
2. скорочення масштабу можливих збитків,
3. підвищення керованості процесів та швидкості реагування.

Проведене оцінювання ефективності запропонованих заходів базується на поєднанні кількісних і якісних інструментів ризик-менеджменту. Для прогнозу очікуваного впливу використовувалися моделі, розглянуті у попередніх розділах ($P \times I$, ALE, FAIR), а також система ключових індикаторів ефективності (KPI) та ризику (KRI), рекомендована стандартами ISO/IEC 27005 і NIST CSF 2.0. Такий підхід дозволяє не лише оцінити поточний стан кіберстійкості, але й змодельовати, як зміниться ризиковий профіль фінансового департаменту після впровадження всіх запропонованих рішень. На основі цього

аналізу можна перейти до деталізованої оцінки очікуваних змін за ключовими сценаріями кібервразливостей.

1. Очікуване зменшення ймовірності реалізації основних кіберризиків BEC-атаки та підміна реквізитів (сценарій А).

Запровадження незалежної (out-of-band) перевірки реквізитів, захисних протоколів DMARC/DKIM/SPF, анти-BEC фільтрації та навчальних програм для персоналу суттєво підвищує надійність електронних комунікацій. Прогнозне моделювання показує, що рівень імовірності таких атак може зменшитися з 4-5 до 2-3 протягом перших шести місяців; моделювання динаміки ризиків свідчить про стабілізацію показника протягом 12 місяців. У практичному вимірі це дозволяє знизити рівень ризику з критичного до помірного рівня, а втрати від підроблених платежів можуть скоротитися щонайменше удвічі.

2. Компрометація облікових записів (сценарій В).

Посилена багатofакторна автентифікація, контроль робочих пристроїв, обмеження за географічними ознаками та виявлення аномальної активності формують стійкий захисний периметр. Результати сценарного моделювання вказують на можливе зниження ймовірності інцидентів з 3-4 до 1-2 після повного розгортання FIDO2-рішень і поведінкової аналітики. Таким чином суттєво мінімізується ризик несанкціонованого доступу через викрадені або перехоплені облікові дані.

3. Збої інтеграцій (сценарій D)

Використання механізмів повторних спроб, резервних каналів взаємодії та регулярне тестування на відмовостійкість безпосередньо впливають на очікуваний рівень фінансових втрати (ALE): зниження річного показника ALE з 72 000 грн до 25 000-30 000 грн після впровадження резервних рішень. Це дозволяє мінімізувати фінансові втрати від простоїв та уникнути збоїв у платіжному циклі під час пікових операційних періодів.

4. КЕП (сценарій С)

Переведення кваліфікованих електронних підписів на апаратні носії, централізоване керування їхнім життєвим циклом і впровадження додаткового підтвердження при підписанні важливих документів значно знижують ризики несанкціонованих дій: ймовірність інцидентів зменшується до рівня 1-2; потенційний масштаб збитків (I) також скорочується завдяки прозорості журналів використання та second-factor approval.

Упровадження заходів, спрямованих на підсилення контролю за використанням кваліфікованих електронних підписів, створює додатковий рівень захисту для фінансових операцій та значно знижує ризики несанкціонованих дій. Разом із цим важливо оцінити, як запропоновані технічні та організаційні рішення впливають на загальний рівень фінансових втрат. Для цього використано кількісні моделі ризик-менеджменту (ALE та FAIR), що дозволяють перевести ефективність заходів у вимірювані економічні показники.

Комплекс ужитих заходів дає можливість прогнозувати істотне зменшення економічних збитків, пов'язаних із реалізацією кіберризиків. Зокрема:

1. зниження SLE (Single Loss Expectancy) для операцій підвищеного ризику на 30-50% завдяки посиленій автентифікації та контролю реквізитів;
2. скорочення ARO (Annualized Rate of Occurrence) для фішингових та соціально-інженерних атак орієнтовно в 2 рази завдяки впровадженню анти-BEC механізмів, навчання та поведінкової аналітики;
3. зменшення загального ризику ($Risk = LEF \times LM$) за моделлю FAIR приблизно на 40%, що відображає одночасне зниження частоти інцидентів та їхнього потенційного впливу.

У грошовому вираженні це означає, що підприємство може зменшити річні сукупні збитки від кіберінцидентів на 45-60%, що є значно вищим за середньоринковий рівень ефективності впроваджених заходів. Для більш детального розуміння економічної користі важливо проаналізувати, як саме зміни у частоті та масштабах інцидентів відображаються на ключових

фінансових метриках ризику, нижче наведено вплив заходів на зменшення фінансових втрат (перерахунок за ALE та FAIR).

У сукупності ці кроки формують стійку, адаптивну та керовану систему управління кіберризиками, яка: переводить CRMS у проактивний режим функціонування; відчутно зменшує залежність від людського фактора; гарантує захищеність платіжного циклу та цілісність довідникових даних; створює передумови для успішного проходження аудитів/сертифікацій з кібербезпеки; підвищує довіру банків, партнерів і постачальників до підприємства.

У довгостроковій перспективі це сприятиме: зростанню фінансової стабільності; скороченню операційних збоїв; зниженню юридичних ризиків; зміцненню репутації ТОВ «Спектр-Агро» як надійного та безпечного бізнес-партнера.

Проведене прогнозування ефективності засвідчило, що запропонований у розділі 3 комплекс організаційних, технічних та процесних рішень здатен якісно змінити ризиковий профіль фінансового департаменту ТОВ «Спектр-Агро». Поєднання кількісних моделей оцінювання ($P \times I$, ALE, FAIR) з системою керованих показників (KPI/KRI) дозволило не лише зафіксувати поточний стан, а й змодельовати очікувані зміни з високим ступенем практичної застосовності для управлінських рішень.

Отримані результати свідчать, що ймовірність реалізації критичних сценаріїв (BEC-атаки, компрометація облікових записів, збої інтеграцій, зловживання КЕП) істотно зменшується завдяки адресним заходам: out-of-band-перевіркам реквізитів, посиленій автентифікації та контролю доступів, підвищенню стійкості інтеграційних потоків і стандартизованому управлінню життєвим циклом КЕП. У фінансовому вимірі це трансформується у зниження SLE та ARO, що, у підсумку, приводить до меншого інтегрального ризику ($Risk = LEF \times LM$) та відчутного скорочення потенційних збитків.

Водночас ефект не обмежується фінансовими показниками. Завдяки автоматизації журналів змін, кореляції подій у SIEM/XDR, використанню «пісочниць» та поведінкової аналітики очікується покращення операційних

метрик: скорочення MTTR, зростання точності виявлення, стабілізація KRI і менша частка ручних втручань у критичні довідникові дані. Це підсилює керованість і передбачуваність процесів, зменшує навантаження на команду та дисциплінує виконання регламентів. Сумарний ефект полягає у переході CRMS до проактивної моделі, де ризики відстежуються динамічно, рішення приймаються на основі даних, а контрольні заходи системно коригуються за PDCA-циклом. У стратегічній перспективі це забезпечує сталість платіжного контуру, цілісність фінансових даних, зниження юридичних ризиків і зміцнення довіри банків і партнерів. Для збереження ефекту необхідні: щоквартальне оновлення профілю ризиків (за KRI/KPI та інцидент-рев'ю), DR-тести відповідно до RTO/RPO, підтримка культури безпеки (тренінги, фішинг-симуляції, адресні інструктажі) та перегляд бюджетів кіберзахисту за ALE/FAIR, аби інвестиції залишалися економічно виправданими.

Отже, запропоновані рішення демонструють економічну та операційну обґрунтованість і формують стійкий фундамент кіберзахисту фінансового департаменту. Їх упровадження забезпечує не лише разове зниження ризиків, а й здатність системи адаптуватися до нових загроз, що критично важливо для довгострокової фінансової стабільності та безперервності бізнес-процесів ТОВ «Спектр-Агро».

Висновок до розділу 3

У розділі 3 обґрунтовано та розроблено практичні напрями підвищення рівня кібербезпеки фінансового департаменту ТОВ «Спектр-Агро» з урахуванням специфіки його фінансових процесів і результатів оцінювання кіберризиків, отриманих у попередніх розділах. Основний акцент зроблено на переході від фрагментарних і реактивних заходів до цілісної ризик-орієнтованої системи управління кіберризиками (CRMS).

У підрозділі 3.1 доведено, що фінансовий контур підприємства є найбільш уразливим через високу концентрацію критичних активів,

інтенсивність платіжних операцій і залежність від зовнішніх цифрових сервісів. Обґрунтовано стратегічні напрями розвитку CRMS відповідно до стандартів ISO/IEC 27001, ISO/IEC 27005 та NIST CSF 2.0, що передбачають визначення критичних активів, регулярне моделювання сценаріїв атак, застосування кількісних методів оцінювання (ALE, FAIR), використання KPI/KRI та чіткий розподіл управлінських ролей між CFO, CISO, CIO і внутрішнім аудитом.

У підрозділі 3.2 запропоновано комплекс організаційних і технічних заходів щодо мінімізації кіберризиків. Вони охоплюють формалізацію процедур фінансових операцій, посилення контролю доступів, підвищення захищеності електронної пошти та платіжного контуру, забезпечення відмовостійкості інтеграцій між ERP, CRM і клієнт-банком, а також централізоване управління життєвим циклом кваліфікованих електронних підписів. Обґрунтовано, що поєднання процесних, організаційних і технічних механізмів дозволяє суттєво знизити вплив людського фактора та унеможливити обходи контрольних процедур.

У підрозділі 3.3 здійснено прогнозування ефективності запропонованих рішень. Застосування моделей P×I, ALE та FAIR підтвердило очікуване зниження ймовірності реалізації ключових сценаріїв (BEC-атаки, компрометація облікових записів, збої інтеграцій, зловживання КЕП) і скорочення потенційних фінансових збитків на 45-60% у річному вимірі. Окрім фінансового ефекту, прогнозується покращення операційних показників: зменшення часу реагування на інциденти, стабілізація KRI та підвищення прозорості управлінських рішень.

Отже, результати розділу 3 свідчать, що запропонована модель підвищення кіберстійкості фінансового департаменту є комплексною, економічно обґрунтованою та практично реалізованою. Її впровадження забезпечує проактивне управління кіберризиками, підвищує надійність фінансових процесів, знижує юридичні й операційні ризики та сприяє зміцненню фінансової стабільності й безперервності діяльності ТОВ «Спектр-Агро».

ВИСНОВКИ

У межах дипломної роботи проведено комплексне дослідження проблематики кіберризиків у фінансових процесах підприємства та здійснено розроблення практичних рішень для посилення кіберзахисту фінансового департаменту ТОВ «Спектр-Агро». Актуальність теми зумовлена активною цифровізацією фінансових процесів, зростанням кількості цілеспрямованих кібератак, домінуванням соціальної інженерії та посиленням залежності бізнесу від інтеграцій із банківськими, хмарними та державними електронними сервісами. У результаті фінансовий контур підприємства стає однією з найбільш уразливих ділянок з позиції кібербезпеки та потребує системного, ризик-орієнтованого підходу до захисту.

У першому розділі роботи сформовано теоретико-методичну основу дослідження. Уточнено економічну та управлінську сутність поняття «кіберризик» у контексті фінансових процесів і доведено, що його доцільно розглядати як імовірність реалізації кіберзагрози з вимірюваними фінансовими, операційними й репутаційними наслідками. Узагальнено класифікації кіберризиків і обґрунтовано необхідність їх інтеграції в систему корпоративного ризик-менеджменту (ERM). Проаналізовано міжнародні стандарти й фреймворки ISO/IEC 27001, ISO/IEC 27005, NIST CSF 2.0 та NIST SP 800-30, які формують методологічну базу управління кіберризиками. Встановлено, що найбільш ефективним є комбіноване застосування якісних, напівкількісних і кількісних методів оцінювання ($P \times I$, ALE, FAIR), що дозволяє поєднати пріоритизацію ризиків із їх економічним обґрунтуванням.

У другому розділі здійснено аналітико-дослідницьку оцінку кіберризиків фінансового департаменту ТОВ «Спектр-Агро». Досліджено структуру фінансових підрозділів, основні інформаційні потоки та критичні цифрові активи. Виявлено, що найбільшу загрозу для підприємства становлять сценарії підміни банківських реквізитів (BEC-атаки), компрометації облікових записів

користувачів, збоїв інтеграцій між ERP, CRM, клієнт-банком і державними сервісами, а також зловживання кваліфікованими електронними підписами. Напівкількісна оцінка за моделлю P×I та кількісні розрахунки за методиками ALE і FAIR дали змогу визначити пріоритетні ризики, оцінити їх очікуваний річний фінансовий ефект і довести критичність фінансового контуру як об'єкта кіберзахисту.

У третьому розділі розроблено стратегічні напрями та практичний комплекс організаційних і технічних заходів, спрямованих на підвищення рівня кібербезпеки фінансового департаменту підприємства. Обгрунтовано необхідність переходу від переважно реактивного реагування на інциденти до проактивної системи управління кіберризиками, побудованої на циклі PDCA, чіткому розподілі ролей і відповідальності, використанні KPI/KRI та економічно обгрунтованому плануванні заходів безпеки. Запропоновані рішення охоплюють посилення захисту електронних комунікацій і платіжного контуру, підвищення стійкості інтеграційних потоків, централізоване управління життєвим циклом КЕП і системне зниження впливу людського фактора. Прогнозування ефективності із застосуванням кількісних моделей показало можливість скорочення потенційних фінансових збитків від кіберінцидентів на 45-60 % у річному вимірі та підвищення керованості фінансових процесів.

Загалом результати дослідження підтверджують, що мету кваліфікаційної роботи досягнуто, а поставлені завдання виконано в повному обсязі. Запропонований підхід до оцінювання та управління кіберризиками є методично обгрунтованим, узгодженим з міжнародними стандартами та придатним для практичної реалізації в діяльності фінансового департаменту. Його впровадження сприятиме підвищенню кіберстійкості ТОВ «Спектр-Агро», зниженню фінансових, операційних і юридичних ризиків, зміцненню довіри з боку банків і контрагентів та забезпеченню безперервності бізнес-процесів в умовах зростаючих кіберзагроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Адаменко С. М. Управління інформаційною безпекою фінансових процесів підприємства: монографія – Київ: КНЕУ, 2021–228 с.
2. Андрусак Т. З., Ткаченко В. М. Кіберризики в економічних системах: навч. посіб. – Львів: ЛНУ ім. І. Франка, 2020 –244 с.
3. Аудиторська палата України. Рекомендації щодо оцінки ризиків ІТ-середовища у фінансовій звітності – Київ: АПУ, 2023 – 42 с.
4. Alberts C. J., Dorofee A. J. OCTAVE Method Implementation Guide. Version 2.0. Volume 1: Introduction. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2001–34 с.
5. Бараннік В. В., Горбенко І. Д., Корабельникова О. Л. Кібербезпека в інформаційних системах: монографія –Харків: ХНУРЕ, 2021–312 с.
6. Боднар О. С. Цифрова трансформація фінансової діяльності підприємства: монографія –Тернопіль: ТНЕУ, 2020 –180 с.
7. Бутенко Н. В. Інформаційні ризики в діяльності підприємств: навч. посіб. – Київ: КНЕУ, 2021–192 с.
8. Верба І. В. Управління ризиками в корпоративних інформаційних системах – Київ: Наук. думка, 2019 –220 с.
9. Верховна Рада України. Закон України «Про електронні комунікації» № 1089-IX від 16.12.2020 – Київ: ВРУ, 2020 – 68 с.
10. Верховна Рада України. Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 05.10.2017. № 45. Стор. 42. Ст. 403
11. Гайдай М. І. Кібербезпека: методологія оцінки ризиків: монографія – Одеса: ОНЕУ, 2022 – 280 с.
12. Геворкян С. А. Захист фінансових даних підприємства: навч. посіб. – Київ: КНЕУ, 2019 – 156 с.
13. Гнатюк С. О. Кіберзагрози та методи їх попередження – Львів: Вид-во ЛНТУ, 2021–204 с.

14. Державна служба спеціального зв'язку та захисту інформації України. Доповідь про стан кібербезпеки в Україні за 2023 рік – Київ: ДССЗІ, 2024 – 120с.
15. Дорошенко С. І. Моделі оцінювання ризиків у фінансових процесах – Харків: ХНЕУ ім. Кузнеця, 2021–168 с.
16. ENISA. Cybersecurity Threat Landscape 2021– Heraklion: European Union Agency for Cybersecurity, 2021–186 p.
17. ENISA. ENISA Threat Landscape 2023–Heraklion: EU Agency for Cybersecurity, 2023 –198p.
18. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – ISMS Requirements. Geneva: ISO, 2022 – 41 p.
19. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection – Information security risk management. Geneva: ISO, 2022 – 76 p.
20. IBM Security. Cost of a Data Breach Report 2023 – New York: IBM Corporation, 2023 – 88 p.
21. ISACA. COBIT 2019 Framework: Governance and Management Objectives. Chicago: Information Systems Audit and Control Association, 2018 –134 p.
22. Freund J., Jones J. Measuring and Managing Information Risk: A FAIR Approach. Oxford: Butterworth-Heinemann (Elsevier), 2014 – 408 с.ISBN 978-0-12-420231-3.
23. Кабінет Міністрів України. Концепція розвитку цифрової економіки України: Розпорядження № 67-р від 17.01.2018 – Київ: КМУ, 2018 – 32 с.
24. Кириленко В. В. Ризики цифровізації бізнес-процесів: монографія – Київ: КНЕУ, 2022 – 256 с.
25. Коваленко Д. С. Інформаційні загрози та фінансова безпека підприємств – Дніпро: ДУ ім. Альфреда Нобеля, 2020 –176 с.
26. Костенко Т. Г. Кіберризики у корпоративному секторі – Київ: НАДУ, 2021– 144 с.
27. Мінцифра. Методичні рекомендації з управління кіберризиками – Київ: Міністерство цифрової трансформації України, 2022 – 56 с.

28. Мостовий О. Б. Захист інформаційних ресурсів підприємства: монографія – Київ: КНЕУ, 2019 – 204 с.
29. Microsoft Security. Digital Defense Report 2023 – Redmond: Microsoft Corporation, 2023 – 136 p.
30. NIST SP 800-30 Rev. 1. Guide for Conducting Risk Assessments – Gaithersburg, MD: NIST, 2022 – 95 p.
31. NIST SP 800-53 Rev. 5. Security and Privacy Controls for Information Systems – Gaithersburg: NIST, 2020 – 494 p.
32. NIST CSF 2.0. National Cybersecurity Framework – Gaithersburg: NIST, 2024 – 68p.
33. Омельченко А. І., Кузнецов В. П. Кіберризики у фінансовому секторі: методи оцінювання: навч. посіб. – Київ: КНЕУ, 2020 – 248 с.
34. Офіс Президента України. Стратегія кібербезпеки України на період до 2025 року: Указ Президента № 447/2021 – Київ: Офіційний вісник України. 2021 – No 70. Стор. 42. Ст. 4417.
35. Петренко О. В. Ризик-менеджмент у діяльності підприємств: навч. посіб. – Київ: КНЕУ, 2020 – 300 с.
36. PwC. Global Digital Trust Insights Report 2024 – London : PwC, 2024 – 72 p.
37. Palo Alto Networks. State of Cybersecurity 2023 – Santa Clara: PANW, 2023 – 112p.
38. RSA. Cybersecurity and Risk Report 2022 – Bedford: RSA Security, 2022 – 89 p.
39. SANS Institute. 2023 Cybersecurity Skills Survey – Bethesda: SANS, 2023 – 54 p.
40. Symantec. Internet Security Threat Report 2021 – Mountain View: Symantec Corp., 2021 – 102 p.
41. Sophos. State of Ransomware 2024 – Oxford: Sophos, 2024 – 66 p.
42. Trend Micro. Cybersecurity Annual Report 2023 – Tokyo: Trend Micro Inc., 2023 – 132 p.
43. Український інститут розвитку бізнесу. Кіберризики та цифрова економіка – Київ: УІРБ, 2023 – 164 с.

44. Урядовий портал. Національна програма кіберзахисту об'єктів критичної інфраструктури - Київ: Кабінет Міністрів, 2023 – Режим доступу: <https://www.kmu.gov.ua>. Дата звернення: 14.04.2026.
45. Федоренко А. В. Безпека інформаційних технологій: навч. посіб. – Київ: КНЕУ, 2020 –192 с.
46. Фінансовий клуб. Аналітичний звіт «Кіберризики фінансових установ 2023» – Київ: ФК, 2023 – 68 с.
47. Холоненко В. М. Цифрова безпека підприємства: монографія–Харків: ХНЕУ, 2022–220 с.
48. Шевченко А. О. Управління фінансовими ризиками в умовах цифровізації – Київ: КНЕУ, 2021– 256 с.
49. World Bank. Cybersecurity in Finance: Managing Digital Risks in Emerging Markets – Washington, DC: World Bank, 2022 –140 p.
50. World Economic Forum. Global Cybersecurity Outlook 2024 – Geneva: WEF, 2024 – 90 p.
51. Verizon. Data Breach Investigations Report 2024–New York: Verizon, 2024 – 98p.
52. Zscaler. ThreatLabZ 2023 Ransomware Report–San Jose: Zscaler Inc.,2023–74 p.
53. Національний банк України. Інформаційна політика НБУ щодо кіберзагроз –Київ: НБУ, 2024 – Режим доступу: <https://bank.gov.ua>. Дата звернення: 04.05.2026.

Метадані

ДОКУМЕНТ

Заголовок

КБР_Тригуб Є. В.

Автор

Тригуб Є. В.

Науковий керівник / Експерт

Труш М.

ІД документу

334256192

ОРГАНІЗАЦІЯ

Назва організації

Kyiv National Economic University named after Vadym Hetman
KNEU

підрозділ

кафедра системного аналізу та кібербезпеки

ЗВІТ

Дата звіту

6/10/2026

Дата редагування

Обсяг знайдених подібностей

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



КП 1

25

Довжина фрази для коефіцієнта подібності 2



КП 2

22132

Кількість слів



КЦ

176057

Кількість символів

Тривога

У цьому розділі ви знайдете інформацію щодо текстових спотворень. Ці спотворення в тексті можуть говорити про МОЖЛИВІ маніпуляції в тексті.

Спотворення в тексті можуть мати навмисний характер, але частіше характер технічних помилок при конвертації документа та його збереженні, тому ми рекомендуємо вам підходити до аналізу цього модуля відповідально. У разі виникнення запитань, просимо звертатися до нашої служби підтримки.

Заміна букв		1
Інтервали		0
Мікропробіли		39
Білі знаки		0
Парафрази (SmartMarks)		13

Джерела

Нижче наведений список джерел. В цьому списку є джерела із різних баз даних. Колір тексту означає в якому джерелі він був знайдений. Ці джерела і значення Коефіцієнту Подібності не відображають прямого плагіату. Необхідно відкрити кожне джерело і проаналізувати зміст і правильність оформлення джерела.

10 найдовших фраз	Колір тексту
#	НАЗВА ТА АДРЕСА ДЖЕРЕЛА URL (НАЗВА БАЗИ)
	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)

1	MODERN CYBER RISKS: THEIR CONCEPT, STRUCTURE AND APPLICATION IN THE FIELD OF COMMERCIAL SHIPPING Б. М. Орловський;	42 (0.19 %)
2	MODERN CYBER RISKS: THEIR CONCEPT, STRUCTURE AND APPLICATION IN THE FIELD OF COMMERCIAL SHIPPING Б. М. Орловський;	16 (0.07 %)
3	The process of declaring information security profiles M.V. Yesina, O.V. Potii, D.Yu. Golubnychiy, Yu.K. Vasiliev;	15 (0.07 %)
4	https://www.ukrbanks.info/article/Sertifikaciya-ISO-27001-27701-Sho-ce-take-i-chomu-vona-vazhliva.html	12 (0.05 %)
5	https://www.linkedin.com/pulse/%D0%BC%D0%BE%D0%B4%D0%B5%D1%80%D0%BD%D1%96%D0%B7%D0%B0%D1%86%D1%96%D1%8F-%D0%BA%D1%81%D0%B7%D1%96-%D1%87%D0%B8-%D1%81%D1%82%D0%B0%D0%BD%D0%B4%D0%B0%D1%80%D1%82%D0%B8-nist-ivan-gokin-beh7f	12 (0.05 %)
6	ММГКТС2024-1_ПЗ_Ахматжанова З. Б. 12/19/2025 O.M.Beketov National University of Urban Economy in Kharkiv (O.M.Beketov National University of Urban Economy in Kharkiv)	11 (0.05 %)
7	https://commons.erau.edu/cgi/viewcontent.cgi?article=1438&context=edt	10 (0.05 %)
8	Кур_роб_Пилипенко_С_М(ФБССФР_бд_22) 4/17/2026 Poltava State Agrarian Academy (PSAA) (Deanary)	10 (0.05 %)
9	Технологія побудови комплексної системи захисту інформації приватного підприємства 5/30/2026 Ukrainian national aviation university (ФАЕТ Кафедра телекомунікаційних та радіоелектронних систем)	8 (0.04 %)
10	076-Репетацький_Сергій_Юрійович-2025 11/30/2025 Donetsk National University named after V. Stus (Vasyl Stus DonNU)	7 (0.03 %)

База даних RefBooks (0.33 %)



#	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
джерело: Paperity		
1	MODERN CYBER RISKS: THEIR CONCEPT, STRUCTURE AND APPLICATION IN THE FIELD OF COMMERCIAL SHIPPING Б. М. Орловський;	58 (2) (0.26 %)
2	The process of declaring information security profiles M.V. Yesina, O.V. Potii, D.Yu. Golubnychiy, Yu.K. Vasiliev;	15 (1) (0.07 %)

Домашня база даних



#	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
Програма обміну базами даних (0.31 %)		
#	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)

3	УПРАВЛІННЯ ЕНЕРГЕТИЧНОЮ БЕЗПЕКОЮ УКРАЇНИ НА ЗАСАДАХ СТАЛОГО РОЗВИТКУ 1/15/2026 Khmelnitskyi National University (Кафедра економіки, аналітики, моделювання та інформаційних технологій в бізнесі)	21 (4) (0.09 %)
4	Технологія побудови комплексної системи захисту інформації приватного підприємства 5/30/2026 Ukrainian national aviation university (ФАЕТ Кафедра телекомунікаційних та радіоелектронних систем)	14 (2) (0.06 %)
5	076-Репетацький_Сергій_Юрійович-2025 11/30/2025 Donetsk National University named after V. Stus (Vasyl Stus DonNU)	13 (2) (0.06 %)
6	ММГКТС2024-1_ПЗ_Ахматжанова З. Б. 12/19/2025 O.M.Beketov National University of Urban Economy in Kharkiv (O.M.Beketov National University of Urban Economy in Kharkiv)	11 (1) (0.05 %)
7	Кур_роб_Пилипенко_С_М(ФБССФР_бд_22) 4/17/2026 Poltava State Agrarian Academy (PSAA) (Deanary)	10 (1) (0.05 %)
Інтернет (0.18 %)		
#	ДЖЕРЕЛО URL	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
8	https://www.linkedin.com/pulse/%D0%BC%D0%BE%D0%B4%D0%B5%D1%80%D0%BD%D1%96%D0%B7%D0%B0%D1%86%D1%96%D1%8F-%D0%BA%D1%81%D0%B7%D1%96-%D1%87%D0%B8-%D1%81%D1%82%D0%B0%D0%BD%D0%B4%D0%B0%D1%80%D1%82%D0%B8-nist-ivan-gokin-beh7f	18 (2) (0.08 %)
9	https://www.ukrbanks.info/article/Sertifikaciya-ISO-27001-27701-Sho-ce-take-i-chomu-vona-vazhliva.html	12 (1) (0.05 %)
10	https://commons.erau.edu/cgi/viewcontent.cgi?article=1438&context=edt	10 (1) (0.05 %)
 Список принятых фрагментів		
#	ЗМІСТ	КІЛЬКІСТЬ ОДНАКОВИХ СЛІВ (ФРАГМЕНТІВ)