МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “МОДЕЛЬ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У КОНТЕКСТІ БЕЗПЕРЕРВНОСТІ БІЗНЕСУ”

на здобуття освітнього ступеня магістра
зі спеціальності 125 Кібербезпека та захист інформації
освітньо-професійної програми Управління інформаційною та кібернетичною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Олексій МИКОЛАЄНКО

(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБДМ-61
Олексій МИКОЛАЄНКО

Керівник:
д.т.н., професор Іван ОПІРСЬКИЙ
Ім’я, ПРІЗВИЩЕ

Рецензент:

Ім’я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра Управління кібербезпекою та захистом інформації
Ступінь вищої освіти магістр
Спеціальність 125 Кібербезпека та захист інформації
Освітньо-професійна програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедрою УКБЗІ
_____ Світлана ЛЕГОМІНОВА
"____" _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Студенту Миколаєнку Олексію Сергійовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: "Модель управління ризиками інформаційної безпеки у контексті безперервності бізнесу"

керівник кваліфікаційної роботи Іван ОПІРСЬКИЙ, д.т.н., професор.
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від "30" жовтня 2025 р. № 467.

2. Строк подання кваліфікаційної роботи "11" грудня 2025 р.
3. Вихідні дані до кваліфікаційної роботи:.
4. Перелік питань, які потрібно розробити:
   1.Проаналізувати проблемну сферу управління ризиками інформаційної безпеки в контексті безперервності бізнесу.
   2. Розробити модель управління ризиками інформаційної безпеки в контексті забезпечення безперервності бізнесу.
   3. Дослідити та оцінити ефективність запропонованої моделі.
5. Перелік ілюстративного матеріалу: *презентація*
6. Дата видачі завдання "02" жовтня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назви етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	10.10.2025	
2.	Збір та аналіз літератури.	23.10.2025	
3.	Аналіз проблемної сфери управління ризиками інформаційної безпеки в контексті безперервності бізнесу	27.10.2025	
4.	Розробка моделі управління ризиками інформаційної безпеки в контексті забезпечення безперервності бізнесу	10.11.2025	
5.	Дослідження та оцінка ефективності запропонованої моделі	15.11.2025	
6.	Формулювання висновків за результатами дослідження.	22.11.2025	
7.	Оформлення роботи.	04.12.2025	
8.	Оформлення презентації.	14.12.2025	
9.	Отримання рецензії на роботу.	18.12.2025	
10.	Захист в ЕК.	__.01.2026	

Здобувач вищої освіти _____ Олексій МИКОЛАЄНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Іван ОПІРСЬКИЙ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Миколаєнко О.С. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека та захист інформації
(код, найменування спеціальності)
Освітньо-професійної програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Модель управління ризиками інформаційної безпеки у контексті безперервності бізнесу"
Кваліфікаційна робота і рецензія додаються.

Директор ННІКБЗІ _____ Євгенія ІВАНЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач **МИКОЛАЄНКО Олексій** у кваліфікаційній роботі проаналізував проблемну сферу управління ризиками інформаційної безпеки в контексті безперервності бізнесу, розробив модель управління ризиками інформаційної безпеки в контексті забезпечення безперервності бізнесу, а також дослідив та оцінив ефективність запропонованої моделі.

МИКОЛАЄНКО Олексій показав високу теоретичну і практичну підготовку, володіння науково-дослідницькими методами, вміння самостійно знаходити шляхи вирішення проблеми дослідження. Результати дослідження апробовані на конференції "Стратегії кіберстійкості: управління ризиками та безперервність бізнесу" 27 лютого 2025 року.

Все це дозволяє оцінити кваліфікаційну роботу здобувача **МИКОЛАЄНКА Олексія** на оцінку "добре" та присвоїти йому кваліфікацію "Магістр з кібербезпеки та захисту інформації за освітньо-професійною програмою Управління інформаційною та кібернетичною безпекою".

Керівник кваліфікаційної роботи _____ Іван ОПІРСЬКИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____"_____2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Миколаєнко О.С. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедрою
Управління кібербезпекою та захистом
інформації _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну магістерську роботу

здобувача вищої освіти Миколаєнка Олексія Сергійовича
на тему "Модель управління ризиками інформаційної безпеки у контексті безперервності бізнесу"

Актуальність Сучасні підприємства та організації функціонують у складному інформаційному середовищі, де постійно зростає обсяг цифрових даних і водночас підвищується рівень кіберзагроз. Різноманітні види ризиків інформаційної безпеки, зокрема кібератаки, витоки даних, технічні збої та внутрішні загрози, здатні порушити критично важливі бізнес-процеси та завдати фінансових і репутаційних втрат. Тому розробка ефективної моделі управління ризиками інформаційної безпеки, інтегрованої з процесами забезпечення безперервності бізнесу, є надзвичайно актуальною науково-практичною проблемою. Запровадження такої моделі дозволяє не лише прогнозувати потенційні загрози, а й мінімізувати їхній вплив, забезпечуючи стабільність і стійкість організації в умовах динамічного інформаційного середовища.

Позитивні сторони

1. У роботі детально досліджено основи управління ризиками інформаційної безпеки та їх вплив на безперервність бізнесу, проведено системний аналіз існуючих моделей, визначено їхні сильні і слабкі сторони. Розроблено класифікацію ризиків та представлено схему взаємозв'язку між різними видами загроз і бізнес-процесами, що дозволяє організації ефективніше планувати заходи захисту.

2. Кваліфікаційна робота оформлена відповідно до вимог, матеріал викладено логічно та послідовно, зроблено чіткі висновки. Ключові положення представлені у вигляді схем, таблиць та графіків. Автор опрацював значну джерельну базу: близько 60 публікацій та електронних ресурсів, включаючи англомовні джерела з галузі інформаційної безпеки та управління ризиками.

3. На основі проведеного дослідження запропоновано практичні рекомендації щодо впровадження моделі управління ризиками інформаційної безпеки в організаціях, що дозволяє забезпечити адаптивний захист критичних бізнес-процесів і підтримати безперервність діяльності навіть за умов реалізації загроз.

Недоліки

1. Доцільно було б приділити більше уваги деталізації методів інтеграції моделі управління ризиками з існуючими процесами безперервності бізнесу, а також адаптації запропонованих підходів до специфіки різних галузей і розмірів організацій.

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує позитивної оцінки, а здобувач Миколаєнко Олексій Сергійович заслуговує присвоєння кваліфікації "Магістр кібербезпеки за освітньо-професійною програмою "Управління інформаційною безпекою".

Рецензент:

_____
підпис *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 73 стор., 6 рис., 17 табл., 50 джерел.

Метою роботи є дослідження засад управління ризиками інформаційної безпеки та розробка моделі, що забезпечує інтеграцію цих процесів із безперервністю бізнесу.

Об'єктом дослідження є процеси управління інформаційною безпекою в організаціях та їх вплив на стабільність і безперервність бізнес-процесів.

Предмет дослідження – методи оцінки, мінімізації та контролю ризиків інформаційної безпеки в контексті забезпечення безперервності бізнесу.

Методи дослідження. Для вирішення завдань оцінки та управління ризиками інформаційної безпеки використовувалися методи системного аналізу, теорії складних систем та мереж, теорія ймовірностей і статистичні методи, а також підходи управління ризиками за міжнародними стандартами. Для моделювання взаємозв'язків між бізнес-процесами, інформаційними активами та ризиками застосовувалися методи системного моделювання та побудови сценаріїв, що дозволяє прогнозувати потенційні загрози та оцінювати ефективність заходів з їх мінімізації.

Короткий зміст роботи. Як результат у роботі проаналізовано проблемну сферу управління ризиками інформаційної безпеки в контексті безперервності бізнесу, розроблено модель управління ризиками інформаційної безпеки в контексті забезпечення безперервності бізнесу, а також досліджено та оцінено ефективність запропонованої моделі.

Галузь застосування. Розроблені підходи можуть бути використані при плануванні, впровадженні та оптимізації системи управління ризиками інформаційної безпеки організації з урахуванням забезпечення безперервності бізнес-процесів. Модель дозволяє інтегрувати оцінку ризиків, контроль загроз та заходи з відновлення діяльності, що особливо актуально для підприємств із критично важливими бізнес-процесами та інформаційними активами.

КЛЮЧОВІ СЛОВА: ІНФОРМАЦІЙНА БЕЗПЕКА, УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, БЕЗПЕРЕРВНІСТЬ БІЗНЕСУ, МОДЕЛЬ УПРАВЛІННЯ РИЗИКАМИ, ОЦІНКА ТА МІНІМІЗАЦІЯ РИЗИКІВ, КРИТИЧНІ БІЗНЕС-ПРОЦЕСИ.

ABSTRACT

The text part of the qualification work for obtaining a master's degree: 73 pages, 6 figures, 17 tables, 50 sources.

The purpose of the work is to study the principles of information security risk management and develop a model that ensures the integration of these processes with business continuity.

Object of research is the processes of information security management in organisations and their impact on the stability and continuity of business processes.

Subjec*t ***of research is methods for assessing, minimising and controlling information security risks in the context of ensuring business continuity.

Research methods To solve the tasks of assessing and managing information security risks, methods of system analysis, complex systems and networks theory, probability theory and statistical methods, as well as risk management approaches in accordance with international standards were used. To model the relationships between business processes, information assets and risks, methods of system modelling and scenario building were used, which allow predicting potential threats and assessing the effectiveness of measures to minimise them.

Brief content of research. As a result, the work analyses the problematic area of information security risk management in the context of business continuity, develops a model for managing information security risks in the context of ensuring business continuity, and researches and evaluates the effectiveness of the proposed model.

Field of research. The developed approaches can be used in planning, implementing, and optimising an organisation's information security risk management system, taking into account the need to ensure business continuity. The model allows for the integration of risk assessment, threat control, and business recovery measures, which is particularly relevant for enterprises with critical business processes and information assets.

KEYWORDS: INFORMATION SECURITY, INFORMATION SECURITY RISK MANAGEMENT, BUSINESS CONTINUITY, RISK MANAGEMENT

MODEL, RISK ASSESSMENT AND MINIMISATION, CRITICAL BUSINESS PROCESSES.

ЗМІСТ

ВСТУП

Актуальність теми. Бізнес-організації та підприємства будь-якого масштабу дедалі більше залежать від безперебійного функціонування своїх інформаційних систем, які забезпечують критично важливі бізнес-процеси. З огляду на постійне зростання складності, кількості та цілеспрямованості кіберзагроз, управління ризиками інформаційної безпеки стає ключовим елементом забезпечення стабільності та безперервності бізнесу. Недостатній рівень контролю за інформаційними ризиками може призвести до збоїв у роботі підприємства, фінансових втрат, шкоди репутації та навіть порушення законодавчих вимог.

Сучасні технології управління інформаційною безпекою, зокрема автоматизовані системи оцінки ризиків та моніторингу загроз, відкривають нові можливості для підвищення ефективності процесів управління. Вони дозволяють обробляти великі обсяги даних, виявляти потенційні загрози, оцінювати їхній вплив на бізнес-процеси та приймати обґрунтовані управлінські рішення щодо мінімізації ризиків. Водночас застосування таких технологій потребує розробки науково обґрунтованих моделей управління ризиками, які враховують специфіку організацій, критичні активи та залежності між бізнес-процесами.

У зв’язку з цим розробка моделі управління ризиками інформаційної безпеки, інтегрованої з процесами забезпечення безперервності бізнесу, є актуальним науково-практичним завданням. Впровадження такої моделі дозволяє підвищити стійкість організації до інцидентів інформаційної безпеки, забезпечити безперервність критичних бізнес-процесів та сприяти стратегічному розвитку підприємства в умовах сучасного інформаційно-насиченого середовища.

Мета роботи полягає у дослідженні засад управління ризиками інформаційної безпеки та розробка моделі, що забезпечує інтеграцію цих процесів із безперервністю бізнесу.

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання**:

1. Проаналізувати проблемну сферу управління ризиками інформаційної безпеки в контексті безперервності бізнесу.

2. Розробити модель управління ризиками інформаційної безпеки в контексті забезпечення безперервності бізнесу.

3. Дослідити та оцінити ефективність запропонованої моделі.

Об'єкт дослідження **–** процеси управління інформаційною безпекою в організаціях та їх вплив на стабільність і безперервність бізнес-процесів.

Предмет дослідження – методи оцінки, мінімізації та контролю ризиків інформаційної безпеки в контексті забезпечення безперервності бізнесу.

Методи дослідження. Аналіз і синтез – для опрацювання наукових публікацій, міжнародних та національних стандартів і рекомендацій у сфері управління ризиками інформаційної безпеки та забезпечення безперервності бізнесу, а також для формування цілісного уявлення про сучасні підходи до інтеграції управління ризиками та процесів бізнес-стійкості.

Системний та структурно-функціональний аналіз – для дослідження організацій та їхніх інформаційних систем як складних соціотехнічних систем, визначення взаємозв'язків між бізнес-процесами, інформаційними активами та ризиками, а також оцінки впливу цих ризиків на безперервність бізнесу.

Порівняльний аналіз – для зіставлення існуючих моделей управління ризиками інформаційної безпеки та визначення можливостей їх удосконалення шляхом інтеграції з процесами забезпечення безперервності бізнесу та адаптивного реагування на загрози.

Метод експертних оцінок – для визначення вагових коефіцієнтів критеріїв ризиків, пріоритетності загроз та ефективності заходів мінімізації ризиків, а також для оцінки практичної доцільності застосування запропонованої моделі у конкретних організаційних умовах.

Моделювання – для розроблення та апробації моделі управління ризиками інформаційної безпеки в контексті безперервності бізнесу, включаючи етапи ідентифікації ризиків, їх оцінки, формування інтегральних показників ризику,

розробки заходів мінімізації та контролю, а також для прогнозування впливу ризиків на критичні бізнес-процеси та ефективності заходів захисту.

Наукова новизна роботи полягає в тому, що розроблено інтегровану модель управління ризиками інформаційної безпеки, що забезпечує поєднання оцінки ризиків, заходів контролю та мінімізації загроз із процесами забезпечення безперервності бізнесу. Запропоновано методику кількісної та якісної оцінки ризиків, яка враховує технологічні, організаційні, людські та процесні аспекти інформаційної безпеки. Удосконалено підхід до визначення пріоритетів ризиків та формування ефективних заходів реагування, що дозволяє не лише зменшити негативний вплив загроз на бізнес-процеси, а й підвищити адаптивність організації до нових та змінних кіберзагроз. Розроблена модель інтегрує оцінку ризиків із моніторингом та управлінням безперервністю бізнесу, що забезпечує комплексний, системний та практично застосовний підхід до управління інформаційною безпекою.

Практичне значення одержаних результатів. Застосування розробленої моделі управління ризиками інформаційної безпеки в контексті безперервності бізнесу дозволяє організаціям проводити обґрунтовану оцінку ризиків, визначати пріоритетні загрози та ефективно планувати заходи з їх мінімізації. Модель забезпечує інтеграцію процесів оцінки, контролю та реагування на ризики з безперервністю критичних бізнес-процесів, що сприяє підвищенню стійкості організації до інцидентів та кіберзагроз.

Отримані результати можуть бути використані під час розробки та вдосконалення систем управління інформаційною безпекою, включно з автоматизованим моніторингом інцидентів, виявленням вразливостей, прогнозуванням потенційних загроз і формуванням рекомендацій щодо мінімізації їхнього впливу на бізнес-процеси. Запропонована модель може бути інтегрована в діяльність центрів моніторингу безпеки, систем управління інформаційною безпекою та процеси управління безперервністю бізнесу. Крім того, результати дослідження сприятимуть розробці та актуалізації внутрішніх політик і процедур управління ризиками інформаційної безпеки відповідно до

міжнародних стандартів та нормативних документів, а також забезпечать практичну основу для прийняття управлінських рішень щодо підвищення стійкості організації та ефективності захисту критично важливих бізнес-процесів.

Апробація результатів кваліфікаційної роботи відбулася на конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 27 лютого 2025 року.

РОЗДІЛ 1
АНАЛІЗ ПРОБЛЕМНОЇ СФЕРИ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КОНТЕКСТІ БЕЗПЕРЕРВНОСТІ БІЗНЕСУ

Забезпечення безперервності бізнесу набуває стратегічного значення для організацій різних секторів. Інформаційні активи стають критичною складовою операційної стійкості, а порушення їх конфіденційності, цілісності чи доступності безпосередньо впливає на здатність підприємства підтримувати ключові бізнес-процеси. Це зумовлює необхідність формування ефективних підходів до управління ризиками інформаційної безпеки, які враховують взаємозв'язок між технічними, організаційними та процесними чинниками. У межах цього розділу здійснюється аналіз проблемної сфери управління ризиками інформаційної безпеки в контексті безперервності бізнесу, що створює основу для подальшої розробки моделі, спрямованої на мінімізацію впливу інцидентів та підвищення стійкості організації до сучасних загроз.

1.1 Поняття, сутність та класифікація ризиків інформаційної безпеки

Управління ризиками інформаційної безпеки є фундаментальним компонентом системи забезпечення сталого функціонування організації в умовах зростаючої залежності бізнес-процесів від інформаційних технологій та цифрових активів. Формування ефективної стратегії реагування на кіберзагрози починається з чіткого розуміння сутності ризику, його ключових характеристик, чинників формування та класифікаційних ознак [1]. Відповідно до міжнародних стандартів, зокрема ISO/IEC 27005 та ISO 31000, ризик трактується як комбінація ймовірності виникнення інциденту інформаційної безпеки та масштабів його негативного впливу на діяльність організації. Такий підхід дозволяє оцінювати ризики з позиції потенційних втрат з урахуванням стратегічної стійкості підприємства та його здатності забезпечувати безперервність виконання критичних операцій.

З концептуальної точки зору ризик інформаційної безпеки є наслідком взаємодії трьох базових компонентів: активів, загроз і вразливостей. Активи можуть мати матеріальний (обладнання, інфраструктура) і нематеріальний (дані, репутація, ноу-хау) характер; загрози формуються як умисними діями порушників, так і техногенними чи природними чинниками; вразливості є слабкими місцями системи, які можуть бути використані для реалізації загроз [2]. Взаємозв'язок між цими елементами створює умови для виникнення інцидентів, які за певних обставин здатні перерости у критичні порушення бізнес-процесів (рис. 1.1).

Рис. 1.1 Класична модель взаємодії ключових елементів ризику інформаційної безпеки

Сутність ризиків інформаційної безпеки полягає у можливості нанесення шкоди інформаційним активам і, як наслідок, у зниженні рівня операційної ефективності, фінансової стабільності, правової відповідності та ділової репутації. У контексті безперервності бізнесу це особливо важливо, оскільки інформаційні інциденти можуть призвести до тривалих простоїв, збоїв у функціонуванні сервісів, втрати керованості процесами та зупинки критичних операцій, що безпосередньо впливає на ринкову позицію підприємства та його здатність виконувати зобов'язання перед клієнтами й партнерами [3].

Варто зазначити, що ризики інформаційної безпеки володіють певними характерними властивостями, які необхідно враховувати при їх аналізі та управлінні [4]:

1. **Динамічність**, що проявляється у постійному виникненні нових уразливостей, зміні моделей атак і розширенні цифрового середовища.

2. **Невизначеність**, обумовлена складністю передбачення дій атакувальників та швидкістю трансформації цифрових технологій.

3. **Багатовимірність**, яка характеризує взаємодію технічних, організаційних, людських і зовнішніх чинників.

4. **Системність**, оскільки інциденти часто впливають не на окремий актив, а на весь ланцюг пов'язаних бізнес-процесів.

5. **Кумулятивність**, що означає накопичення дрібних уразливостей, які можуть призвести до масштабного порушення.

Для коректної побудови процесу управління ризиками необхідно застосовувати чітку класифікацію ризиків. Це дає змогу сегментувати їх за різними ознаками та застосовувати релевантні заходи реагування [5]. Одним із найбільш поширених підходів є класифікація ризиків за їх походженням, що включає технічні, організаційні, людські, природні та зовнішні (екзогенні) ризики (табл. 1.1).

Таблиця 1.1

Класифікація ризиків ІБ за походженням

Категорія ризику	Характеристика	Приклади
Технічні	Пов'язані з відмовами ІТ-систем	Збій серверів, помилки ПЗ
Організаційні	Недоліки процедур та політик	Невірні права доступу
Людські	Дії та помилки персоналу	Phishing, інсайдерські атаки
Природні	Стихійні та техногенні події	Пожежі, затоплення
Зовнішні	Ризики від третіх сторін	Компрометація партнерів

Технічні ризики охоплюють інциденти, пов’язані з відмовами апаратного забезпечення, помилками програмного забезпечення, збоями мережевої інфраструктури, порушенням цілісності даних через технічні несправності. Вони є типовими для інфраструктур, що характеризуються високим рівнем автоматизації та складністю архітектури. Наявність технічних ризиків часто корелює з життєвим циклом ІТ-компонентів та адекватністю процесів технічної підтримки.

Організаційні ризики пов’язані з недосконалістю внутрішніх політик, процедур, регламентів і процесів управління інформаційною безпекою. До них належать неадекватні правила доступу, відсутність механізмів моніторингу, слабкість процесів контролю змін, недостатність аудитів, неузгодженість управлінських рішень. Організаційні ризики часто стають першопричиною масштабних інцидентів, оскільки визначають ефективність системи безпеки загалом.

Людські ризики є наслідком помилок персоналу, зловмисних дій співробітників, соціальної інженерії, браку компетенцій або порушення трудової дисципліни. У сучасних компаніях саме людський фактор є критично значущим, оскільки близько 60–80 % інцидентів пов’язані з діями співробітників різного рівня [6]. Ці ризики можуть бути як ненавмисними (помилки, випадкові порушення), так і навмисними (інсайдерські атаки).

Природні та техногенні ризики включають стихійні лиха, аварії на об’єктах інфраструктури, пожежі та інші події, що мають зовнішній характер і можуть спричинити значні втрати доступності даних та ІТ-сервісів. З огляду на безперервність бізнесу вони є одним із ключових об’єктів аналізу, оскільки здатні обумовити повну недоступність критичних систем.

Зовнішні ризики, пов’язані з діяльністю третіх сторін, включають взаємодію з контрагентами, постачальниками та сервіс-провайдерами, зокрема у разі використання хмарних сервісів або аутсорсингових моделей. Недостатня зрілість системи безпеки партнера може спричинити компрометацію даних компанії або порушення критичних процесів [7].

Крім класифікації за походженням, ризики інформаційної безпеки поділяють за типом впливу на бізнес-процеси, що дає змогу оцінювати масштаб їх впливу на безперервність діяльності (табл. 1.2).

Таблиця 1.2

Класифікація ризиків за типом впливу

Тип впливу	Сутність	Можливі наслідки
Фінансові	Прямі і непрямі збитки	Штрафи, втрати від простоїв
Операційні	Збої у бізнес-процесах	Недоступність сервісів
Юридичні	Порушення нормативів	Санкції, судові позови
Репутаційні	Падіння довіри	Втрата клієнтів
Стратегічні	Порушення довгострокових цілей	Зниження конкурентності

До основних типів впливу належать [8]:

1. **Фінансові ризики**, що проявляються у прямих і непрямих збитках, пов’язаних із ліквідацією інцидентів, штрафами регуляторів, втратами від простоїв і порушення договірних зобов’язань.

2. **Операційні ризики**, які зумовлюють збої у критичних бізнес-процесах, недоступність сервісів, порушення логістичних або виробничих ланцюгів.

3. **Юридичні ризики**, пов’язані з порушенням вимог законодавства та нормативних актів, насамперед у сфері захисту персональних даних.

4. **Репутаційні ризики**, що впливають на рівень довіри клієнтів, партнерів та інвесторів.

5. **Стратегічні ризики**, пов’язані зі зниженням конкурентоспроможності та порушенням довгострокових цілей розвитку підприємства.

Окремо варто виокремити класифікацію ризиків залежно від способу реалізації загрози. Цей підхід дозволяє врахувати характер шкідливих дій та моделі атак. Зокрема, розрізняють (рис. 1.2):

- кібератаки (DDoS, phishing, ransomware, SQL-injection, APT-атаки);
- інсайдерські загрози (навмисні чи помилкові дії співробітників);
- компрометацію облікових даних;
- зловживання довіреними відносинами;
- фізичні загрози (несанкціонований доступ до приміщень, крадіжка обладнання);
- загрози ланцюгів постачання [9].

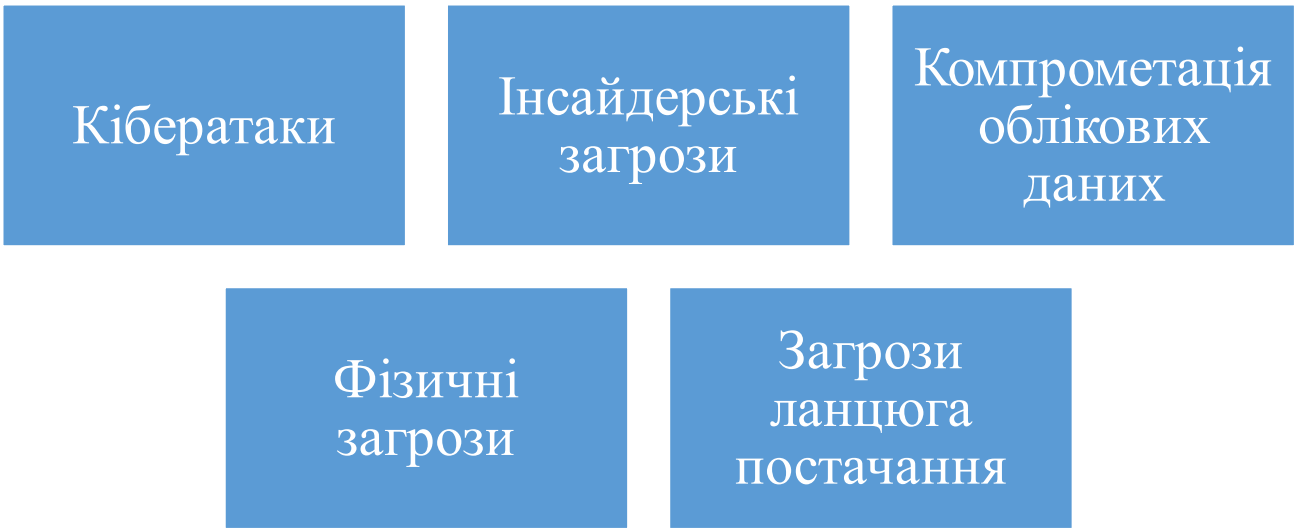

Рис. 1.2 Класифікація ризиків ІБ за способом реалізації загроз»

У контексті забезпечення безперервності бізнесу критично важливим є також віднесення ризиків до категорій залежно від часу впливу та відновлення. Такий підхід використовується у практиці Business Continuity Management (BCM) і Disaster Recovery (DR), де ризики оцінюються з урахуванням [10]:

- Recovery Time Objective (RTO) – максимальний допустимий час відновлення сервісу;
- Recovery Point Objective (RPO) – допустима втрата даних у часі;
- Maximum Tolerable Downtime (MTD) – граничний час, протягом якого бізнес може функціонувати в умовах відмови.

Ризики, які здатні спричинити перевищення цих показників, вважаються критичними і потребують негайного впровадження компенсуючих заходів.

Узгодженість класифікації ризиків з моделлю безперервності бізнесу дозволяє застосовувати методи пріоритизації, зокрема аналіз критичності (BIA – Business Impact Analysis). Це забезпечує можливість виділення ризиків, що потребують першочергового реагування, та оптимізації витрат на безпеку, оскільки ресурси спрямовуються на захист саме тих активів, які мають найбільший вплив на стабільність бізнесу [11].

Поняття і класифікація ризиків інформаційної безпеки формують методологічну основу для подальших етапів управління, включаючи оцінку, моніторинг і розробку заходів реагування. У контексті безперервності бізнесу систематизація ризиків дозволяє інтегрувати процеси IT-безпеки з корпоративними механізмами стратегічного та операційного планування, що сприяє підвищенню стійкості організації до інцидентів, які можуть порушити стабільність її роботи.

1.2 Аналіз існуючих моделей управління ризиками інформаційної безпеки

Управління ризиками інформаційної безпеки є ключовим елементом системи забезпечення стійкого функціонування організації в умовах зростаючої залежності бізнес-процесів від інформаційних технологій та цифрових активів. В умовах інтенсивного розвитку кіберзагроз організації змушені впроваджувати структуровані підходи до виявлення, оцінки та обробки ризиків, спрямовані на зниження ймовірності виникнення інцидентів і забезпечення оперативного відновлення критично важливих бізнес-процесів [12]. Розробка та застосування моделей управління ризиками базується на системному аналізі взаємодії активів, загроз, вразливостей та потенційного впливу інцидентів на організацію.

Моделі управління ризиками інформаційної безпеки формуються на основі міжнародних стандартів, національних методик, а також на практичному досвіді провідних організацій у сфері кібербезпеки. Вони надають керівництво щодо визначення об’єктів захисту, оцінки рівня їх уразливості, прогнозування ймовірності загроз та масштабів їхнього впливу на діяльність організації [13].

Основна мета таких моделей полягає у створенні інтегрованої системи управління ризиками, яка дозволяє організації ефективно використовувати ресурси для захисту інформаційних активів і забезпечення безперервності бізнес-процесів.

Серед міжнародних стандартів, що визначають принципи управління ризиками, найбільш поширеними є ISO/IEC 27005:2018, ISO 31000:2018, NIST SP 800-30/800-37, а також кількісні та організаційні методики, такі як FAIR, OCTAVE та EBIOS [14]. Кожна з цих моделей має власну специфіку, проте їх об'єднує системний підхід до управління ризиками, що включає ідентифікацію активів, виявлення загроз та вразливостей, оцінку ймовірності та наслідків інцидентів, визначення пріоритетності ризиків і планування заходів щодо їх обробки.

ISO/IEC 27005

ISO/IEC 27005 є частиною системи менеджменту інформаційної безпеки (ISMS) і надає структуровану методологію для управління ризиками інформаційної безпеки. Основні етапи процесу включають (рис. 1.3):

1. Ідентифікацію активів – визначення критично важливих інформаційних ресурсів, включаючи дані, програмне забезпечення, апаратні засоби та репутацію організації.

2. Ідентифікацію загроз і вразливостей – аналіз потенційних загроз (зловмисних дій, технічних відмов, природних явищ) та слабких місць системи безпеки.

3. Оцінку ризику – визначення ймовірності настання інцидентів та масштабів їхнього впливу на бізнес-процеси.

4. Обробку ризику – прийняття рішень щодо уникнення, зменшення, перенесення або прийняття ризику.

5. Моніторинг та перегляд – постійний контроль ефективності обробки ризиків та оновлення моделі у відповідності до змін зовнішнього і внутрішнього середовища організації.

ISO/IEC 27005 забезпечує уніфікований підхід до управління ризиками, інтегруючи його з політиками та процедурами ISMS, що дозволяє організаціям системно реагувати на нові загрози та підвищувати стійкість бізнес-процесів [15].

Рис. 1.3 Цикл управління ризиками за ISO/IEC 27005

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)

OCTAVE – методика, розроблена CERT/SEI, орієнтована на організаційний рівень управління ризиками. Основна особливість OCTAVE полягає в стратегічному підході до оцінки критичності активів та бізнес-процесів, що дозволяє організації виділяти пріоритетні сфери захисту. Методика включає три основні фази:

1. Стратегічне оцінювання – аналіз організаційної структури, бізнес-процесів та ключових активів.
2. Технологічна оцінка – виявлення технічних уразливостей та оцінка їхнього потенційного впливу.
3. Розробка планів дій – визначення заходів щодо мінімізації ризиків та планування ресурсів для їх реалізації.

OCTAVE є корисним інструментом для комплексної оцінки організаційних ризиків, оскільки забезпечує врахування технічних аспектів, організаційних процесів і людського фактора [16].

NIST SP 800-30 / 800-37

Національний інститут стандартів і технологій США (NIST) розробив серію керівництв для управління ризиками, орієнтованих на державні та приватні організації. Основні етапи NIST включають:

1. Ідентифікацію активів та загроз.
2. Аналіз вразливостей.
3. Оцінку ризику.
4. Обробку та реагування.
5. Моніторинг та оновлення ризиків.

NIST SP 800-30/37 відрізняються високим ступенем деталізації та наданням конкретних практичних рекомендацій для оцінки ризиків, що робить їх особливо корисними у регульованих секторах [17].

FAIR (Factor Analysis of Information Risk)

FAIR – кількісна модель, яка дозволяє оцінити фінансовий вплив ризиків інформаційної безпеки. На відміну від ISO/IEC 27005 та OCTAVE, FAIR орієнтована на кількісну оцінку ймовірності та наслідків інцидентів, що дозволяє інтегрувати ризики ІБ у загальну фінансову модель організації. Основні компоненти FAIR:

- події ризику (Risk Events);
- вразливості (Vulnerabilities);
- ймовірність настання (Probability);
- втрати / наслідки (Loss Magnitude).

FAIR дозволяє отримати точні фінансові показники потенційних збитків, що сприяє оптимізації витрат на інформаційну безпеку та пріоритизації заходів захисту [18].

EBIOS – методика, яка поєднує аналіз потреб безпеки та оцінку ризиків з визначенням цілей захисту. Основні етапи:

1. Аналіз контексту – оцінка середовища та умов функціонування організації.
2. Оцінка ризиків – ідентифікація загроз, вразливостей та потенційних наслідків.
3. Визначення цілей безпеки – формулювання політик та вимог до захисту.

4. Планування заходів – розробка стратегії управління ризиками та реалізації контролів.

EBIOS дозволяє поєднувати якісну та контекстну оцінку ризиків, що особливо цінно для підприємств з високими вимогами до безперервності бізнесу [19].

Порівняльний аналіз моделей

Загальний аналіз існуючих моделей показує, що кожна з них має свої сильні та слабкі сторони. ISO/IEC 27005 та NIST SP забезпечують структуровані процеси управління ризиками, OCTAVE та EBIOS орієнтовані на бізнес-процеси та організаційний контекст, тоді як FAIR дозволяє кількісно оцінити фінансові наслідки (табл. 1.3). Для забезпечення безперервності бізнесу доцільно застосовувати комбінований підхід, який поєднує організаційні, технічні та фінансові аспекти оцінки ризиків [20].

Таблиця 1.3

Переваги та обмеження моделей управління ризиками

Модель	Переваги для бізнесу	Обмеження при впровадженні
ISO/IEC 27005	стандартна методика, інтеграція з isms	потребує адаптації
OCTAVE	орієнтація на критичні активи	трудомістка реалізація
FAIR	кількісна оцінка, фінансовий фокус	необхідні дані та експерти
EBIOS	врахування бізнес-потреб	складність для малих організацій
NIST SP 800-30	детальні керівництва	часто використовується в державному секторі

1.3 Порівняльний аналіз моделей управління ризиками інформаційної безпеки

Організації змушені впроваджувати системні підходи до управління ризиками інформаційної безпеки, які спрямовані на захист інформаційних активів і підтримання стійкості критичних бізнес-процесів у контексті забезпечення безперервності діяльності. Науково-практичний аналіз існуючих моделей управління ризиками свідчить про те, що жодна з них не є універсальною

для всіх типів організацій, однак кожна модель має власні переваги та обмеження, які визначають ефективність її застосування у конкретному бізнес-середовищі.

Міжнародні стандарти, такі як ISO/IEC 27005, ISO 31000, методики національного рівня, зокрема NIST SP 800-30/37, а також аналітичні та організаційні моделі, такі як FAIR, OCTAVE і EBIOS, формують основу сучасного управління ризиками інформаційної безпеки [21]. Їх порівняльний аналіз дозволяє визначити ступінь придатності для різних організаційних контекстів, оцінити відповідність вимогам безперервності бізнесу, а також інтеграцію з існуючими системами менеджменту.

Порівняння моделей ISO, OCTAVE, NIST, FAIR та EBIOS за такими параметрами, як: орієнтація, переваги, обмеження і призначення вказані в табл. 1.4.

Таблиця 1.4

Порівняння моделей управління ризиками (ISO, OCTAVE, NIST, FAIR, EBIOS)

Модель	Орієнтація	Переваги	Обмеження	Призначення
ISO/IEC 27005	Стандартизована	Системність, інтеграція з ISMS	Потребує адаптації	Управління ризиками на корпоративному рівні
OCTAVE	Організаційна	Орієнтація на критичність активів	Складна реалізація	Визначення пріоритетів захисту бізнес-процесів
NIST SP 800-30/37	Деталізована	Практичні рекомендації, регуляторна підтримка	Складна для приватного сектора	Формалізований процес управління ризиками
FAIR	Кількісна	Фінансова оцінка, пріоритизація ресурсів	Потребує статистичних даних	Кількісна оцінка ризиків та планування бюджету
EBIOS	Контекстна	Врахування бізнес-потреб	Громіздкість, складність впровадження	Комплексна оцінка ризиків з урахуванням контексту організації

ISO/IEC 27005 забезпечує чітку методологію управління ризиками як складової системи менеджменту інформаційної безпеки, включаючи послідовні етапи ідентифікації активів, загроз і вразливостей, оцінки ймовірності та наслідків інцидентів, визначення пріоритетності ризиків і планування заходів реагування. Основною перевагою цього стандарту є його міжнародне визнання, системність і можливість інтеграції з існуючими політиками ISMS, що дозволяє організаціям впроваджувати уніфіковану методику оцінки ризиків незалежно від галузевої специфіки [22]. Однією з особливостей ISO/IEC 27005 є гнучкість у виборі методів оцінки ризиків, що дає змогу поєднувати якісні та кількісні підходи відповідно до ресурсів та потреб організації. Проте стандарт вимагає адаптації до конкретного бізнес-контексту, а його реалізація може бути трудомісткою для малих підприємств з обмеженими ресурсами.

OCTAVE, розроблена CERT/SEI, відрізняється орієнтацією на організаційний контекст та стратегічну оцінку критично важливих активів. Методика включає три основні фази: стратегічне оцінювання організаційної структури та бізнес-процесів, технологічну оцінку вразливостей і розробку планів дій щодо мінімізації ризиків. Основною перевагою OCTAVE є можливість комплексного аналізу організаційних ризиків, який охоплює технічні аспекти, процедури, політики та людський фактор, що робить цю методику особливо придатною для великих організацій зі складною структурою бізнес-процесів [23]. Водночас OCTAVE є порівняно складною для впровадження, вимагає високої експертності та часу на збір і аналіз інформації, що може обмежувати її використання у малих та середніх підприємствах.

Модель NIST SP 800-30/37, розроблена Національним інститутом стандартів і технологій США, пропонує деталізовану методологію управління ризиками, яка охоплює ідентифікацію активів та загроз, аналіз вразливостей, оцінку ймовірності та наслідків інцидентів, обробку ризиків і їх моніторинг. Перевагою цього підходу є високий рівень деталізації та практичні рекомендації щодо оцінки ризиків, що особливо цінно для регульованих секторів економіки та державних установ. Однак

модель відносно складна для реалізації у приватних комерційних організаціях, особливо малих підприємствах, і потребує певної адаптації під конкретні умови.

FAIR, у свою чергу, являє собою аналітичну модель кількісної оцінки ризиків, яка дозволяє визначати фінансовий вплив потенційних інцидентів. Основні компоненти FAIR включають визначення подій ризику, аналіз вразливостей, оцінку ймовірності настання інцидентів та визначення масштабів втрат. Перевагою FAIR є можливість отримання конкретних фінансових показників, що дозволяє організації оптимізувати витрати на інформаційну безпеку та пріоритизувати заходи захисту. Однак для ефективного застосування FAIR необхідно мати достатню статистичну інформацію та експертні оцінки, що може бути обмежуючим фактором для організацій з невеликою базою даних про інциденти.

EBIOS, розроблена у Франції, поєднує аналіз потреб безпеки з оцінкою ризиків та визначенням цілей захисту. Методика включає аналіз контексту організації, ідентифікацію ризиків, визначення цілей безпеки та планування заходів щодо їх реалізації. EBIOS дозволяє враховувати бізнес-потреби організації та специфіку функціонування, що підвищує ефективність управління ризиками у складних корпоративних середовищах. До недоліків методики належить її громіздкість та складність впровадження, особливо у малих організаціях із обмеженими ресурсами.

Порівняльний аналіз показує, що моделі управління ризиками можна класифікувати за двома ключовими ознаками: організаційно-стратегічні та кількісно-аналітичні. Організаційно-стратегічні моделі, такі як OCTAVE та EBIOS, орієнтовані на оцінку критичності бізнес-процесів, аналіз внутрішніх процедур і людського фактору та визначення пріоритетних сфер захисту. Кількісні та аналітичні моделі, зокрема FAIR, спрямовані на визначення ймовірності інцидентів та фінансових наслідків, що дозволяє інтегрувати оцінку ризиків з управлінською та фінансовою звітністю організації. ISO/IEC 27005 та NIST SP 800-30/37 поєднують ознаки обох підходів, пропонуючи системну методологію управління ризиками із можливістю комбінування якісних і кількісних оцінок [24].

У сенсі забезпечення безперервності бізнесу порівняльний аналіз моделей дозволяє зробити висновок про необхідність комбінованого підходу, який інтегрує організаційні, технологічні та фінансові аспекти ризиків. Такий підхід забезпечує можливість пріоритизації критичних активів, оптимізації ресурсів на реалізацію заходів захисту та забезпечення швидкого відновлення бізнес-процесів після інцидентів. Важливим аспектом є також адаптивність моделей до змін зовнішнього середовища, появи нових загроз та технологічних інновацій. Комбінування організаційно-стратегічних та кількісно-аналітичних підходів дозволяє підвищити точність оцінки ризиків, забезпечити баланс між витратами на безпеку та ефективністю бізнес-процесів, а також сформувати прозору систему прийняття рішень на рівні керівництва.

Практичне застосування комбінованого підходу передбачає використання організаційних моделей для визначення пріоритетних активів і процесів, кількісних моделей для оцінки фінансового впливу ризиків, а стандартизованих методик ISO/NIST – для побудови формалізованого циклу управління ризиками, моніторингу та контролю ефективності заходів безпеки.

Порівняльний аналіз моделей дозволяє виділити також ключові критерії ефективності управління ризиками: відповідність бізнес-цілям, здатність до інтеграції з іншими системами менеджменту, можливість адаптації до динамічного середовища, прозорість оцінки ризиків, а також наявність методів пріоритизації та контролю реалізації заходів.

Систематичний аналіз існуючих моделей показує, що організаційні моделі забезпечують глибоке розуміння внутрішніх бізнес-процесів і взаємозв’язку активів, загроз і вразливостей, тоді як кількісні моделі дозволяють об’єктивізувати оцінку ризиків, що особливо важливо для стратегічного та фінансового планування [25].

Оптимальним рішенням для сучасних організацій є інтеграція цих підходів у єдину систему управління ризиками, що дозволяє знизити негативний вплив інцидентів на безперервність бізнесу, підвищити рівень стійкості та забезпечити ефективне використання ресурсів на реалізацію заходів безпеки. Слід також

зазначити, що ефективне впровадження будь-якої моделі вимагає врахування специфіки організації, рівня зрілості її процесів, доступних ресурсів та стратегічних цілей, а також постійного моніторингу змін у зовнішньому та внутрішньому середовищі.

Отже, порівняльний аналіз дозволяє систематизувати переваги та недоліки існуючих моделей управління ризиками, визначити їх придатність для різних типів організацій, а також сформувати основу для розробки інтегрованої моделі, яка буде одночасно орієнтована на стратегічні, організаційні та фінансові аспекти управління ризиками інформаційної безпеки.

Висновки до розділу 1

Підсумовуючи аналіз проблемної сфери управління ризиками інформаційної безпеки в контексті безперервності бізнесу, слід зазначити, що сучасні організації оперують у складному середовищі, де поєднуються технологічні, організаційні та фінансові ризики.

Показано, що ризики інформаційної безпеки є багатофакторними та взаємопов'язаними, а їх класифікація за різними ознаками дозволяє більш чітко визначити критичні активи та потенційні загрози. Аналіз показав, що для ефективного управління ризиками необхідно комплексно оцінювати ймовірність виникнення загроз, вразливості системи та потенційні наслідки інцидентів, що є основою для планування заходів захисту та забезпечення безперервності бізнес-процесів.

Продемонстровано різноманіття моделей управління ризиками інформаційної безпеки та їх специфічні особливості. Стандартизовані підходи ISO/IEC 27005 та NIST SP 800-30/37 забезпечують системність та формалізований процес управління ризиками, організаційні методики OCTAVE і EBIOS акцентують увагу на аналізі бізнес-процесів та людського фактору, а кількісні моделі FAIR дозволяють визначати фінансовий вплив ризиків і пріоритизувати ресурси. Аналіз показав, що кожна модель має свої переваги та обмеження, і жодна з них не є універсальною, що підкреслює необхідність адаптації під конкретні умови організації.

Підкреслено, що оптимальним підходом є комбіноване застосування організаційно-стратегічних та кількісно-аналітичних моделей, що дозволяє отримати комплексну оцінку ризиків, поєднати якісну та кількісну оцінку, визначити пріоритети захисту критичних активів та забезпечити ефективне планування ресурсів. Порівняльний аналіз моделей показав, що інтеграція цих підходів дозволяє підвищити точність оцінки ризиків, забезпечити прозорість прийняття рішень та сформувати систему управління ризиками, яка максимально відповідає потребам бізнесу та вимогам забезпечення безперервності діяльності. У результаті застосування комбінованого підходу організація отримує можливість системно контролювати ризики, оперативно реагувати на інциденти та забезпечувати стійкість бізнес-процесів у довгостроковій перспективі.

РОЗДІЛ 2 РОЗРОБКА МОДЕЛІ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОСТІ БІЗНЕСУ

2.1 Концепція та принципи побудови моделі

Сучасні організації функціонують у середовищі, що характеризується високим рівнем цифровізації бізнес-процесів, зростанням залежності від інформаційних систем та постійною еволюцією кіберзагроз. Інформаційні ресурси, інформаційно-комунікаційні системи та дані стають критично важливими активами, порушення доступності, цілісності або конфіденційності яких безпосередньо впливає на стабільність функціонування організації. У таких умовах управління ризиками інформаційної безпеки перестає бути виключно технічною задачею та набуває стратегічного значення, оскільки кіберінциденти дедалі частіше призводять до зупинки або деградації ключових бізнес-процесів, фінансових втрат, репутаційних збитків і порушення договірних зобов'язань. Саме тому управління ризиками інформаційної безпеки тісно пов'язується із забезпеченням безперервності бізнесу та стійкості організації до деструктивних впливів.

Управління ризиками інформаційної безпеки та управління безперервністю бізнесу мають спільну цільову спрямованість, яка полягає у зниженні негативного впливу інцидентів на діяльність організації. Ризики інформаційної безпеки реалізуються через загрози, що впливають на інформаційні активи, однак їхні наслідки проявляються на рівні бізнес-процесів, операційної діяльності та управлінських рішень [26]. Порушення роботи інформаційних систем може призвести до неможливості виконання критичних функцій, затримок у наданні послуг, втрати даних або зупинки виробничих процесів. У цьому контексті управління ризиками інформаційної безпеки виступає не ізольованим процесом, а важливою складовою забезпечення

безперервності бізнесу, оскільки саме кіберризики дедалі частіше є першопричиною порушення нормального режиму функціонування організації.

Ізольований підхід до управління ризиками інформаційної безпеки, який зосереджується переважно на технічних засобах захисту та окремих інцидентах, не забезпечує достатнього рівня стійкості організації [27]. За такого підходу ризики оцінюються без урахування критичності бізнес-процесів, часових параметрів відновлення та допустимого рівня втрат. Аналогічно, процеси забезпечення безперервності бізнесу, що не інтегровані з управлінням кіберризиками, часто не враховують специфіку сучасних загроз інформаційній безпеці, що знижує ефективність планів реагування та відновлення. Це зумовлює необхідність формування інтегрованої моделі управління ризиками інформаційної безпеки, яка враховує бізнес-контекст, пріоритети організації та вимоги до безперервності діяльності.

Концепція запропонованої моделі ґрунтується на інтеграції процесів управління ризиками інформаційної безпеки з процесами забезпечення безперервності бізнесу в межах єдиної системи управління. Модель орієнтована на поєднання технічних, організаційних та управлінських аспектів інформаційної безпеки з урахуванням впливу ризиків на критичні бізнес-процеси [28]. Її ключовою ідеєю є перехід від фрагментарного реагування на інциденти до системного управління ризиками, спрямованого на підтримку стійкості організації, мінімізацію часу простою та забезпечення керованого відновлення діяльності.

Метою запропонованої моделі є підвищення рівня стійкості організації шляхом системного управління ризиками інформаційної безпеки з урахуванням вимог безперервності бізнесу. Для досягнення цієї мети модель передбачає ідентифікацію ризиків інформаційної безпеки, оцінювання їхнього впливу на бізнес-процеси, підтримку прийняття управлінських рішень щодо обробки ризиків та забезпечення адаптації до змін у ландшафті загроз. Реалізація таких завдань дозволяє забезпечити узгодженість між цілями інформаційної безпеки та стратегічними цілями організації [29].

Основою побудови моделі є принцип системності, відповідно до якого управління ризиками розглядається як складова цілісної системи управління інформаційною безпекою організації. У межах цього принципу враховується взаємозв'язок між інформаційними активами, загрозами, вразливостями та бізнес-процесами, а також забезпечується узгодженість між організаційними структурами, політиками та процедурами. Системний підхід дозволяє уникнути фрагментарності в управлінні ризиками та забезпечує цілісне бачення впливу кіберзагроз на діяльність організації.

Важливим принципом моделі є безперервність управління ризиками, яка зумовлена динамічним характером загроз інформаційної безпеки та постійними змінами у внутрішньому й зовнішньому середовищі організації. Ризики не можуть розглядатися як статичні величини, оскільки їхній рівень змінюється залежно від технологічних, організаційних і регуляторних факторів. Безперервний характер управління ризиками передбачає регулярний перегляд оцінок, моніторинг змін та актуалізацію заходів захисту, що особливо важливо для підтримки безперервності бізнесу [30].

Принцип ризик-орієнтованого підходу забезпечує концентрацію ресурсів на найбільш значущих ризиках, які становлять загрозу для критичних бізнес-процесів. У межах цього підходу пріоритет надається не всім ризикам однаковою мірою, а тим, що можуть призвести до суттєвих операційних або фінансових втрат. Це дозволяє оптимізувати використання ресурсів, підвищити ефективність заходів безпеки та забезпечити досягнення прийнятного рівня ризику для організації.

Адаптивність і гнучкість моделі є необхідною умовою її ефективного функціонування в умовах постійної зміни загроз і технологій. Запропонована модель передбачає можливість коригування параметрів оцінювання ризиків, перегляду пріоритетів та адаптації заходів реагування відповідно до змін у бізнес-середовищі [31]. Такий підхід сприяє підвищенню здатності організації швидко реагувати на нові виклики та підтримувати стабільність діяльності.

Окрему роль у побудові моделі відіграє принцип відповідності міжнародним стандартам у сфері інформаційної безпеки та безперервності бізнесу. Стандарти розглядаються як методологічна основа, що забезпечує узгодженість підходів, відтворюваність процесів і підвищення рівня довіри до результатів управління ризиками. При цьому модель не є жорстко прив'язаною до конкретного стандарту, що дозволяє адаптувати її до особливостей організації [32].

Місце запропонованої моделі в загальній системі управління інформаційною безпекою організації визначається її інтеграційною функцією. Модель виступає сполучною ланкою між системою управління інформаційною безпекою та процесами забезпечення безперервності бізнесу, забезпечуючи узгодженість між оцінкою ризиків, плануванням заходів захисту та прийняттям управлінських рішень [33]. Узагальнене позиціонування моделі в системі управління подано у вигляді схеми (рисунок 2.1).

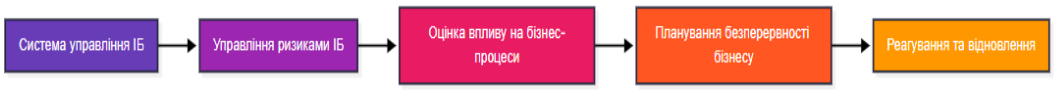

Рис. 2.1 Концептуальна схема інтеграції управління ризиками інформаційної безпеки з процесами безперервності бізнесу

Для наочного відображення принципів побудови моделі доцільно використати узагальнювальну таблицю.

Таблиця 2.1

Принципи побудови моделі управління ризиками інформаційної безпеки

Принцип	Характеристика	Роль у забезпеченні безперервності
Системність	Врахування взаємозв'язків між активами, загрозами та процесами	Забезпечує цілісне управління
Безперервність	Постійний перегляд і моніторинг ризиків	Підтримує актуальність рішень
Ризик-орієнтованість	Пріоритезація критичних ризиків	Оптимізує використання ресурсів
Адаптивність	Гнучке коригування моделі	Підвищує стійкість до змін
Відповідність стандартам	Орієнтація на міжнародні підходи	Забезпечує узгодженість практик

Отже, концепція та принципи побудови запропонованої моделі формують методологічну основу для подальшого опису її архітектури, компонентів і методів оцінювання ризиків, що розглядаються в наступних підрозділах роботи.

2.2 Архітектура та ключові компоненти запропонованої моделі

Архітектура запропонованої моделі управління ризиками інформаційної безпеки визначає логіку її функціонування, взаємодію структурних компонентів та послідовність реалізації процесів, спрямованих на зниження впливу кіберризиків на безперервність бізнесу. Саме архітектура забезпечує практичну реалізацію концептуальних положень, викладених у попередньому підрозділі, перетворюючи загальні принципи на формалізовану систему управління. Чітко визначена архітектура дозволяє забезпечити керованість процесів, прозорість прийняття рішень, а також масштабованість моделі відповідно до розміру та специфіки діяльності організації.

Запропонована модель побудована за модульним принципом і має багаторівневу структуру, що дає змогу інтегрувати управління ризиками інформаційної безпеки з процесами забезпечення безперервності бізнесу в межах єдиного управлінського циклу [34]. Модульний підхід обрано з огляду на

необхідність гнучкої адаптації моделі до змін у зовнішньому та внутрішньому середовищі, а також можливість її поетапного впровадження. Архітектура моделі формує замкнений цикл управління ризиками, у якому результати кожного етапу використовуються як вхідні дані для наступних компонентів, а механізми зворотного зв'язку забезпечують актуалізацію оцінок і управлінських рішень.

У структурі архітектури доцільно виокремити кілька логічних рівнів, кожен з яких виконує власну функціональну роль. Операційний рівень забезпечує збір і структурування первинних даних про інформаційні активи, події та інциденти. Аналітичний рівень відповідає за аналіз загроз, вразливостей і оцінювання ризиків з урахуванням імовірності їх реалізації та впливу на бізнес-процеси [35]. Управлінський рівень реалізує процеси прийняття рішень щодо обробки ризиків і контролю ефективності заходів. Стратегічний рівень пов'язаний із забезпеченням безперервності бізнесу та використанням результатів управління ризиками для планування реагування і відновлення діяльності організації. Узагальнення функцій рівнів архітектури подано в таблиці 2.2.

Таблиця 2.2

Рівні архітектури моделі управління ризиками інформаційної безпеки

Рівень архітектури	Основні функції	Результат функціонування
Операційний	Збір та облік даних про активи і події	Структуровані первинні дані
Аналітичний	Аналіз загроз, вразливостей і ризиків	Оцінені рівні ризиків
Управлінський	Формування та реалізація рішень	Заходи обробки ризиків
Стратегічний	Підтримка безперервності бізнесу	Плани реагування і відновлення

Ключовим компонентом архітектури є модуль ідентифікації інформаційних активів, який формує базу для подальшого аналізу ризиків. У межах цього модуля здійснюється виявлення та класифікація активів, до яких

належать інформаційні ресурси, інформаційні системи, сервіси, технічні засоби та персонал. Особлива увага приділяється встановленню зв'язку між активами та бізнес-процесами, що дозволяє визначити критичність кожного активу з точки зору безперервності діяльності. Результатом функціонування модуля є формування актуального реєстру активів із зазначенням їхньої ролі в забезпеченні бізнес-функцій [36].

Наступним елементом архітектури є модуль ідентифікації загроз і вразливостей, який використовує дані про активи для формування можливих сценаріїв реалізації ризиків. У межах цього модуля враховуються як зовнішні, так і внутрішні джерела загроз, а також технічні, організаційні та людські вразливості, що створюють умови для їх реалізації. Аналіз загроз і вразливостей здійснюється з урахуванням специфіки активів і контексту їх використання в бізнес-процесах, що дозволяє перейти від абстрактних загроз до конкретних ризикових сценаріїв.

Центральним елементом моделі є модуль оцінювання ризиків, який забезпечує аналітичну обробку інформації, отриманої з попередніх модулів. У межах цього компонента здійснюється оцінка ймовірності реалізації загроз і визначення потенційного впливу на бізнес-процеси, зокрема на доступність, час відновлення та рівень допустимих втрат [37]. Оцінювання ризиків проводиться у формі якісної або напівкількісної оцінки, що дозволяє порівнювати ризики між собою та визначати пріоритети їх обробки. Для узагальнення результатів оцінювання може використовуватися таблиця відповідності активів, загроз і рівнів ризику, приклад якої наведено в таблиці 2.3.

Таблиця 2.3

Приклад структури результатів оцінювання ризиків

Актив	**Загроза**	**Ймовірність**	**Вплив на бізнес**	**Рівень ризику**
Інформаційна система	Кіберінцидент	Середня	Високий	Високий
Дані клієнтів	Несанкціонований доступ	Низька	Критичний	Середній

Результати оцінювання ризиків передаються до модуля прийняття рішень щодо обробки ризиків, який виконує управлінську функцію в межах архітектури моделі. У цьому модулі здійснюється вибір варіантів реагування на ризики з урахуванням бізнес-пріоритетів, ресурсних обмежень і допустимого рівня ризику [38]. Управлінські рішення формуються на основі встановлених політик і регламентів та спрямовані на зниження негативного впливу ризиків на діяльність організації. Формалізація таких рішень забезпечує їхню узгодженість і контрольованість.

Модуль моніторингу та перегляду ризиків забезпечує безперервний характер функціонування моделі та реалізацію механізмів зворотного зв'язку. У межах цього модуля здійснюється аналіз змін у середовищі, виявлення нових загроз, контроль ефективності впроваджених заходів і своєчасна актуалізація оцінок ризиків. Завдяки цьому модель зберігає актуальність і здатність адаптуватися до динамічного ландшафту кіберзагроз.

Окремим компонентом архітектури є модуль підтримки безперервності бізнесу, який інтегрує результати управління ризиками інформаційної безпеки з процесами планування реагування та відновлення діяльності. Дані про ризики високого рівня використовуються для визначення пріоритетних бізнес-процесів, планування сценаріїв реагування та встановлення пріоритетів відновлення. Таким чином забезпечується узгодженість між управлінням ризиками інформаційної безпеки та стратегією забезпечення безперервності бізнесу [39].

Функціонування архітектури моделі ґрунтується на чітко визначених інформаційних потоках між її компонентами. Дані про активи передаються до аналітичних модулів, результати оцінювання ризиків надходять до управлінських і стратегічних компонентів, а результати моніторингу повертаються на початкові етапи для коригування оцінок і рішень. Така послідовність забезпечує цілісність і узгодженість управління ризиками в межах всієї моделі.

Важливу роль у реалізації архітектури відіграє персонал організації, зокрема власники активів, фахівці з інформаційної безпеки та керівництво, які

беруть участь у формуванні даних, аналізі ризиків і прийнятті управлінських рішень. ІТ-системи виконують допоміжну функцію, забезпечуючи автоматизацію збору та обробки інформації, тоді як регламенти та політики визначають правила взаємодії між компонентами моделі та відповідальність учасників процесу [40].

Узагальнююча архітектура запропонованої моделі представлена на рисунку 2.2 і відображає повну логіку її функціонування. Архітектура моделі має вигляд послідовно з'єднаних модулів, об'єднаних у замкнений цикл управління ризиками. На вході моделі формується інформаційний потік, що включає дані про інформаційні активи, бізнес-процеси та організаційне середовище. Цей потік надходить до модуля ідентифікації активів, результати якого передаються до модуля ідентифікації загроз і вразливостей, де формуються сценарії ризиків. Далі інформація надходить до модуля оцінювання ризиків, який визначає їхні рівні з урахуванням впливу на безперервність бізнесу. Результати оцінювання передаються до модуля прийняття управлінських рішень і паралельно до модуля підтримки безперервності бізнесу для планування реагування та відновлення. Модуль моніторингу та перегляду ризиків охоплює всі компоненти архітектури, забезпечуючи зворотний зв'язок і актуалізацію моделі в разі змін у середовищі або появи нових загроз. Така архітектура забезпечує інтегроване, послідовне та кероване управління ризиками інформаційної безпеки в контексті забезпечення безперервності бізнесу

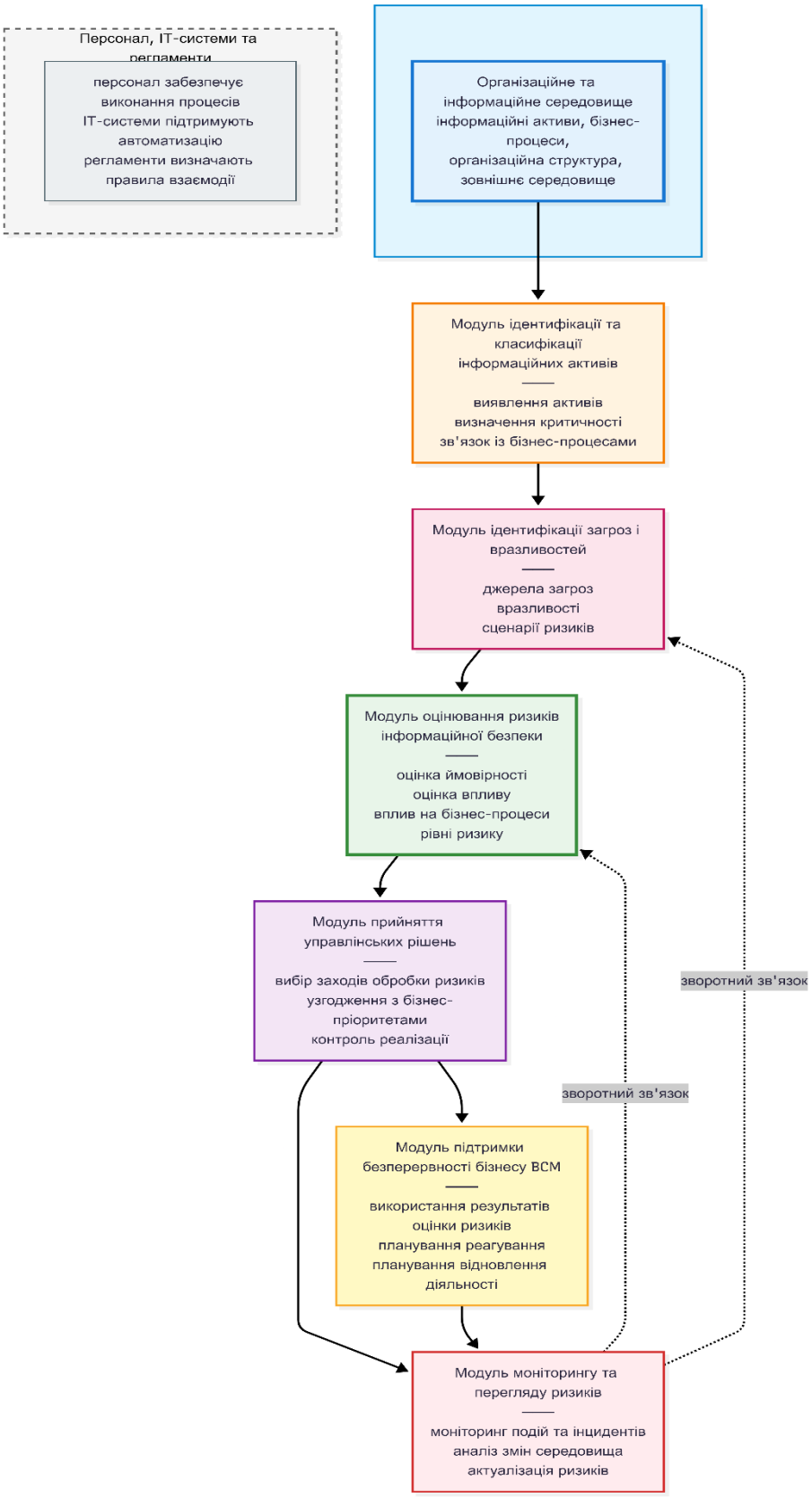

Рис. 2.2 Архітектура моделі управління ризиками інформаційної безпеки в контексті забезпечення безперервності бізнесу

2.3 Методи оцінювання ризиків у рамках моделі

Оцінювання ризиків інформаційної безпеки є центральним аналітичним етапом запропонованої моделі управління ризиками, оскільки саме на цьому етапі формується інформаційна основа для прийняття обґрунтованих управлінських рішень. У контексті забезпечення безперервності бізнесу оцінювання ризиків виконує функцію виявлення потенційних загроз інформаційним активам і визначення їхнього впливу на здатність організації підтримувати виконання критичних бізнес-процесів у допустимих часових і ресурсних межах. Тому методи оцінювання ризиків у рамках запропонованої моделі орієнтовані на поєднання підходів інформаційної безпеки та управління безперервністю бізнесу з урахуванням практичної придатності та керованості процесу.

Методологічною основою оцінювання ризиків у моделі є комбінований підхід, який поєднує елементи класичного управління ризиками інформаційної безпеки з вимогами до стійкості бізнес-процесів. Такий підхід передбачає відмову від надмірно складних кількісних методів на користь якісних і напівкількісних методів, які забезпечують достатню точність для управлінських рішень і водночас не потребують значних обчислювальних ресурсів. Це особливо важливо для організацій, у яких процеси управління ризиками мають бути інтегровані в повсякденну діяльність і регулярно переглядатися [41].

Загальний підхід до ідентифікації ризиків у рамках моделі ґрунтується на розгляді ризику як результату взаємодії інформаційного активу, загрози та вразливості. На цьому етапі формується перелік ризикових сценаріїв, які відображають можливі шляхи реалізації загроз та їхні потенційні наслідки. Важливою особливістю запропонованого підходу є перехід від суто технічного трактування ризиків до їхнього розгляду в бізнес-контексті. Це означає, що кожен ризик аналізується з точки зору порушення властивостей інформаційної безпеки з урахуванням його впливу на виконання конкретних бізнес-функцій.

Ідентифікація ризиків у контексті бізнес-процесів є ключовою умовою інтеграції управління ризиками інформаційної безпеки з процесами забезпечення безперервності бізнесу. У межах цього підходу кожен ідентифікований ризик прив'язується до одного або кількох бізнес-процесів, що дозволяє визначити їхню критичність і взаємозалежність [42]. Особливу увагу приділяється критичним бізнес-процесам, порушення яких може призвести до суттєвих операційних або репутаційних втрат. Крім того, враховується кумулятивний ефект ризиків, коли реалізація одного інциденту може спричинити ланцюгові наслідки для кількох процесів одночасно. У цьому контексті важливу роль відіграють власники бізнес-процесів, які залучаються до оцінювання наслідків ризиків і формування пріоритетів.

Якісне оцінювання ризиків є базовим методом, що застосовується на початкових етапах аналізу або на стратегічному рівні управління. Воно передбачає використання описових категорій для оцінювання ймовірності реалізації ризику та рівня його впливу. Такий підхід дозволяє швидко отримати загальне уявлення про рівень загроз і зосередити увагу на найбільш проблемних ділянках. Якісне оцінювання ґрунтується на експертних оцінках, аналізі історичних інцидентів і знанні специфіки діяльності організації. Приклад якісної шкали оцінювання наведено в таблиці 2.4.

Таблиця 2.4

Приклад якісної шкали оцінювання ризиків

Параметр	Категорія	Характеристика
Ймовірність	Низька	Реалізація малоймовірна
	Середня	Можлива за певних умов
	Висока	Ймовірна у короткостроковій перспективі
Вплив	Низький	Незначний вплив на діяльність
	Суттєвий	Порушення окремих процесів
	Критичний	Зупинка критичних процесів

Разом із тим якісне оцінювання має низку обмежень, пов’язаних із суб’єктивністю експертних суджень і складністю порівняння ризиків між собою. Це зумовлює необхідність деталізації оцінок шляхом використання напівкількісних, або бальних, методів оцінювання ризиків. Такі методи поєднують експертний підхід із формалізованими шкалами, що дозволяє підвищити об’єктивність і відтворюваність результатів [43].

Напівкількісне оцінювання ризиків передбачає використання числових шкал для оцінювання ймовірності та впливу, наприклад у діапазоні від 1 до 5. Кожне значення шкали має чітке описове тлумачення, що знижує варіативність оцінок і спрощує їх порівняння. Такий підхід дозволяє ранжувати ризики за рівнем значущості та визначати пріоритети для їх подальшої обробки. Приклад бальної шкали наведено в таблиці 2.5.

Таблиця 2.5

Приклад бальної шкали оцінювання ризиків

Бал	Ймовірність	Вплив
1	Дуже низька	Мінімальний
2	Низька	Незначний
3	Середня	Помірний
4	Висока	Суттєвий
5	Дуже висока	Критичний

Комбінування показників ймовірності та впливу дозволяє визначити інтегральний рівень ризику, який використовується для подальшої класифікації та прийняття рішень. У запропонованій моделі поєднання цих параметрів здійснюється без застосування складних формул, шляхом використання матриці ризиків. Такий інструмент є наочним і зручним для використання на практиці, оскільки дозволяє швидко ідентифікувати ризики з неприйнятним рівнем. Приклад матриці ризиків подано в таблиці 2.6.

Таблиця 2.6

Приклад матриці ризиків

Ймовірність \ Вплив	1	2	3	4	5
1	Низький	Низький	Низький	Середній	Середній

2	Низький	Низький	Середній	Середній	Високий
3	Низький	Середній	Середній	Високий	Високий
4	Середній	Середній	Високий	Високий	Критичний
5	Середній	Високий	Високий	Критичний	Критичний

На основі матриці ризиків здійснюється класифікація ризиків за рівнями, такими як низький, середній, високий і критичний. Критерії віднесення ризиків до певного рівня визначаються з урахуванням прийнятного рівня ризику для організації та її стратегічних цілей. Важливо, що порогові значення ризиків встановлюються за участю керівництва, що забезпечує узгодженість технічних оцінок із бізнес-пріоритетами. Відповідність рівнів ризику управлінським діям наведено в таблиці 2.7.

Таблиця 2.7

Відповідність рівнів ризику та управлінських дій

Рівень ризику	Характеристика	Тип реагування
Низький	Прийнятний	Моніторинг
Середній	Контрольований	Зниження
Високий	Неприйнятний	Негайні заходи
Критичний	Загрозливий	Пріоритетне реагування

Особливістю запропонованої моделі є обов’язкове урахування впливу ризиків інформаційної безпеки на критичні бізнес-процеси. Оцінювання ризиків доповнюється аналізом наслідків для ключових функцій організації, що дозволяє визначити, які процеси потребують першочергового захисту. Такий підхід забезпечує узгодженість між управлінням ризиками та забезпеченням безперервності бізнесу.

Важливим параметром оцінювання є час відновлення діяльності, який визначає допустиму тривалість простою бізнес-процесів у разі реалізації ризику. Ризики, реалізація яких може призвести до перевищення допустимого часу відновлення, автоматично відносяться до вищих рівнів пріоритету незалежно від їхньої ймовірності. Це дозволяє зосередити ресурси на захисті процесів, критичних з точки зору часових обмежень [44].

Окрім часових параметрів, у процесі оцінювання враховуються допустимі втрати, які можуть бути як фінансовими, так і нефінансовими, зокрема репутаційними або правовими. Визначення меж допустимих втрат дозволяє встановити критерії прийнятності ризиків і уникнути ситуацій, коли технічно незначний інцидент має непропорційно великий вплив на діяльність організації.

Результати оцінювання ризиків використовуються як основа для вибору заходів реагування в межах запропонованої моделі. Рівень ризику визначає пріоритетність реагування, характер заходів і необхідність залучення ресурсів. Таким чином забезпечується прямий зв'язок між аналітичними результатами оцінювання та управлінськими рішеннями, що підвищує ефективність системи управління ризиками.

З метою забезпечення простежуваності та актуальності оцінювання всі результати фіксуються в установленому форматі та підлягають регулярному перегляду. Оцінювання ризиків не розглядається як одноразова процедура, а є безперервним процесом, що актуалізується у разі змін у середовищі, появи нових загроз або змін у бізнес-процесах.

2.4 Механізми забезпечення інтеграції з процесами безперервності бізнесу

Одним із ключових механізмів інтеграції є взаємодія управління ризиками інформаційної безпеки з процесами планування безперервності бізнесу. Результати оцінювання ризиків, отримані в межах моделі, використовуються як вхідні дані для формування та актуалізації планів безперервності бізнесу. Зокрема, ідентифіковані ризики високого та критичного рівнів дозволяють визначити найбільш вразливі ділянки діяльності організації та сформувати сценарії порушення бізнес-процесів, що враховують кіберінциденти як першопричину. Отже, планування безперервності бізнесу базується на конкретних ризикових сценаріях, характерних для інформаційного середовища організації, а не на загальних припущеннях щодо можливих кризових ситуацій.

Важливим елементом інтеграції є узгодження управління ризиками інформаційної безпеки з планами реагування на інциденти. У межах запропонованої моделі рівень ризику використовується як критерій пріоритезації інцидентів і визначення порядку реагування. Інциденти, пов'язані з ризиками високого або критичного рівня, потребують негайного залучення відповідних підрозділів і керівництва, оскільки їх реалізація може безпосередньо вплинути на виконання критичних бізнес-функцій [45]. Такий підхід дозволяє узгодити технічні дії з реагування на інциденти з управлінськими рішеннями та забезпечити своєчасне інформування зацікавлених сторін.

Інтеграція управління ризиками інформаційної безпеки з планами аварійного відновлення спрямована на забезпечення швидкого та контрольованого відновлення інформаційних систем і сервісів після інцидентів. Результати оцінювання ризиків використовуються для визначення пріоритетів відновлення IT-ресурсів з урахуванням їхньої ролі у підтримці бізнес-процесів. Такий підхід дозволяє уникнути ситуацій, коли технічне відновлення здійснюється без урахування реальних потреб бізнесу, та забезпечує узгодженість дій між підрозділами інформаційної безпеки, інформаційних технологій і бізнес-підрозділами.

У межах запропонованої моделі критичність процесів визначається їхньою функціональною значущістю з урахуванням рівня ризиків інформаційної безпеки, що на них впливають. Це дозволяє сформувати обґрунтований перелік процесів, які потребують першочергового захисту та підтримки. Приклад використання оцінки ризиків для визначення критичності бізнес-процесів наведено в таблиці 2.8.

Таблиця 2.8

Використання оцінки ризиків для визначення критичних бізнес-процесів

Бізнес-процес	**Пов'язані ризики інформаційної безпеки**	**Рівень ризику**	**Критичність процесу**

Обробка даних клієнтів	Несанкціонований доступ, витік даних	Критичний	Критичний
Фінансові операції	Порушення доступності систем	Високий	Високий
Допоміжні процеси	Локальні інциденти	Середній	Середній

Оцінка ризиків також використовується для встановлення пріоритетів відновлення діяльності в разі реалізації інцидентів. Пріоритетність відновлення визначається на основі поєднання рівня ризику, допустимого часу простою та потенційних втрат для організації. Такий підхід дозволяє оптимізувати використання ресурсів у кризових ситуаціях і забезпечити відновлення найбільш критичних процесів у першу чергу. Взаємозв'язок між рівнем ризику та пріоритетами відновлення наведено в таблиці 2.9.

Таблиця 2.9

Вплив рівня ризику на пріоритети відновлення діяльності

Рівень ризику	**Допустимий час простою**	**Пріоритет відновлення**
Низький	Тривалий	Низький
Середній	Обмежений	Середній
Високий	Короткий	Високий
Критичний	Мінімальний	Найвищий

Окрім визначення пріоритетів, результати оцінювання ризиків використовуються для вибору заходів захисту та організаційних рішень. Ризик-орієнтований підхід дозволяє зосередити зусилля на впровадженні заходів, які забезпечують максимальний ефект для зниження ризиків, що загрожують безперервності бізнесу. При цьому враховується баланс між вартістю заходів і рівнем зниження ризику, що сприяє прийняттю економічно обґрунтованих рішень [46].

Важливим механізмом підтримки інтеграції управління ризиками інформаційної безпеки з процесами безперервності бізнесу є регулярний моніторинг та тестування планів безперервності. Моніторинг змін у середовищі, результатів оцінювання ризиків і реалізованих інцидентів дозволяє своєчасно виявляти невідповідності між фактичним станом ризиків і запланованими заходами. Проведення навчань і тестувань планів безперервності бізнесу та

аварійного відновлення сприяє перевірці їхньої актуальності, виявленню слабких місць і підвищенню готовності персоналу до дій у кризових ситуаціях.

Узагальнююча схема інтеграції управління ризиками інформаційної безпеки з процесами безперервності бізнесу подана на рисунку 2.3. Схема відображає замкнений цикл, у межах якого результати ідентифікації та оцінювання ризиків інформаційної безпеки використовуються для планування безперервності бізнесу, формування планів реагування на інциденти та планів аварійного відновлення. У свою чергу, результати тестування та реалізації планів безперервності повертаються до системи управління ризиками у вигляді зворотного зв'язку, що забезпечує актуалізацію оцінок ризиків і коригування управлінських рішень. Така схема наочно демонструє, що управління ризиками інформаційної безпеки та забезпечення безперервності бізнесу функціонують як взаємопов'язані елементи єдиної системи управління стійкістю організації [47].

Інтегрований підхід, реалізований у запропонованій моделі, забезпечує низку практичних переваг для організації, зокрема підвищення узгодженості управлінських рішень, зменшення часу простою бізнес-процесів у разі інцидентів та підвищення здатності організації адаптуватися до змін у ландшафті загроз. Завдяки використанню результатів оцінювання ризиків у процесах безперервності бізнесу забезпечується цілісне бачення загроз і їхніх наслідків, що сприяє підвищенню загального рівня стійкості організації.

Висновки до розділу 2

Висновки до розділу 2

У другому розділі роботи розроблено модель управління ризиками інформаційної безпеки, орієнтовану на забезпечення безперервності бізнесу в умовах зростання кіберзагроз та цифровізації діяльності організацій.

Концептуальну основу моделі складають принципи системності, безперервності, ризик-орієнтованості, адаптивності та відповідності міжнародним стандартам. Ці принципи формують методологічну базу для

інтеграції управління ризиками інформаційної безпеки з процесами забезпечення безперервності бізнесу в межах єдиної управлінської системи.

Архітектура моделі побудована за модульним принципом і включає шість взаємопов'язаних компонентів: модулі ідентифікації активів, ідентифікації загроз і вразливостей, оцінювання ризиків, прийняття управлінських рішень, моніторингу та підтримки безперервності бізнесу. Чотирирівнева структура архітектури охоплює операційний, аналітичний, управлінський та стратегічний рівні, що забезпечує цілісність управління ризиками від збору первинних даних до стратегічного планування.

Для оцінювання ризиків запропоновано комбінований підхід, що поєднує якісні та напівкількісні методи з використанням матриці ризиків. Особливістю методів є обов'язкове врахування впливу ризиків на критичні бізнес-процеси, допустимий час простою та рівень втрат, що забезпечує релевантність оцінок для прийняття управлінських рішень.

Механізми інтеграції з процесами безперервності бізнесу реалізовані через використання результатів оцінювання ризиків для планування безперервності, визначення пріоритетів реагування та відновлення діяльності. Замкнений цикл управління із зворотним зв'язком забезпечує актуалізацію моделі відповідно до змін у середовищі та ландшафті загроз.

Запропонована модель формує практичний інструментарій для підвищення стійкості організацій до кіберінцидентів та забезпечує узгодженість між технічними заходами захисту й стратегічними цілями бізнесу.

РОЗДІЛ 3 ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ ТА ОЦІНКА ЕФЕКТИВНОСТІ ЗАПРОПОНОВАНОЇ МОДЕЛІ

3.1 Методика проведення експерименту

Експериментальне дослідження спрямоване на кількісну оцінку ефективності запропонованої моделі управління ризиками інформаційної безпеки в контексті забезпечення безперервності бізнесу та перевірку її практичної придатності в умовах реалістичного технічного середовища. Основною метою експерименту є визначення впливу інтеграції управління ризиками інформаційної безпеки з процесами безперервності бізнесу на зміну рівнів ризику та показників відновлення критичних бізнес-процесів. У межах дослідження висувається гіпотеза, що застосування інтегрованого підходу дозволяє знизити середній інтегральний рівень ризику та скоротити час відновлення критичних процесів порівняно з класичним підходом, у якому управління ризиками інформаційної безпеки розглядається ізольовано від процесів безперервності бізнесу.

Для проведення експерименту сформовано умовне технічне середовище сервісної онлайн-платформи середнього масштабу, яке моделює типову архітектуру сучасної цифрової організації, що надає послуги клієнтам через веб-інтерфейс. Середовище є штучно змодельованим і не відображає інфраструктуру конкретної реальної організації, проте побудоване з урахуванням поширених практик проєктування корпоративних інформаційних систем. Організація функціонує на базі одного централізованого дата-центру та підтримує цілодобовий доступ користувачів до онлайн-сервісів. У межах експерименту визначено п’ять основних інформаційних систем, які забезпечують реалізацію бізнес-функцій платформи, а саме систему вебдоступу користувачів, прикладну серверну систему обробки запитів, систему керування базами даних, систему зберігання файлів та резервного копіювання, а також систему моніторингу та централізованого журналювання подій.

Критичні бізнес-процеси організації визначено на основі їхньої ролі в забезпеченні основної діяльності сервісної платформи. До таких процесів віднесено процес надання онлайн-сервісу клієнтам, процес обробки операцій та запитів у прикладному рівні, а також процес зберігання та обробки персональних і конфіденційних даних користувачів. Для кожного з цих процесів встановлено вимоги до безперервності діяльності у вигляді цільових значень RTO та RPO, які використовуються в подальшому аналізі для оцінки впливу ризиків на здатність організації підтримувати функціонування у разі інцидентів. Зовнішній доступ користувачів до сервісу реалізується через мережевий периметр з використанням сегмента демілітаризованої зони, тоді як внутрішні серверні компоненти розміщені у внутрішньому сегменті мережі з обмеженим доступом. Така сегментація дозволяє відокремити публічні компоненти від критичних внутрішніх ресурсів та є типовою для корпоративних середовищ [48].

Інформаційні системи сервісної платформи оперують різними типами даних, серед яких виділяються персональні дані користувачів, операційні журнали, службові дані конфігурації, а також резервні копії інформації. Кожен тип даних має різний рівень критичності з точки зору конфіденційності, цілісності та доступності, що безпосередньо впливає на оцінку наслідків реалізації ризиків. Залежності між інформаційними системами та бізнес-процесами описуються як послідовні ланцюги взаємодії, у межах яких відмова або компрометація одного компонента може призвести до порушення виконання відповідного бізнес-процесу. Саме ці залежності враховуються під час формування ризикових сценаріїв і подальшої кількісної оцінки.

На основі аналізу архітектури середовища та характеру діяльності організації сформовано набір технічних ризикових сценаріїв, які відображають найбільш імовірні та небезпечні кіберінциденти для сервісної онлайн-платформи. У межах експерименту розглядається дванадцять типових кіберризиків, серед яких відмова серверного обладнання, атака типу програм-вимагачів, порушення доступності мережевої інфраструктури, витік конфіденційних даних, несанкціонований доступ до прикладних сервісів,

помилки конфігурації систем зберігання даних, відмова систем резервного копіювання та компрометація облікових записів адміністраторів. Для кожного ризикового сценарію визначається інформаційний актив, на який спрямовано загрозу, тип загрози, відповідна вразливість та можливі наслідки для інформаційної системи і бізнес-процесів. Такий підхід дозволяє формалізувати сценарії інцидентів і використовувати їх як основу для кількісного аналізу ефективності управління ризиками [49].

Оцінювання ризиків у базовому стані здійснюється із застосуванням класичного підходу до управління ризиками інформаційної безпеки, у межах якого ризик визначається як поєднання ймовірності реалізації загрози та рівня її впливу. На цьому етапі вплив оцінюється переважно з технічної точки зору, зокрема через втрату доступності сервісів, порушення цілісності даних або їх компрометацію, без детального врахування вимог до безперервності бізнес-процесів. Кожному ризиковому сценарію присвоюється бальна оцінка ймовірності та впливу за п’ятибальною шкалою, після чого розраховується інтегральний ризиковий бал. За результатами базової оцінки фіксується середній рівень ризику для всієї сукупності сценаріїв, а також кількість ризиків, що відносяться до високого та критичного рівнів. Отримані значення використовуються як контрольна група для подальшого порівняння.

Наступним етапом експерименту є застосування запропонованої моделі управління ризиками інформаційної безпеки, яка інтегрує результати оцінювання ризиків із процесами безперервності бізнесу. Повторна оцінка проводиться для тих самих ризикових сценаріїв, однак на цьому етапі враховується критичність бізнес-процесів, на які впливає кожен інцидент, а також часові та ресурсні обмеження, визначені показниками RTO та RPO. Якщо прогнозований вплив ризику призводить до перевищення допустимого часу відновлення критичного процесу або до втрати даних понад встановлений поріг, рівень впливу коригується у бік підвищення. Таким чином, технічно однакові інциденти можуть отримувати різні інтегральні оцінки залежно від їхнього

бізнес-контексту, що є ключовою відмінністю запропонованого підходу від класичного.

Перерахунок ризикових показників у межах інтегрованої моделі дозволяє сформувати нові пріоритети реагування та відновлення. Ризики, які безпосередньо загрожують виконанню критичних бізнес-процесів у межах допустимого часу, відносяться до вищих пріоритетів незалежно від їхньої початкової технічної оцінки. Це забезпечує орієнтацію управлінських рішень на підтримку стійкості діяльності організації з фокусом на запобігання порушенням бізнес-процесів, а не на усунення окремих технічних наслідків інцидентів. У межах експерименту фіксуються зміни в розподілі ризиків за рівнями, а також зміни в переліку сценаріїв, що потребують першочергового реагування [50].

Для кількісної оцінки ефективності запропонованої моделі використовується низка простих інтерпретаційних метрик. Інтегральний рівень ризику для кожного сценарію визначається як добуток бальної оцінки ймовірності та впливу, що дозволяє зберегти порівнянність результатів між базовою та інтегрованою оцінками. Середній інтегральний ризик розраховується як середнє арифметичне значень для всієї сукупності сценаріїв і використовується як узагальнений показник ризикового профілю організації. Відносне зниження середнього рівня ризику визначається шляхом порівняння значень до та після впровадження моделі, що дозволяє кількісно оцінити ефект інтеграції управління ризиками інформаційної безпеки з процесами безперервності бізнесу.

Додатково в межах експерименту аналізуються показники, пов’язані з відновленням діяльності, зокрема прогнозований час виявлення інциденту та час відновлення критичних бізнес-процесів. Хоча значення цих показників є умовними, вони ґрунтуються на реалістичних припущеннях щодо організації процесів реагування та відновлення. Порівняння значень до та після застосування моделі дозволяє оцінити вплив ризик-орієнтованої пріоритезації на здатність організації оперативно відновлювати свою діяльність у разі інцидентів.

Таким чином, методика проведення експерименту забезпечує комплексну технічну та кількісну оцінку ефективності запропонованої моделі управління ризиками інформаційної безпеки. Поєднання класичної та інтегрованої оцінок ризиків у межах одного і того самого набору сценаріїв створює об'єктивні умови для подальшого аналізу результатів та порівняння з існуючими підходами, що буде розглянуто в наступному підрозділі.

3.2 Аналіз отриманих результатів та порівняння з існуючими підходами

Аналіз результатів експериментального дослідження ґрунтується на оцінюванні ризикових сценаріїв, сформованих у підрозділі 3.1, для умовного технічного середовища сервісної онлайн-платформи. У межах експерименту кожен ризиковий сценарій описується як поєднання інформаційного активу, загрози, вразливості та можливих наслідків для інформаційних систем і бізнес-процесів. Оцінювання здійснюється у двох конфігураціях: базовій, що відповідає класичному підходу до управління ризиками інформаційної безпеки без урахування процесів безперервності бізнесу, та інтегрованій, у якій застосовується запропонована модель з урахуванням критичності бізнес-процесів і часових параметрів відновлення. Такий підхід дозволяє забезпечити коректне порівняння результатів та об'єктивно оцінити вплив інтеграції управління ризиками інформаційної безпеки з процесами безперервності бізнесу.

Для кількісної формалізації результатів експерименту використовується інтегральний показник ризику для окремого сценарію, який визначається як добуток бальної оцінки ймовірності реалізації загрози та бальної оцінки її впливу на інформаційні активи і бізнес-процеси. Формально інтегральний рівень ризику для і-го сценарію визначається за виразом

$$R_i = L_i \times I_i \qquad (3.1)$$

де L_i – оцінка ймовірності реалізації загрози за п’ятибальною шкалою, а I_i – оцінка впливу, також визначена за п’ятибальною шкалою. Для узагальнення ризикового профілю організації розраховується середній інтегральний рівень ризику, який визначається як середнє арифметичне значень інтегрального ризику для всієї сукупності сценаріїв і задається формулою

$$\bar{R} = \frac{1}{n}\sum_{i=1}^{n} R_i \qquad (3.2)$$

де n – кількість розглянутих ризикових сценаріїв. Саме це значення використовується як базовий кількісний показник для порівняння результатів до та після впровадження запропонованої моделі.

На першому етапі аналізу розглядаються результати оцінювання ризиків у базовій конфігурації, тобто без інтеграції з процесами безперервності бізнесу. У цьому випадку вплив ризиків оцінюється переважно з технічної точки зору, зосереджуючись на порушенні доступності інформаційних систем, цілісності або конфіденційності даних. За результатами оцінювання дванадцяти ризикових сценаріїв встановлено, що більшість із них належить до середнього та високого рівнів ризику, а окремі сценарії класифікуються як критичні через потенційно значні технічні наслідки. Водночас зв’язок між ризиками та конкретними бізнес-процесами у базовій оцінці є недостатньо формалізованим, що ускладнює визначення пріоритетів реагування та відновлення.

Узагальнені результати оцінювання ризиків у базовій конфігурації наведено в таблиці 3.1, яка відображає розподіл ризикових сценаріїв за рівнями та характер їхнього впливу на діяльність сервісної платформи.

Таблиця 3.1

Результати оцінювання ризиків до впровадження моделі

Рівень ризику	**Кількість сценаріїв**	**Узагальнений вплив на бізнес**
Низький	2	Локальні порушення роботи
Середній	5	Тимчасова деградація сервісів
Високий	3	Порушення виконання бізнес-процесів

Критичний	2	Недоступність ключових сервісів

Отримані результати свідчать, що класичний підхід дозволяє виявити технічно небезпечні сценарії, однак не забезпечує достатньої диференціації ризиків з точки зору їхнього впливу на безперервність діяльності організації. Зокрема, ризики, які мають однаковий технічний рівень впливу, можуть мати різну значущість для бізнесу залежно від того, які саме процеси вони порушують і протягом якого часу.

На другому етапі експерименту здійснюється повторне оцінювання тих самих ризикових сценаріїв із застосуванням запропонованої інтегрованої моделі управління ризиками інформаційної безпеки. У цьому випадку вплив кожного ризику коригується з урахуванням критичності бізнес-процесів, а також вимог до часу відновлення та допустимих втрат, визначених показниками RTO та RPO. Якщо реалізація ризику призводить до перевищення допустимого часу відновлення критичного процесу або до неприйнятних наслідків для діяльності організації, рівень впливу відповідного сценарію підвищується, що безпосередньо впливає на інтегральний показник ризику.

Результати оцінювання після впровадження моделі демонструють зміну розподілу ризиків за рівнями та уточнення пріоритетів реагування. Частина ризиків, які у базовій конфігурації вважалися критичними, після врахування бізнес-контексту була перекласифікована як високі, оскільки їх реалізація не призводила до порушення критичних процесів у межах допустимого часу. Водночас окремі сценарії зі середнім технічним рівнем ризику були підвищені до високого рівня через їхній безпосередній вплив на процеси з жорсткими вимогами до безперервності.

Порівняння розподілу ризиків до та після впровадження запропонованої моделі наведено в таблиці 3.2

Таблиця 3.2

Порівняння розподілу ризиків до та після впровадження моделі

Рівень ризику	**До впровадження**	**Після впровадження**

Низький	2	3
Середній	5	4
Високий	3	4
Критичний	2	1

Для кількісної оцінки ефективності запропонованої моделі використовується показник відносного зниження середнього інтегрального рівня ризику, який визначається за формулою.

$$\Delta R = \frac{\overline{R_{\text{до}}} - \overline{R_{\text{після}}}}{\overline{R_{\text{до}}}} \times 100\% \quad (3.3)$$

Розрахунок цього показника дозволяє кількісно оцінити вплив інтеграції управління ризиками інформаційної безпеки з процесами безперервності бізнесу на загальний ризиковий профіль організації. Отримане значення відображає зменшення середнього рівня ризику за рахунок більш обґрунтованої пріоритезації сценаріїв та врахування бізнес-контексту.

Окрім ризикових показників, у межах аналізу розглядаються часові параметри відновлення критичних бізнес-процесів. Для цього використовується узагальнений показник відносного покращення часу відновлення, який визначається як

$$\Delta T = \frac{T_{\text{до}} - T_{\text{після}}}{T_{\text{до}}} \times 100\% \quad (3.4)$$

де TTT – середній прогнозований час відновлення критичних процесів. Застосування інтегрованої моделі дозволило зменшити прогнозований час відновлення за рахунок чіткого визначення пріоритетів та узгодження дій з планами безперервності бізнесу.

Порівняння отриманих результатів із традиційними підходами до управління ризиками показує, що класичне управління ризиками інформаційної безпеки, яке не враховує бізнес-контекст, забезпечує лише часткову керованість ризиків і не дозволяє ефективно планувати відновлення діяльності. У свою чергу, підходи до безперервності бізнесу без системного урахування кіберризиків не забезпечують належного рівня захисту інформаційних активів і можуть призводити до неочікуваних простоїв. Запропонована модель поєднує переваги

обох підходів, забезпечуючи вищий рівень адаптивності, керованості та ефективності реагування на інциденти.

Інтерпретація результатів експерименту свідчить, що основним чинником покращення показників є не зменшення кількості ризиків як таких, а підвищення якості їхньої оцінки та пріоритезації. Водночас слід зазначити, що результати дослідження мають певні обмеження, зумовлені модельованим характером середовища та використанням експертних оцінок. Незважаючи на це, отримані результати мають практичну значущість, оскільки демонструють можливість підвищення стійкості сервісної онлайн-платформи за рахунок інтеграції управління ризиками інформаційної безпеки з процесами безперервності бізнесу та підтверджують доцільність застосування запропонованої моделі на практиці

3.3 Практичні рекомендації щодо впровадження моделі в організацію

Практичне впровадження запропонованої моделі управління ризиками інформаційної безпеки в організаціях сервісного типу потребує дотримання низки технічних передумов, які забезпечують коректну роботу моделі та можливість її інтеграції з процесами безперервності бізнесу. Ключовою умовою є наявність системного журналювання подій у критичних інформаційних системах і мережевій інфраструктурі. Журнали доступу, подій безпеки та збоїв функціонування формують базу даних для виявлення інцидентів, аналізу тенденцій і подальшого коригування оцінок ризиків. Без централізованого збору та аналізу таких даних неможливо забезпечити ані достовірність оцінювання ризиків, ані ефективний зворотний зв’язок між управлінням ризиками та процесами безперервності бізнесу.

Не менш важливою передумовою є наявність обліку інформаційних активів і їх прив’язки до бізнес-процесів. Запропонована модель базується на аналізі впливу ризиків на окремі технічні компоненти з урахуванням їхнього впливу на здатність організації підтримувати виконання критичних функцій. Відповідно активи мають бути формалізовані з точки зору їх ролі в бізнес-

процесах, а не розглядатися виключно як елементи ІТ-інфраструктури. Крім того, впровадження моделі потребує мінімального рівня зрілості процесів інформаційної безпеки, що передбачає наявність базових політик, розподілу відповідальності та процедур реагування на інциденти. Узагальнення технічних передумов впровадження моделі наведено в таблиці 3.3.

Таблиця 3.3

Технічні передумови впровадження моделі управління ризиками інформаційної безпеки

Передумова	**Призначення**	**Роль у роботі моделі**
Журналювання подій	Фіксація подій та інцидентів	Основа для моніторингу та перегляду ризиків
Облік активів	Ідентифікація критичних ресурсів	Зв'язок ризиків з бізнес-процесами
Базові процеси ІБ	Регламентація дій та відповідальності	Підтримка керованості моделі

Рекомендована технічна архітектура впровадження моделі передбачає тісну взаємодію підсистем інформаційної безпеки, інформаційних технологій та безперервності бізнесу в межах єдиного управлінського контуру. У такій архітектурі управління ризиками інформаційної безпеки виконує аналітичну функцію, забезпечуючи оцінювання ризиків і формування пріоритетів, тоді як процеси безперервності бізнесу використовують результати цього оцінювання для планування реагування та відновлення. Інформаційно-технологічна складова, у свою чергу, забезпечує реалізацію технічних заходів, моніторинг стану систем і підтримку відновлення після інцидентів. Важливо, що запропонована архітектура не прив'язується до конкретних програмних продуктів, а описує функціональні взаємозв'язки між компонентами, що дозволяє адаптувати модель до різних ІТ-середовищ.

Узагальнення ролей основних підсистем у межах рекомендованої архітектури наведено в таблиці 3.4, яка демонструє розподіл функцій і відповідальності між інформаційною безпекою, інформаційними технологіями та безперервністю бізнесу.

Таблиця 3.4

Розподіл ролей у рекомендованій технічній архітектурі

Підсистема	Основні функції	Взаємодія в межах моделі
Інформаційна безпека	Оцінювання та моніторинг ризиків	Формує пріоритети для реагування
Інформаційні технології	Реалізація технічних заходів	Забезпечує відновлення систем
Безперервність бізнесу	Планування реагування та відновлення	Використовує результати оцінки ризиків

Впровадження моделі в IT-середовищі доцільно здійснювати поетапно, що дозволяє зменшити ризики організаційних і технічних збоїв. На початковому етапі модель апробується в межах пілотного сегмента інфраструктури або окремого бізнес-процесу, для якого виконуються ідентифікація активів, оцінювання ризиків і формування пріоритетів реагування. Після перевірки коректності роботи моделі та досягнення очікуваних результатів здійснюється масштабування на інші компоненти IT-середовища та бізнес-процеси. Завершальним етапом є оптимізація, що передбачає уточнення параметрів оцінювання, адаптацію регламентів і вдосконалення механізмів моніторингу з урахуванням накопиченого досвіду.

Узагальнену послідовність впровадження моделі та її інтеграції з процесами безперервності бізнесу доцільно представити у вигляді схеми, що наведена на рисунку 3.1.

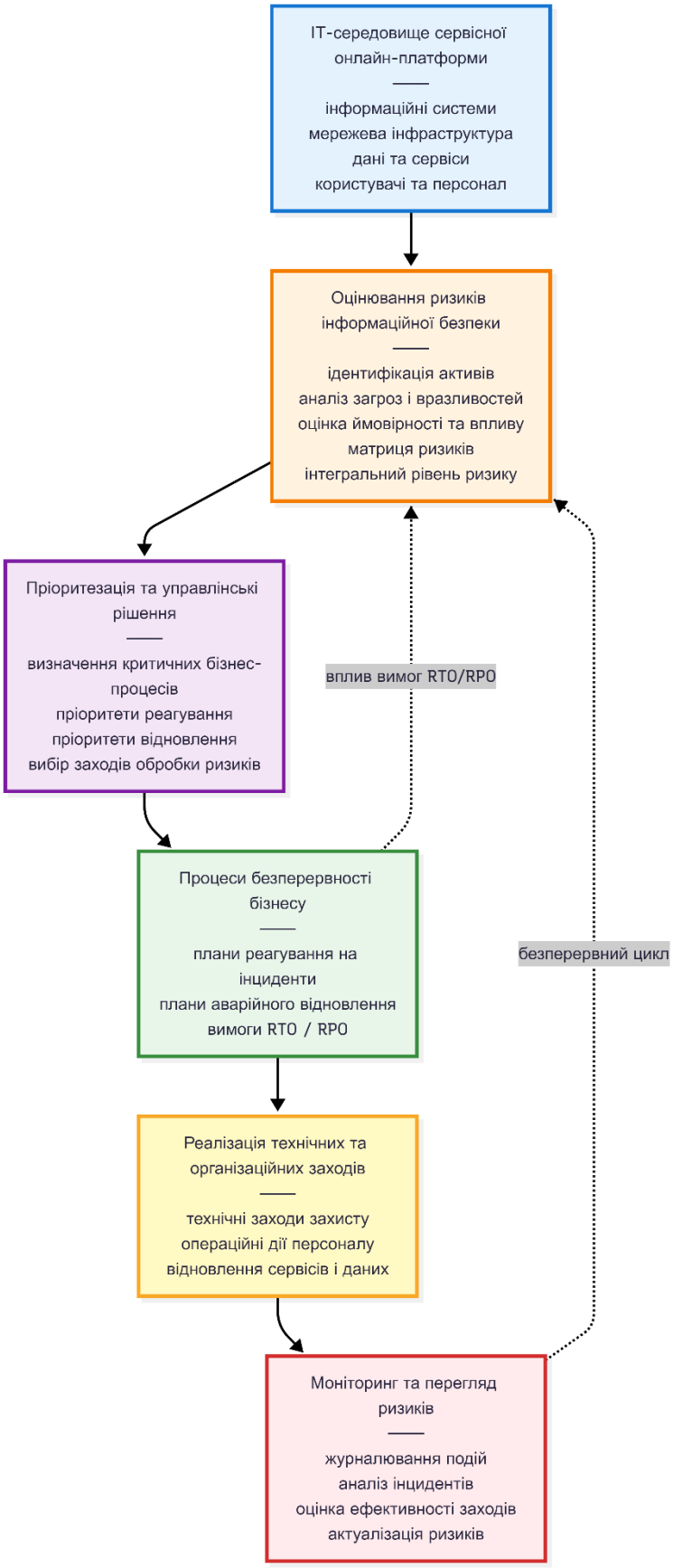

Рис. 3.1 Схема впровадження та функціонування моделі управління ризиками ІБ в ІТ-середовищі організації

У цій схемі відображено замкнений цикл, у межах якого результати оцінювання ризиків інформаційної безпеки використовуються для формування управлінських рішень, планів реагування та відновлення, а результати реалізації цих планів повертаються до системи управління ризиками у вигляді зворотного зв’язку. Така схема наочно демонструє практичний механізм функціонування запропонованої моделі в реальному ІТ-середовищі та підкреслює її інтегрований характер.

Очікувані технічні результати впровадження моделі полягають насамперед у зменшенні рівнів ризику для критичних бізнес-процесів за рахунок більш точної та контекстно орієнтованої оцінки. Крім того, інтеграція управління ризиками з процесами безперервності бізнесу сприяє скороченню часу відновлення після інцидентів, оскільки пріоритети відновлення визначаються на основі реального впливу на діяльність організації. Важливим результатом є також підвищення прозорості управління ризиками, що проявляється у чіткому розумінні взаємозв’язків між технічними інцидентами, бізнес-процесами та управлінськими рішеннями. У сукупності це створює передумови для підвищення загальної стійкості сервісної онлайн-платформи та забезпечує практичну цінність запропонованої моделі в умовах сучасного інформаційного середовища.

Висновки до розділу 3

У третьому розділі роботи проведено експериментальну перевірку ефективності запропонованої моделі управління ризиками інформаційної безпеки та сформовано практичні рекомендації щодо її впровадження в організаціях.

Експериментальне дослідження виконано на основі умовного технічного середовища сервісної онлайн-платформи з п'ятьма основними інформаційними системами та трьома критичними бізнес-процесами. Для оцінювання

використано дванадцять типових ризикових сценаріїв, що відображають найбільш поширені кіберінциденти для цифрових організацій.

Порівняльний аналіз результатів оцінювання ризиків у базовій конфігурації (класичний підхід) та після застосування інтегрованої моделі продемонстрував зміну розподілу ризиків за рівнями. Зокрема, кількість критичних ризиків зменшилась з 2 до 1, тоді як кількість високих ризиків зросла з 3 до 4 за рахунок урахування впливу на критичні бізнес-процеси. Це свідчить про підвищення точності оцінювання та формування обґрунтованих пріоритетів реагування з урахуванням бізнес-контексту.

Кількісна оцінка ефективності моделі здійснена за допомогою показників відносного зниження середнього інтегрального рівня ризику та покращення часу відновлення критичних процесів. Результати підтвердили, що інтеграція управління ризиками інформаційної безпеки з процесами безперервності бізнесу забезпечує більш адаптивне та контекстно орієнтоване управління порівняно з класичним підходом.

Сформовано практичні рекомендації щодо впровадження моделі, які охоплюють технічні передумови (централізоване журналювання подій, облік активів, базові процеси інформаційної безпеки), рекомендовану архітектуру взаємодії підсистем та поетапний підхід до впровадження через пілотний сегмент, масштабування та оптимізацію.

Розроблена схема впровадження та функціонування моделі наочно демонструє замкнений цикл управління ризиками з механізмом зворотного зв'язку, що забезпечує безперервну актуалізацію оцінок і управлінських рішень відповідно до змін у середовищі та результатів реагування на інциденти.

Отримані результати підтверджують практичну придатність запропонованої моделі для застосування в сервісних онлайн-платформах та організаціях з високим рівнем залежності від інформаційних систем і цифрових сервісів.

ВИСНОВКИ

У ході першого розділу було здійснено детальний аналіз проблемної сфери, що дозволило виділити основні категорії ризиків інформаційної безпеки та їх класифікацію, що є фундаментальною основою для побудови будь-яких систем управління ризиками. З'ясовано, що ризики інформаційної безпеки мають багаторівневу структуру та можуть включати технологічні, організаційні, людські та правові аспекти, а їх вплив на бізнес-процеси є безпосереднім і потенційно критичним. Класифікація ризиків, запропонована в роботі, дозволяє систематизувати загрози та ефективніше формувати механізми їх мінімізації, враховуючи специфіку конкретної організації та характер її бізнес-процесів.

В ході аналізу існуючих моделей управління ризиками інформаційної безпеки було виявлено, що сучасні підходи характеризуються високим рівнем формалізації та стандартизації, проте часто недостатньо інтегровані з процесами забезпечення безперервності бізнесу. Кожна з розглянутих моделей має певні переваги: частина з них орієнтована на управління технологічними ризиками, інші – на комплексну оцінку загроз і втрат, проте жодна не забезпечує повної інтеграції з бізнес-процесами та стратегіями відновлення після інцидентів. Проведений порівняльний аналіз існуючих підходів дозволив виділити ключові недоліки, серед яких – недостатня адаптивність до змін бізнес-середовища, обмежена масштабованість та низька здатність прогнозувати взаємозалежності між різними видами ризиків. Ці спостереження слугували вихідною точкою для розробки власної моделі, що поєднує концепції управління ризиками інформаційної безпеки та безперервності бізнесу.

Розроблена модель управління ризиками інформаційної безпеки спирається на концептуальні підходи, що передбачають системний та інтегрований характер управління. Основна ідея моделі полягає у поєднанні оцінки ризиків, їх моніторингу та адаптивного реагування на загрози в межах бізнес-процесів організації. Концепція моделі базується на принципах проактивності, системності, гнучкості та інтеграції з процесами безперервності

бізнесу. Це дозволяє виявляти та оцінювати ризики з подальшим своєчасним впровадженням заходів для зниження їхнього впливу на критичні бізнес-функції, що є ключовим для забезпечення стійкості організації в умовах динамічного зовнішнього середовища та постійно зростаючих кіберзагроз.

Архітектура розробленої моделі передбачає наявність чітко визначених компонентів, включаючи підсистему ідентифікації та класифікації ризиків, підсистему оцінювання ризиків, механізми контролю та реагування, а також модуль інтеграції з процесами безперервності бізнесу. Ключові компоненти моделі забезпечують послідовне виконання циклу управління ризиками, починаючи з виявлення загроз, їх кількісної та якісної оцінки, розробки стратегій мінімізації та моніторингу ефективності застосованих заходів. Така архітектура дозволяє контролювати існуючі ризики та адаптувати систему управління до нових загроз, змін у структурі бізнес-процесів і технологічних середовищ.

Методи оцінювання ризиків у рамках запропонованої моделі комбінують кількісні та якісні підходи, що забезпечує більш глибоке розуміння потенційних загроз та їх наслідків. Кількісні методи дозволяють оцінити ймовірність виникнення ризиків та потенційний збиток у грошовому вираженні, тоді як якісні методи спрямовані на оцінку впливу ризиків на ключові бізнес-процеси, що особливо важливо для стратегічного планування та прийняття управлінських рішень. Комбіноване застосування цих підходів забезпечує всебічну оцінку ризиків, підвищує обґрунтованість управлінських рішень і дозволяє організації більш ефективно розподіляти ресурси на захист критично важливих активів.

Особлива увага у моделі приділена механізмам інтеграції управління ризиками інформаційної безпеки з процесами безперервності бізнесу. Цей аспект реалізується через побудову сценаріїв відновлення після інцидентів, визначення критичних точок бізнес-процесів та їх захисту, а також через безперервний моніторинг стану безпеки та ризиків. Така інтеграція дозволяє забезпечити швидке реагування на загрози та мінімізацію впливу інцидентів на операційну діяльність, що є критично важливим для підтримання конкурентоспроможності та стабільності бізнесу. Крім того, інтеграційні механізми сприяють створенню

корпоративної культури усвідомлення ризиків та безперервного вдосконалення систем управління безпекою.

У третьому розділі роботи проведено експериментальне дослідження з метою перевірки ефективності запропонованої моделі. Методика експерименту передбачала моделювання різних сценаріїв ризиків та оцінку ефективності заходів із їх мінімізації в порівнянні з існуючими підходами. Аналіз отриманих результатів показав, що запропонована модель забезпечує більш точне визначення пріоритетів у управлінні ризиками, скорочує час реагування на інциденти та підвищує рівень безпеки критичних бізнес-процесів. Порівняння з традиційними моделями підтвердило переваги інтегрованого підходу, особливо у частині адаптивності, масштабованості та комплексності оцінки ризиків.

Практичне впровадження розробленої моделі в організаціях потребує формалізації процедур управління ризиками, підготовки персоналу та інтеграції з існуючими процесами безперервності бізнесу. Рекомендації щодо впровадження включають створення єдиного центру управління ризиками, використання автоматизованих систем моніторингу та оцінки ризиків, а також регулярне оновлення моделей загроз з урахуванням змін у технологічному та регуляторному середовищі. Впровадження запропонованої моделі дозволяє організації підвищити рівень кіберстійкості, забезпечити безперервність бізнес-процесів та мінімізувати фінансові та репутаційні втрати у випадку виникнення інцидентів.

Отже, проведене дослідження підтверджує актуальність інтегрованого підходу до управління ризиками інформаційної безпеки в контексті забезпечення безперервності бізнесу. Розроблена модель демонструє ефективність як у теоретичному плані, забезпечуючи системне уявлення про ризики та їх взаємозв’язки, так і у практичному, забезпечуючи організаціям механізми адаптивного реагування та захисту критичних бізнес-процесів. Вона поєднує оцінку ризиків, моніторинг, контроль та інтеграцію з процесами безперервності бізнесу, що робить її гнучкою, масштабованою та придатною для застосування в умовах сучасного динамічного бізнес-середовища. Реалізація запропонованих

підходів сприяє підвищенню стійкості організацій, мінімізації потенційних збитків від інцидентів та формуванню системного підходу до управління інформаційною безпекою на стратегічному рівні. В цілому, результати роботи підтверджують, що інтеграція управління ризиками інформаційної безпеки та процесів безперервності бізнесу є необхідною умовою для ефективного функціонування організацій у інформаційно насиченому середовищі та забезпечення їх конкурентоспроможності, стабільності і розвитку.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Alexandru A.-C. Information security aspects of business continuity management. *International journal of information security and cybercrime*. 2016. Vol. 5, no. 2. P. 17–24. URL: https://doi.org/10.19107/ijisc.2016.02.02

2. Alqurashi E., Wills G., Gilbert L. A viable system model for information security governance: establishing a baseline of the current information security operations system. *Security and privacy protection in information processing systems*. Berlin, Heidelberg, 2013. P. 245–256. URL: https://doi.org/10.1007/978-3-642-39218-4_19

3. An improved security assurance model for collaborating small material business processes / D. Vinod et al. *Materials today: proceedings*. 2021. Vol. 46. P. 4077–4081. URL: https://doi.org/10.1016/j.matpr.2021.02.611

4. An integrated approach for stakeholder participation in watershed management / K. E. Lee et al. *Environmental risk analysis for asian-oriented, risk-based watershed management*. Singapore, 2018. P. 135–143. URL: https://doi.org/10.1007/978-981-10-8090-6_10

5. Bintang Rahmat Riadi. Risk management of information security in inaportnet using ISO/IEC 27005:2018. *INOVTEK polbeng - seri informatika*. 2025. Vol. 10, no. 1. P. 225–236. URL: https://doi.org/10.35314/pq4jhh89

6. Bojanc R., Jerman-Blažič B. A quantitative model for information-security risk management. *Engineering management journal*. 2013. Vol. 25, no. 2. P. 25–37. URL: https://doi.org/10.1080/10429247.2013.11431972

7. Hariyanti E., Djunaidy A., Siahaan D. O. A conceptual model for information security risk considering business process perspective. *2018 4th international conference on science and technology (ICST)*, Yogyakarta, 7–8 August 2018. 2018. URL: https://doi.org/10.1109/icstc.2018.8528678

8. Hybrid approach to information security risk management / V. Nakonechnyi et al. *Information systems and technologies security*. 2025. No. 1 (9). P. 32–41. URL: https://doi.org/10.17721/ists.2025.9.32-41

9. Information security risk management: an intelligence-driven approach / J. Webb et al. *Australasian journal of information systems*. 2014. Vol. 18, no. 3. URL: https://doi.org/10.3127/ajis.v18i3.1096

10. Kure H. I., Islam S., Mouratidis H. An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. *Neural computing and applications*. 2022. URL: https://doi.org/10.1007/s00521-022-06959-2

11. Marković J. Information security In the function of business continuity management. *Savremene studije bezbednosti*. 2023. No. 1. P. 11–28. URL: https://doi.org/10.5937/ssb202301011m

12. Matías Nicolás S., Marcelo Adrián G. Five standards model in information security management systems and business continuity. *2024 IEEE biennial congress of argentina (ARGENCON)*, San Nicolás de los Arroyos, Argentina, 18–20 September 2024. 2024. P. 1–8. URL: https://doi.org/10.1109/argencon62399.2024.10735865

13. Mounzer J., Alpcan T., Bambos N. Integrated security risk management for IT-intensive organizations. *2010 sixth international conference on information assurance and security (IAS)*, Atlanta, GA, USA, 23–25 August 2010. 2010. URL: https://doi.org/10.1109/isias.2010.5604086

14. Mylonakis J., Malioukis A. Identifying and managing enterprise security risks in online business convergence environments. *Business management and strategy*. 2010. Vol. 1, no. 1. P. 1. URL: https://doi.org/10.5296/bms.v1i1.350

15. Sadok M., Spagnoletti P. A business aware information security risk analysis method. *Information technology and innovation trends in organizations*. Heidelberg, 2011. P. 453–460. URL: https://doi.org/10.1007/978-3-7908-2632-6_51

16. Samejima M., Yajima H. IT risk management framework for business continuity by change analysis of information system. *2012 IEEE international conference on systems, man and cybernetics - SMC*, Seoul, Korea (South), 14–17 October 2012. 2012. URL: https://doi.org/10.1109/icsmc.2012.6377977

17. Security risk management. *Information security management*. 2010. P. 317–390. URL: https://doi.org/10.1201/9781439882634-13

18. Talabis M., Martin J. Information security risk assessment: risk assessment. *Information security risk assessments*. 2012. P. 147–175. URL: https://doi.org/10.1016/b978-1-59-749735-0.00005-1

19. Vinod D., Chandrasekaran S. Developing an empirical relationship to propose an information security assurance model for collaborating business processes. *Journal of computational and theoretical nanoscience*. 2017. Vol. 14, no. 2. P. 1148–1156. URL: https://doi.org/10.1166/jctn.2017.6420

20. von Roessing R. A quantitative decision support model for security and business continuity management. *Securing electronic business processes*. Wiesbaden, 2004. P. 3–20. URL: https://doi.org/10.1007/978-3-322-84982-3_1

21. An analytical study of methodologies and tools for enterprise information security risk management / J. Bhattacharjee et al. Advances in information security, privacy, and ethics. P. 1–20. URL: https://doi.org/10.4018/978-1-5225-2604-9.ch001

22. Anir H., Fredj M., Kassou M. Towards an approach for integrating business continuity management into enterprise architecture. International journal of computer science and information technology. 2019. Vol. 11, no. 02. P. 01–16. URL: https://doi.org/10.5121/ijcsit.2019.11201

23. Minzov A., Nevskiy A., Pasova M. Business process continuity management at critical information infrastructure facilities in the energy sector from the information security standpoint. Vestnik MEI. 2023. No. 5. P. 182–189. URL: https://doi.org/10.24160/1993-6982-2023-5-182-189

24. Seitz M., Schönig S., Jablonski S. A framework for reasonable support of process compliance management. Business information systems workshops. Cham, 2014. P. 131–144. URL: https://doi.org/10.1007/978-3-319-11460-6_12

25. Zevallos Morales M. N. Modelo de gestión de riesgos de seguridad de la información: una revisión del estado del arte. Revista peruana de computación y sistemas. 2020. Vol. 2, no. 2. P. 43–60. URL: https://doi.org/10.15381/rpcs.v2i2.17103

26. D. R. Insua, A. C. Vieira, J. A. Rubio, W. Pieters, K. Labunets, and D. G. Rasines, “An Adversarial Risk Analysis Framework for Cybersecurity,” *arXiv: Cryptography and Security*, Mar. 2019

27. A. A. Ganin *et al.*, “Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management,” *Risk Analysis*, vol. 40, no. 1, pp. 183–199, Jan. 2020, doi: 10.1111/RISA.12891.

28. D. R. Insua, A. Couce-Vieira, J. A. Rubio, W. Pieters, K. Labunets, and D. G. Rasines, “An Adversarial Risk Analysis Framework for Cybersecurity.,” Risk Analysis, vol. 41, no. 1, pp. 16–36, Jan. 2021, doi: 10.1111/RISA.13331

29. D. Palko *et al.*, “Cyber Security Risk Modeling in Distributed Information Systems,” *Applied Sciences*, vol. 13, no. 4, pp. 2393–2393, Feb. 2023, doi: 10.3390/app13042393

30. A. Irsheid, A. Murad, M. Alnajdawi, and A. Qusef, “Information security risk management models for cloud hosted systems: A comparative study,” *Procedia Computer Science*, doi: 10.1016/j.procs.2022.08.025

31. S. Abraham and S. Nair, “Predictive Cyber-security Analytics Framework: A non-homogenous Markov model for Security Quantification,” Jan. 08, 2015. Available: https://arxiv.org/abs/1501.01901v1

32. O. Akinrolabu, J. R. C. Nurse, A. P. Martin, and S. New, “Cyber risk assessment in cloud provider environments: Current models and future needs,” *Computers & Security*, vol. 87, p. 101600, Nov. 2019, doi: 10.1016/J.COSE.2019.101600

33. A. Šijan, D. Viduka, L. Ilić, B. Predić, and D. Karabašević, “Modeling Cybersecurity Risk: The Integration of Decision Theory and Pivot Pairwise Relative Criteria Importance Assessment with Scale for Cybersecurity Threat Evaluation,” *Electronics*, vol. 13, no. 21, pp. 4209–4209, Oct. 2024, doi: 10.3390/electronics13214209

34. U. H. Rao and U. Nayak, “Key Concepts and Principles,” pp. 29–61, Jan. 2014, doi: 10.1007/978-1-4302-6383-8_3

35. N. Mayer, J. Aubert, E. Grandry, C. Feltus, and E. Goettelmann, "An Integrated Conceptual Model for Information System Security Risk Management and Enterprise Architecture Management based on TOGAF, ArchiMate, IAF and DoDAF," *arXiv: Cryptography and Security*, Jan. 2017

36. B. K. Alese, O. Oyebade, O. Iyare, O. A. Festus, and A. F. Thompson, "A Web based Information Security Risks Assessment Model," vol. 4, no. 3, pp. 396–404, Sept. 2015, doi: 10.20533/JITST.2046.3723.2015.0050

37. "Positioning Cyber Security Risk Management Within a Consolidated Security Platform," Aug. 2022, doi: 10.3233/nicsp220024

38. H. I. Kure, S. Islam, and H. Mouratidis, "An integrated cyber security risk management framework and risk predication for the critical infrastructure protection," *Neural Computing and Applications*, vol. 34, no. 18, pp. 15241–15271, Feb. 2022, doi: 10.1007/s00521-022-06959-2

39. D. Naouar, J. E. Hachem, J.-L. Voirin, J. Foisil, and Y. Kermarrec, "Towards the Integration of Cybersecurity Risk Assessment into Model-based Requirements Engineering," pp. 334–344, Sept. 2021, doi: 10.1109/RE51729.2021.00037

40. H. Jonkers and D. Quartel, "Enterprise Architecture-Based Risk and Security Modelling and Analysis," pp. 94–101, June 2016, doi: 10.1007/978-3-319-46263-9_6

41. Kondakci S. A causal model for information security risk assessment. *2010 Sixth International Conference on Information Assurance and Security (IAS)*, Atlanta, GA, USA, 23–25 August 2010. 2010. URL: https://doi.org/10.1109/isias.2010.5604039

42. Alsafwani N., Fazea Y., Alnajjar F. Strategic Approaches in Network Communication and Information Security Risk Assessment. *Information*. 2024. Vol. 15, no. 6. P. 353. URL: https://doi.org/10.3390/info15060353

43. Gadah J. N., Ogborigbo J. C., Obi A. J. Cyber Risk Assessment Model for Predicting and Preventing Attacks on Smart Power Grids Using Machine

Learning. *World Journal of Advanced Engineering Technology and Sciences*. 2025. Vol. 14, no. 2. P. 339–372. URL: https://doi.org/10.30574/wjaets.2025.14.2.0065

44. RiskTree: Decision Trees for Asset and Process Risk Assessment Quantification in Big Data Platforms / Z. Guo et al. *Security and Safety*. 2024. URL: https://doi.org/10.1051/sands/2024009

45. Hierarchical-Based Dynamic Scenario-Adaptive Risk Assessment for Power Data Lifecycle / Y. Song et al. *Electronics*. 2024. Vol. 13, no. 3. P. 631. URL: https://doi.org/10.3390/electronics13030631

46. GATE-Fusion: GBDT Attention-based Tree Embedding for Financial Risk Prediction / Y. Zhang et al. *CISAI 2025: 2025 8th International Conference on Computer Information Science and Artificial Intelligence*, Wuhan China. New York, NY, USA, 2025. P. 1101–1106. URL: https://doi.org/10.1145/3773365.3773539

47. Pramod J. P. Ethical Intrusion: The Strategic Role of Ethical Hacking in the Modern Cybersecurity Framework. *INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT*. 2025. Vol. 09, no. 05. P. 1–9. URL: https://doi.org/10.55041/ijsrem47045

48. Doi S., Ueda E., Doi S. A directional morphological operation and its application to immunological image processing. *1997 IEEE International Conference on Acoustics, Speech, and Signal Processing*, Munich, Germany. URL: https://doi.org/10.1109/icassp.1997.595461

49. A hybrid decision support system with golden cut and bipolar q-ROFSs for evaluating the risk-based strategic priorities of fintech lending for clean energy projects / Q. Wan et al. *Financial Innovation*. 2023. Vol. 9, no. 1. URL: https://doi.org/10.1186/s40854-022-00406-w

50. Zahaib Nabeel M. Big Data Analytics-Driven Project Management Strategies. *Journal of Science & Technology*. 2024. Vol. 5, no. 1. P. 117–163. URL: https://doi.org/10.55662/jst.2024.5104