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: “УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ОРГАНІЗАЦІЇ”

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 ІЛЛЯШЕНКО
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБДМ-61 ІЛЛЯШЕНКО Олексій
Керівник: САВЧЕНКО Віталій Анатолійович, д-р техн. наук, проф.
Рецензент:

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 Ілляшенко Олексію
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: "Управління інформаційною безпекою в умовах цифрової трансформації організації"
керівник кваліфікаційної роботи САВЧЕНКО Віталій Анатолійович, д-р техн. наук, проф.
затверджені наказом Державного університету інформаційно-комунікаційних технологій від "15" жовтня 2024 р. № 320.
2. Строк подання кваліфікаційної роботи "25" грудня 2025 р.
3. Вихідні дані до кваліфікаційної роботи: інформаційна безпека організації, цифрова трансформація, загрози та вразливості інформаційних систем, методи та моделі управління інформаційною безпекою, оцінювання ризиків, нормативно-правові акти у сфері захисту інформації, міжнародні стандарти інформаційної безпеки, наукова та технічна література.
4. Перелік питань, які потрібно розробити:
    1. Дослідити науково-теоретичні підходи до управління інформаційною безпекою організації в умовах цифрової трансформації.
    2. Проаналізувати методи та моделі оцінювання стану інформаційної безпеки організації.
    3. Розробити практичну концепцію вдосконалення управління інформаційною безпекою організації в умовах цифрової трансформації.

4. Перелік ілюстративного матеріалу: *презентація*
5. Дата видачі завдання "02" жовтня 2024 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 науково-теоретичних підходів до управління інформаційною безпекою в умовах цифрової трансформації.	27.10.2025	
4.	Дослідження методів і моделей оцінювання стану інформаційної безпеки організації та аналіз загроз і вразливостей інформаційного середовища в умовах цифрової трансформації.	10.11.2025	
5.	Розроблення практичної концепції вдосконалення управління інформаційною безпекою організації в умовах цифрової трансформації та обґрунтування заходів підвищення рівня захищеності інформаційних ресурсів.	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.	19.01.2026	

Здобувач вищої освіти _____ *(підпис)* ІЛЛЯШЕНКО Олексій

Керівник кваліфікаційної роботи _____ *(підпис)* САВЧЕНКО Віталій Анатолійович

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 Ілляшенко О. 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: "Управління інформаційною безпекою в умовах цифрової трансформації організації"
Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач **ІЛЛЯШЕНКО Олексій** у кваліфікаційній роботі дослідив науково-теоретичні підходи до управління інформаційною безпекою організації в умовах цифрової трансформації, проаналізував методи та моделі оцінювання стану інформаційної безпеки, а також розробив практичну концепцію вдосконалення управління інформаційною безпекою підприємства з урахуванням сучасних цифрових технологій.

ІЛЛЯШЕНКО Олексій продемонстрував високий рівень теоретичної та практичної підготовки, володіння науково-дослідницькими методами, уміння самостійно формулювати проблеми дослідження та пропонувати обґрунтовані рішення.

Все це дозволяє оцінити кваліфікаційну роботу здобувача **ІЛЛЯШЕНКА 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 _____САВЧЕНКО Віталій Анатолійович
(підпис)
"_____"_____2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Ілляшенко О. 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 **ІЛЛЯШЕНКА Олексія**

на тему "Управління інформаційною безпекою в умовах цифрової трансформації організації".

Актуальність У сучасних організаціях цифрова трансформація спричинює збільшення обсягів обробки інформації та використання віддалених сервісів, що значно підвищує ризики для інформаційної безпеки. Забезпечення надійного управління інформаційною безпекою в умовах цифрової трансформації є важливим завданням для підтримки безперервності бізнес-процесів, захисту даних клієнтів та ресурсів організації. З огляду на зазначене, проведене дослідження є актуальним та своєчасним науковим завданням.

Позитивні сторони

1. У роботі детально досліджено науково-теоретичні підходи до управління інформаційною безпекою в умовах цифрової трансформації, проведено аналіз сучасних методів і моделей оцінювання стану безпеки організацій, а також розроблено практичну концепцію вдосконалення управління інформаційною безпекою.

2. Кваліфікаційна робота оформлена відповідно до вимог, виклад матеріалу логічний і структурований, зроблено обґрунтовані висновки. Основні результати представлені у вигляді таблиць та схем. Автор опрацював значну джерельну базу, включаючи 60 публікацій та електронних джерел, у тому числі англомовних.

3. Практичні рекомендації, розроблені у роботі, можуть бути застосовані для підвищення ефективності управління інформаційною безпекою в сучасних організаціях.

Недоліки

1. Доцільно було б більш детально розглянути специфіку впровадження запропонованих заходів у різних типах організацій та у реальних цифрових середовищах.

Проте зазначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на високому науково-методичному рівні і заслуговує позитивної оцінки. Здобувач **ІЛЛЯШЕНКО Олексій** заслуговує присвоєння кваліфікації "Магістр з кібербезпеки та захисту інформації за освітньо-професійною програмою Управління інформаційною та кібернетичною безпекою".

Рецензент: _____ ПІБ

_ підпис

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 75 стор., 11 рис., 12 табл., 60 джерел.

Мета роботи полягає в обґрунтуванні, розробленні та удосконаленні заходів з управління інформаційною безпекою організації в умовах цифрової трансформації.

Об'єктом дослідження є процес управління інформаційною безпекою організації.

Предметом дослідження є методи, моделі та інструменти забезпечення ефективного управління інформаційною безпекою в умовах цифрової трансформації.

Методи дослідження. У роботі використано комплекс загальнонаукових і спеціальних методів, зокрема аналіз і синтез, системний та ризик-орієнтований підходи, методи експертного оцінювання, статистичні методи обробки даних, а також методи моніторингу та аналізу подій інформаційної безпеки. Застосування зазначених методів дозволило здійснити комплексну оцінку рівня інформаційної безпеки та обґрунтувати напрями його підвищення.

Короткий зміст роботи. У роботі проаналізовано науково-теоретичні підходи до управління інформаційною безпекою в умовах цифрової трансформації, досліджено основні загрози та вразливості інформаційного середовища організації, а також нормативно-правові вимоги й міжнародні стандарти у сфері управління ризиками. У прикладній частині здійснено оцінювання поточного стану інформаційної безпеки торговельного підприємства, проведено розрахунок можливих фінансових збитків від реалізації загроз та запропоновано комплекс організаційних і технічних заходів, спрямованих на підвищення рівня захисту інформаційних ресурсів. Обґрунтовано доцільність впровадження багаторівневої системи автентифікації, ролевого розмежування доступу, журналювання подій безпеки та підвищення обізнаності персоналу.

Галузь застосування. Результати дослідження можуть бути використані в діяльності підприємств різних форм власності для удосконалення системи управління інформаційною безпекою, зниження ризиків втрати інформаційних активів та підвищення стійкості організацій до сучасних кіберзагроз.

КЛЮЧОВІ СЛОВА: ІНФОРМАЦІЙНА БЕЗПЕКА, УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, ЦИФРОВА ТРАНСФОРМАЦІЯ, ОЦІНЮВАННЯ РИЗИКІВ, АВТЕНТИФІКАЦІЯ, КОНТРОЛЬ ДОСТУПУ.

ABSTRACT

The text part of the qualification work for obtaining a master's degree: 75 pages, 11 figures, 12 tables, 60 sources.

The purpose of the study is to substantiate, develop, and improve measures for managing an organization's information security in the context of digital transformation.

The object of the research is the process of information security management of an organization.

The subject of the research is methods, models and tools for ensuring effective information security management under conditions of digital transformation.

Research methods. The research applies a set of general scientific and specialized methods, including analysis and synthesis, systemic and risk-oriented approaches, expert evaluation methods, statistical data processing, as well as monitoring and analysis of information security events. These methods made it possible to comprehensively assess the level of information security and substantiate directions for its improvement.

Brief content of the research. The paper analyzes scientific and theoretical approaches to information security management in the context of digital transformation, examines key threats and vulnerabilities of the organizational information environment, and reviews regulatory requirements and international risk management standards. The applied part includes an assessment of the current information security level of a trading enterprise, calculation of potential financial losses from threat realization, and development of organizational and technical measures aimed at strengthening information protection. The feasibility of implementing multi-level authentication, role-based access control, security event logging, and staff awareness enhancement is substantiated.

Field of application. The research results can be used by organizations to improve information security management systems, reduce risks related to information asset loss, and increase resilience to modern cyber threats.

KEYWORDS: INFORMATION SECURITY, INFORMATION SECURITY MANAGEMENT, DIGITAL TRANSFORMATION, RISK ASSESSMENT, AUTHENTICATION, ACCESS CONTROL.

ЗМІСТ

ВСТУП

У сучасних умовах стрімкої цифрової трансформації організацій зростає залежність бізнес-процесів від інформаційних технологій, що зумовлює посилення вимог до забезпечення інформаційної безпеки. Дані, інформаційні потоки та цифрові сервіси є не лише важливим ресурсом розвитку, а й потенційним об’єктом зловмисного впливу. Кібератаки, порушення конфіденційності, модифікація або блокування критичної інформації можуть призвести до втрати керованості, завдання репутаційної шкоди та значних матеріальних збитків.

Традиційні засоби захисту, орієнтовані лише на забезпечення периметру безпеки, стають недостатніми, оскільки цифрова екосистема сучасної організації виходить за межі локальної інфраструктури та охоплює партнерські системи, мережеві сервіси, хмарні платформи й персональні пристрої користувачів. Тому управління інформаційною безпекою має здійснюватися як цілісна динамічна система, здатна швидко реагувати на зміни інформаційного середовища та мінливі загрози.

У цьому контексті особливої актуальності набуває дослідження процесів управління інформаційною безпекою в умовах цифрової трансформації організації. Важливим завданням є формування адаптивної моделі управління, що об’єднує технологічні, організаційні й нормативні механізми та дозволяє забезпечити належний рівень керованості, захищеності та стійкості інформаційної інфраструктури.

Мета роботи полягає в обґрунтуванні, розробленні та удосконаленні заходів з управління інформаційною безпекою організації в умовах цифрової трансформації.

Для досягнення поставленої мети необхідно виконати такі *завдання*:

– Розкрити теоретичні засади управління інформаційною безпекою в умовах цифрової трансформації.

– Проаналізувати методи, моделі та інструменти оцінювання стану інформаційної безпеки організації.

– Дослідити поточний рівень захищеності обраної організації та розробити практичні рекомендації щодо вдосконалення управління інформаційною безпекою.

– Оцінити результативність запропонованих заходів і визначити напрями подальшого розвитку системи інформаційної безпеки.

Об'єкт дослідження – процес управління інформаційною безпекою організації.

Предмет дослідження – методи, моделі та інструменти забезпечення ефективного управління інформаційною безпекою в умовах цифрової трансформації.

У роботі застосовано комплекс загальнонаукових і спеціальних *методів*: аналіз, синтез, системний підхід, ризик-орієнтоване моделювання, методи експертного оцінювання, статистичні методи обробки даних, інструменти моніторингу та аналізу інформаційних подій.

Наукова новизна одержаних результатів полягає в удосконаленні підходів до оцінювання рівня інформаційної безпеки організації на основі використання сучасних моделей моніторингу та ризик-орієнтованого управління, що забезпечують підвищення адаптивності системи до нових кіберзагроз і змін цифрової інфраструктури.

Практичне значення роботи полягає у можливості застосування запропонованих рекомендацій та розроблених рішень для підвищення рівня інформаційної безпеки організації, оптимізації механізмів реагування на інциденти та покращення ефективності функціонування системи управління безпекою.

Апробація результатів кваліфікаційної роботи відбулася на Результати дослідження апробовані на конференції "Стратегії кіберстійкості: управління ризиками та безперервність бізнесу" 28 лютого 2024 року.

Структура роботи. Кваліфікаційна робота складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків. Викладена на 75 сторінках основного тексту та містить 12 таблиць і 11 рисунків. Список використаних джерел налічує 60 найменування.

РОЗДІЛ 1
НАУКОВО-ТЕОРЕТИЧНІ ПІДХОДИ ДО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

1.1. Поняття та ключові характеристики управління інформаційною безпекою організації

В умовах цифрової трансформації діяльності організацій інформація набуває статусу одного з ключових управлінських ресурсів, що безпосередньо впливає на стабільність функціонування та конкурентоспроможність підприємства. Зростання обсягів електронних даних, використання інформаційно-комунікаційних технологій і інтеграція бізнес-процесів у цифрове середовище зумовлюють необхідність формування системного підходу до управління інформаційною безпекою. У цьому контексті особливої уваги потребує з'ясування сутності поняття «інформаційна безпека», оскільки його трактування в наукових джерелах є різноплановим і залежить від специфіки організації, характеру інформаційних ресурсів та умов їх використання.

З огляду на зростаючу роль інформаційної безпеки у системі управління організацією, доцільним є дослідження змісту цієї категорії на рівні підприємства. Аналіз наукових праць свідчить, що поняття «інформаційна безпека» не має уніфікованого визначення, що пояснюється багатогранністю інформаційних процесів і різноманітністю підходів до їх захисту. Сутність інформаційної безпеки організації формується під впливом технічних, організаційних, правових та управлінських чинників, а також залежить від структури інформаційної системи та характеру загроз, з якими стикається підприємство.

У наукових джерелах інформаційна безпека розглядається як певний стан захищеності інформаційних ресурсів, інформаційного середовища або системи

управління, що забезпечує безперервність діяльності організації та мінімізацію негативних наслідків від реалізації внутрішніх і зовнішніх загроз. Окремі автори акцентують увагу на технічних аспектах захисту інформації, інші – на організаційно-економічних або управлінських складових, що підкреслює комплексний характер цієї категорії (табл. 1.1).

Таблиця 1.1

Підходи до визначення поняття «інформаційна безпека підприємства»

Автор / джерело	Ключовий акцент визначення
Закон України «Про телекомунікації» [19]	Захищеність інформації в телекомунікаційних мережах від знищення, спотворення, блокування та несанкціонованого доступу
Ю. М. Якименко, В. А. Савченко, С. В. Легомінова [53]	Стан захищеності інформаційного середовища, що забезпечує його стабільне функціонування та розвиток
В. А. Козачок, Г. І. Гайдур, С. О. Гахов [25]	Сукупність подій і впливів, які можуть завдати шкоди інформаційній системі та її користувачам
В. І. Шульга [52]	Здатність інформаційної системи протидіяти внутрішнім і зовнішнім ризикам без порушення її функціонування
В. А. Забродський [14, с.35]	Характеристика стійкості підприємства до внутрішніх і зовнішніх загроз у процесі його розвитку
М. І. Камлик [21, с. 9]	Стан стабільного розвитку суб'єкта господарювання за умови ефективної нейтралізації негативних факторів
Т. Н. Гладченко [6, с.111-113]	Захищеність ключових інтересів підприємства, що досягається через систему комплексних організаційних заходів
С. І. Ніколаюк, Д. Й. Никифорчук [38, с. 15].	Стан захищеності ресурсів і організаційних зв'язків, який забезпечує стабільність і розвиток підприємства
А. І. Могильний, В. М. Безчастний, Ю. О. Винокуров [39, с.9].	Забезпечення умов функціонування підприємства шляхом захисту від дестабілізуючих факторів

Узагальнення наявних підходів дає змогу стверджувати, що інформаційна безпека підприємства є не лише результатом застосування технічних засобів захисту, а й складовою системи управління, спрямованої на збереження цілісності, доступності та конфіденційності інформації в процесі реалізації стратегічних і операційних цілей організації.

У сучасних умовах функціонування підприємств питання захисту інформації набувають особливої актуальності, зокрема в період воєнного стану та посилення

цифрових загроз. Інформаційні ресурси, що формують конкурентні переваги організації, повинні бути надійно захищені від можливих втрат, зокрема несанкціонованого доступу, викрадення або випадкового знищення. Водночас практика діяльності більшості вітчизняних підприємств свідчить про недостатній рівень організації захисту інформації, що пояснюється як обмеженістю фінансових ресурсів, так і недостатньою увагою до питань інформаційної безпеки з боку управлінського персоналу [9, с. 72].

На рівні підприємства інформаційна безпека розглядається як сукупність складових системи управління, у тому числі стратегічного, які забезпечують конфіденційність, цілісність і доступність інформації, а також її автентичність, достовірність і підзвітність у процесі зберігання, обробки та використання інформаційних ресурсів. Такий підхід підкреслює тісний взаємозв'язок інформаційної безпеки з управлінськими процесами та прийняттям стратегічних рішень [3, с. 55].

Система стратегічного управління інформаційною безпекою являє собою комплексний і систематизований підхід до управління та захисту інформаційних активів підприємства. Вона охоплює сукупність процедур, методів і засобів контролю, спрямованих на ідентифікацію, оцінювання та зменшення потенційних інформаційних ризиків, пов'язаних зі зберіганням, обробкою і передаванням даних. Основною метою такої системи є підтримання рівня залишкового ризику в межах, прийнятних для підприємства.

Ключовим завданням управління інформаційною безпекою є забезпечення довгострокового захисту інформаційних ресурсів, що реалізується через дотримання принципів конфіденційності, цілісності та доступності інформації. Конфіденційність передбачає обмеження доступу до даних виключно для авторизованих користувачів, цілісність – гарантування точності та повноти інформації, а доступність – своєчасне отримання необхідних даних

уповноваженими суб'єктами як усередині підприємства, так і за його межами [27, с. 91].

Порушення зазначених властивостей інформації може виникати внаслідок дії різноманітних внутрішніх і зовнішніх загроз. У зв'язку з цим управління інформаційною безпекою передбачає систематичне виявлення потенційних ризиків, оцінювання ймовірності їх реалізації та можливих наслідків, а також розробку і впровадження заходів реагування, спрямованих на мінімізацію ризиків із використанням наявних ресурсів підприємства [60].

Для цього застосовуються засоби контролю доступу, управління версіями, перевірки цілісності даних, технічного обслуговування інформаційних систем, своєчасного оновлення програмного забезпечення, а також організація процесів реагування на інциденти та аварійного відновлення [54].

Окрім цього, до завдань інформаційної безпеки належать забезпечення достовірності інформації, надання їй юридичної значущості, зокрема в системах електронного документообігу, а також організація механізмів, що унеможливлюють несанкціоноване відстеження дій користувачів у межах інформаційної системи підприємства. Важливим аспектом є також створення умов для захисту конфіденційних даних, підтримання цілісності інформаційних ресурсів та своєчасне виявлення і нейтралізація потенційних загроз. Для цього застосовуються сучасні технології криптографії, багаторівневі системи автентифікації, а також розробляються внутрішні регламенти і політики безпеки, які визначають порядок доступу до інформації та відповідальність за її використання. Таким чином, інформаційна безпека розглядається як комплексне явище, що охоплює технічні та організаційні заходи, спрямовані на стабільне функціонування підприємства і захист його інформаційних активів [42, с. 106].

Формування інформаційної безпеки на будь-якому рівні управління ґрунтується на сукупності базових принципів, які виступають вихідними орієнтирами, нормативними вимогами та правилами діяльності. Саме ці принципи

визначають логіку побудови та функціонування системи управління інформаційною безпекою для всіх суб'єктів господарювання, незалежно від специфіки їх діяльності (рис. 1.1).

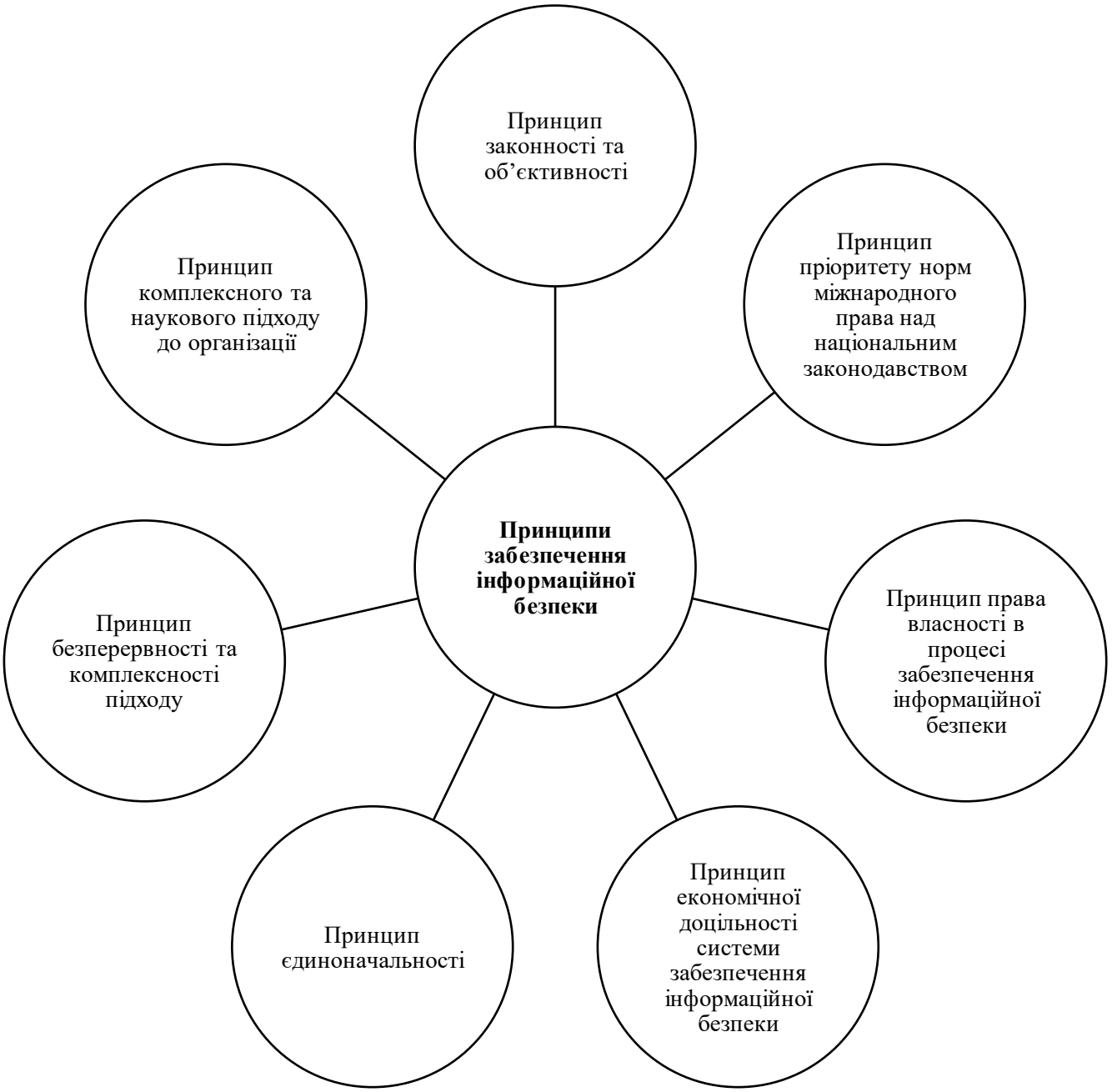

Рис. 1.1. Принципи забезпечення інформаційної безпеки [39]

До основних принципів управління інформаційною безпекою належать:

– принцип законності та об’єктивності, який передбачає здійснення заходів із забезпечення інформаційної безпеки виключно в межах чинного законодавства з урахуванням реального стану загроз та ризиків;

– принцип пріоритету норм міжнародного права над національним законодавством, що забезпечує узгодженість системи інформаційної безпеки організації з міжнародними стандартами та зобов’язаннями;

– принцип права власності в процесі забезпечення інформаційної безпеки, який гарантує захист інформаційних ресурсів відповідно до прав їх законного власника;

– принцип економічної доцільності системи забезпечення інформаційної безпеки, що передбачає співвідношення витрат на захист інформації з можливими збитками від реалізації загроз;

– принцип єдиноначальності, відповідно до якого відповідальність за стан інформаційної безпеки покладається на визначений керівний суб’єкт;

– принцип безперервності та комплексності підходу, що забезпечує постійне функціонування системи інформаційної безпеки та охоплення всіх інформаційних процесів;

– принцип комплексного та наукового підходу до організації, який передбачає використання сучасних наукових методів, технологій і системних рішень у сфері управління інформаційною безпекою.

Інформаційна безпека організації повинна забезпечувати захист інформаційної системи від будь-яких порушень її функціонування, що можуть виникати внаслідок впливу на інформаційні канали, системи сигналізації, керування та віддаленого доступу до баз даних, комутаційного обладнання, системного й прикладного програмного забезпечення. Окрему загрозу становлять неправомірні дії користувачів і персоналу, несанкціонований доступ до інформаційних ресурсів, витік даних, порушення цілісності мережевої

інфраструктури, зниження доступності баз даних, а також руйнування або обходження зовнішніх і вбудованих засобів захисту [42, с. 106].

Процес формування ефективної політики інформаційної безпеки передбачає поетапний підхід. Зокрема, на початковому етапі здійснюється повна ідентифікація та облік інформаційних ресурсів, які потребують захисту. Далі формується перелік потенційних загроз для кожного ресурсу та проводиться оцінка ймовірності їх реалізації. Завершальним етапом є вибір і впровадження адекватних заходів захисту з урахуванням специфіки інформаційних активів підприємства [27, с. 90].

Запровадження системи управління інформаційною безпекою може бути представлене у вигляді узагальненого плану дій, який адаптується залежно від організаційного контексту та рівня цифрової зрілості підприємства. Такий підхід передбачає підтримку з боку вищого керівництва та узгодження заходів інформаційної безпеки з бізнес-цілями організації, створення відповідної управлінської структури, визначення сфери застосування системи інформаційної безпеки, розробку політики високого рівня, а також впровадження програм моніторингу, оцінювання ризиків і реагування на інциденти.

Важливим елементом функціонування системи управління інформаційною безпекою є чітке закріплення ролей і відповідальності між працівниками підприємства, організація навчання та підвищення обізнаності персоналу, а також проведення внутрішнього аудиту й аналізу з боку керівництва. Постійне вдосконалення системи інформаційної безпеки дає змогу адаптувати її до змін у бізнес-середовищі та еволюції інформаційних загроз, а за потреби – підтвердити відповідність міжнародним стандартам шляхом сертифікації, зокрема за ISO/IEC 27001.

Для підприємства ключовими принципами побудови системи інформаційної безпеки є зручність використання, повний контроль за станом захищеності інформації, відкрита архітектура системи, чітке визначення меж доступу,

дотримання принципу найменших привілеїв, забезпечення стабільності функціонування та мінімізація дублювання процедур [3, с. 56–57; 2].

Стандартна система стратегічного управління інформаційною безпекою включає всі базові елементи, притаманні сучасним системам управління. До ключових чинників її ефективності належать наявність сформованої політики інформаційної безпеки, підтримка керівництва всіх рівнів, узгодженість заходів безпеки з корпоративною культурою, системний підхід до управління ризиками, належний рівень обізнаності персоналу, стабільне фінансування заходів захисту, а також ефективне реагування на інциденти та постійне оцінювання результативності системи [38, с. 84–85].

Забезпечення високого рівня інформаційної безпеки потребує комплексного підходу, який охоплює застосування технічних і програмних засобів захисту, організаційних та регламентних заходів, математичних методів захисту інформації, а також морально-етичних інструментів протидії загрозам [34, с. 83].

Водночас навіть сучасні інформаційні технології не гарантують абсолютної захищеності інформаційних систем, що обумовлює необхідність постійного вдосконалення методів захисту та врахування нових способів несанкціонованого доступу [40, с. 82].

Формування системи управління інформаційною безпекою має ґрунтуватися на дотриманні вимог державних і міжнародних нормативно-правових актів та стандартів. Незважаючи на їх універсальний і здебільшого декларативний характер, стандарти створюють основу для уніфікації підходів до управління інформаційною безпекою та дозволяють адаптувати загальні вимоги до специфіки діяльності конкретного підприємства [34, с. 86].

Таким чином, управління інформаційною безпекою організації в умовах цифрової трансформації слід розглядати як складну багаторівневу систему управлінських, організаційних, правових і технічних заходів, спрямованих на захист інформаційних активів та забезпечення безперервності бізнес-процесів.

Ефективність цієї системи визначається не лише рівнем застосування сучасних технологій захисту, а й узгодженістю політики інформаційної безпеки з бізнес-цілями підприємства, підтримкою з боку керівництва, рівнем обізнаності персоналу та здатністю організації адаптуватися до змін зовнішнього середовища й еволюції інформаційних загроз.

1.2. Загрози й вразливості інформаційного середовища в цифровій інфраструктурі підприємства

Активна цифрова трансформація підприємств призводить до того, що інформаційне середовище стає дедалі більш складним і взаємопов'язаним, що суттєво підвищує рівень уразливості інформаційних ресурсів. Використання хмарних сервісів, корпоративних інформаційних систем, віддаленого доступу, електронного документообігу та інтеграція внутрішніх і зовнішніх інформаційних потоків формують нові можливості для розвитку бізнесу, водночас створюючи додаткові ризики для інформаційної безпеки. За таких обставин зростає ймовірність виникнення як технічних, так і організаційних загроз, що можуть негативно впливати на стабільність функціонування підприємства.

Загрози інформаційній безпеці в цифровій інфраструктурі підприємства мають різноманітний характер і походження. Вони можуть виникати як унаслідок зовнішнього впливу, зокрема кібератак, несанкціонованого доступу або шкідливого програмного забезпечення, так і через внутрішні чинники, пов'язані з помилками персоналу, недосконалістю управлінських рішень, недостатнім рівнем контролю або порушенням встановлених регламентів. Особливу небезпеку становлять вразливості інформаційного середовища, які створюють умови для реалізації таких загроз та ускладнюють своєчасне реагування на інциденти.

У разі реалізації зовнішніх загроз зловмисники, як правило, здійснюють цілеспрямований пошук уразливих елементів цифрової інфраструктури

підприємства з метою отримання доступу до критично важливих вузлів, серверів, сховищ даних, робочих станцій персоналу або корпоративної мережі. Такий доступ використовується для копіювання, модифікації або знищення інформації, проведення шпигунських дій, виведення з ладу засобів захисту та порушення стабільності функціонування інформаційних систем.

Найбільш поширені зовнішні загрози інформаційній безпеці та їх потенційний вплив на економічну безпеку підприємства наведено в табл. 1.2.

Таблиця 1.2

Зовнішні загрози інформаційній безпеці підприємства та їх вплив на економічну безпеку [1]

Характеристика внутрішньої загрози інформаційній безпеці	Потенційний вплив на систему економічної безпеки підприємства
Шкідливе програмне забезпечення	Фінансові втрати внаслідок простою систем, витрати на відновлення даних, зниження операційної ефективності
Мережеві атаки та несанкціоновані вторгнення	Порушення цілісності інформації, блокування доступу до інформаційних ресурсів, дестабілізація бізнес-процесів
Фішингові атаки ззовні	Компрометація облікових даних, доступ до фінансової та комерційної інформації, прямі фінансові збитки
Промислове та комерційне шпигунство	Втрата конкурентних переваг, розголошення комерційної та стратегічної інформації
Крадіжка або втрата мобільних пристроїв і обладнання	Несанкціонований доступ до корпоративних даних, витрати на заміну обладнання та відновлення захисту
Цільові кібератаки на інформаційні ресурси підприємства	Значні фінансові та репутаційні втрати, підвищення ризику юридичної відповідальності

Незважаючи на високий рівень небезпеки зовнішніх загроз, практика управління інформаційною безпекою свідчить, що не менш суттєву, а часто й більшу загрозу становлять внутрішні чинники. Внутрішні загрози інформаційній безпеці пов’язані з діяльністю персоналу підприємства та особливостями організації внутрішніх процесів захисту інформації. Їх реалізація може бути наслідком як умисних дій окремих працівників, так і необережності, низького рівня обізнаності або недосконалості організаційних і технічних заходів безпеки (табл. 1.3).

Таблиця 1.3

Внутрішні загрози інформаційній безпеці підприємства та їх вплив на економічну безпеку [1]

Характеристика внутрішньої загрози інформаційній безпеці	Потенційний вплив на систему економічної безпеки підприємства
Несанкціонований витік інформації внаслідок умисних або необережних дій персоналу	Погіршення фінансових показників, зростання збитків, втрата конкурентних позицій
Втрата або розголошення інформації через неналежну організацію процесів захисту даних	Доступ конкурентів до інноваційних розробок, зниження ринкової частки підприємства
Ослаблення рівня захищеності програмного забезпечення та серверної інфраструктури	Зростання операційних витрат, неефективне використання ресурсів
Недостатній рівень фінансування заходів з інформаційної безпеки	Дефіцит інвестиційних ресурсів, обмеження розвитку, підвищення ризику фінансової нестабільності
Повільне оновлення засобів захисту та несвоєчасне реагування на нові типи загроз	Втрата інформаційних ресурсів, підвищення ймовірності витоку даних
Компрометація персональних даних клієнтів	Втрата довіри споживачів, скорочення клієнтської бази, додаткові витрати на відновлення систем захисту

Їх наслідками є фінансові втрати, витік або втрата інформаційних ресурсів, погіршення ділової репутації підприємства та ускладнення взаємовідносин із партнерами й клієнтами. У довгостроковій перспективі реалізація внутрішніх загроз може призводити до зниження рівня довіри до підприємства, посилення контролю з боку регуляторних органів та зростання витрат на відновлення систем захисту. Крім того, такі інциденти здатні негативно впливати на стабільність бізнес-процесів і прийняття управлінських рішень через спотворення або недоступність критично важливої інформації. До внутрішніх загроз належать уразливості програмного забезпечення, випадкові витоки даних з вини персоналу, умисна передача інформації через співробітників, неналежне використання мобільних пристроїв, їх втрата, а також внутрішнє шахрайство.

Узагальнену класифікацію загроз інформаційної безпеки доцільно розглядати за низкою ключових ознак (табл. 1.4).

Таблиця 1.4

Класифікація загроз інформаційної безпеки підприємства [25]

Класифікаційна ознака	Характеристика загроз
За впливом на об'єкт	Збір і передача даних; накопичення даних; обробка даних; форматування інформації; пошук даних; надання доступу до інформації
За метою	Порушення конфіденційності інформації; порушення цілісності інформаційних ресурсів; порушення доступності інформації
За засобами реалізації	Втручання людини; апаратно-технічне втручання; інформаційно-програмне втручання
За наслідками впливу	Загрози, що реалізуються на комп'ютерному обладнанні; у локальних обчислювальних системах; у глобальних транспортних мережах

Реалізація загроз інформаційній безпеці призводить до низки негативних наслідків, що безпосередньо впливають на функціонування підприємства. Зокрема, порушення можуть стосуватися інформаційних ресурсів у системі управління підприємством і проявлятися у вигляді втрати або спотворення даних, обмеження чи повної відмови в доступі до інформації, порушення режиму конфіденційності, несанкціонованого копіювання або викрадення даних, здійснення цілеспрямованих атак, а також помилкової ідентифікації користувачів у інформаційних системах.

Окрім інформаційних ресурсів, наслідки порушення інформаційної безпеки можуть стосуватися й технічної складової цифрової інфраструктури підприємства. До таких наслідків належать відмови та вихід з ладу обладнання, виникнення технічних завад, перегрів апаратних компонентів, вплив електромагнітних наведень, а також негативний вплив зовнішніх факторів, зокрема підвищеної вологості. Подібні порушення не лише знижують рівень захищеності інформаційних систем, а й можуть призвести до зупинки бізнес-процесів та додаткових фінансових втрат підприємства [25].

Загрози інформаційній безпеці цифрової інфраструктури підприємства доцільно класифікувати також за масштабом завданої шкоди. Залежно від розмірів

негативних наслідків виділяють загальні загрози, які спричиняють суттєві порушення функціонування об’єкта безпеки в цілому та призводять до значних матеріальних і репутаційних втрат. Локальні загрози характеризуються впливом на окремі компоненти інформаційної системи або підсистеми цифрової інфраструктури, не порушуючи при цьому загальної працездатності організації. Приватні загрози пов’язані з негативним впливом на окремі властивості елементів інформаційної системи, зокрема на конфіденційність, цілісність або доступність інформації.

Важливим критерієм класифікації є також ступінь впливу загроз на інформаційну систему підприємства. У цьому контексті розрізняють пасивні та активні загрози. Пасивні загрози не передбачають безпосереднього втручання в структуру або зміст інформаційної системи та, як правило, спрямовані на приховане отримання інформації. Активні загрози, навпаки, супроводжуються змінами у структурі, функціонуванні або програмному наповненні інформаційної системи, що може призводити до порушення бізнес-процесів і збоїв у роботі цифрової інфраструктури підприємства.

Забезпечення належного рівня інформаційної безпеки в цифровій інфраструктурі підприємства доцільно розпочинати з ідентифікації суб’єктів інформаційних відносин, діяльність яких пов’язана з використанням інформаційних систем та цифрових ресурсів. Інтереси таких суб’єктів формуються навколо ключових властивостей інформації, зокрема доступності, цілісності та конфіденційності. Доступність передбачає можливість отримання необхідної інформаційної послуги у визначений термін, цілісність характеризує збереження актуальності, повноти та захищеності інформації від несанкціонованих змін або знищення, а конфіденційність полягає у запобіганні неправомірному доступу до інформаційних ресурсів.

З урахуванням зазначених характеристик інформаційну безпеку в межах цифрової інфраструктури підприємства доцільно розглядати як такий стан

інформаційного середовища, за якого унеможливлюється завдання шкоди властивостям об’єктів безпеки, що визначаються інформацією, інформаційними потоками та засобами їх обробки. Порушення хоча б однієї з базових властивостей інформації створює передумови для виникнення загроз та реалізації вразливостей у цифровому середовищі підприємства.

До основних об’єктів інформаційної безпеки в організації належать, насамперед, інформаційні ресурси, що містять відомості з обмеженим доступом, зокрема комерційну та конфіденційну інформацію, представлену у вигляді інформаційних масивів, баз даних та електронних документів. Вразливість таких ресурсів безпосередньо пов’язана з рівнем захищеності цифрових каналів передачі даних і внутрішніх систем зберігання інформації.

Окрім інформаційних ресурсів, важливим об’єктом захисту виступають засоби та системи інформатизації підприємства. До них належать обчислювальна й організаційна техніка, локальні та глобальні мережі, системне і прикладне програмне забезпечення, автоматизовані системи управління, засоби зв’язку та передачі даних, а також технічні засоби збору, реєстрації, обробки та відображення інформації. Саме ці елементи цифрової інфраструктури є потенційними точками виникнення вразливостей, які можуть бути використані для реалізації загроз інформаційній безпеці підприємства.

Вразливості виступають слабкими елементами цифрової інфраструктури, які створюють передумови для негативного впливу на інформаційні ресурси та інформаційні потоки підприємства. Загроза набуває практичної форми лише за умови взаємодії з конкретною вразливістю, що призводить до порушення функціонування інформаційних систем на відповідному об’єкті-носії.

Основні вразливості інформаційного середовища підприємства формуються під впливом низки чинників. До них належать недосконалість програмного забезпечення та апаратної платформи, структурні особливості автоматизованих систем у межах інформаційних потоків, неповноцінність окремих процесів

функціонування інформаційних систем, неточність або застарілість протоколів обміну даними та інтерфейсів, а також складні умови експлуатації й зберігання інформації. У сукупності ці фактори знижують рівень захищеності цифрової інфраструктури та підвищують ймовірність реалізації інформаційних загроз.

За характером походження вразливості систем інформаційної безпеки поділяють на об'єктивні, випадкові та суб'єктивні. Об'єктивні вразливості зумовлені технічними та технологічними обмеженнями інформаційних систем. Випадкові виникають унаслідок непередбачуваних обставин або помилок у процесі експлуатації цифрової інфраструктури. Суб'єктивні вразливості пов'язані з людським фактором, зокрема недостатньою кваліфікацією персоналу або недотриманням встановлених вимог інформаційної безпеки.

Усунення або навіть часткове зменшення рівня вразливостей дає змогу суттєво знизити ймовірність реалізації повномасштабних загроз інформаційній безпеці, спрямованих на системи зберігання, обробки та передавання інформації. З урахуванням цього класифікація загроз інформаційній безпеці доцільно здійснюється за характером загрози, способом і масштабом впливу, джерелом виникнення та об'єктом спрямування.

В умовах цифровізації бізнес-процесів особливого значення набуває взаємозв'язок між загрозами та вразливостями інформаційного середовища підприємства. Навіть за наявності сучасних технічних засобів захисту недостатня увага до управлінських, організаційних або кадрових аспектів інформаційної безпеки може призвести до виникнення критичних вразливостей. Це зумовлює необхідність комплексного підходу до аналізу цифрової інфраструктури, що передбачає одночасне врахування технічних, людських і процесних чинників.

Важливою особливістю сучасних загроз інформаційній безпеці є їх динамічний характер і постійна еволюція. З розвитком інформаційних технологій з'являються нові способи несанкціонованого доступу, шкідливого впливу на інформаційні ресурси та маніпулювання даними. У зв'язку з цим вразливості, які

раніше не мали суттєвого значення, можуть швидко перетворюватися на критичні точки ризику для підприємства. Це потребує регулярного перегляду підходів до ідентифікації загроз, оновлення засобів захисту та адаптації системи управління інформаційною безпекою до змін зовнішнього середовища.

Ефективне управління загрозами й вразливостями інформаційного середовища можливе лише за умови інтеграції заходів інформаційної безпеки у загальну систему управління підприємством. Така інтеграція дозволяє не лише мінімізувати ризики втрати або компрометації інформації, а й забезпечити безперервність бізнес-процесів, зберегти довіру клієнтів і партнерів та підтримати стратегічну стійкість організації в умовах цифрової трансформації.

Таким чином, загрози й вразливості інформаційного середовища є ключовими чинниками, що визначають рівень інформаційної безпеки цифрової інфраструктури підприємства. Їх систематичний аналіз, своєчасне виявлення та комплексне управління створюють основу для побудови ефективної системи захисту інформаційних ресурсів.

1.3. Нормативні вимоги та міжнародні стандарти управління ризиками інформаційної безпеки

Цифрова трансформація підприємств висуває нові вимоги до організації інформаційної безпеки, адже ефективне управління ризиками у цій сфері неможливе без чіткого дотримання нормативно-правових положень та застосування міжнародних стандартів. Саме нормативна база і стандартизація створюють методологічне підґрунтя для ідентифікації, оцінювання та мінімізації інформаційних ризиків, забезпечуючи системний і уніфікований підхід до захисту даних та інформаційних ресурсів.

На нормативно-правовому рівні поняття інформаційної безпеки закріплено в Концепції інформаційної безпеки України, відповідно до якої вона визначається як

стан захищеності життєво важливих інтересів людини, суспільства та держави, за якого запобігається завдання шкоди внаслідок неповноти, несвоєчасності або недостовірності інформації, порушення її цілісності та доступності, несанкціонованого обігу даних з обмеженим доступом, а також негативного інформаційно-психологічного впливу та зловживання інформаційними технологіями [26].

Національне нормативно-правове забезпечення інформаційної безпеки в Україні формується сукупністю законодавчих актів, які визначають правові засади функціонування інформаційних відносин та встановлюють вимоги до захисту інформації в діяльності суб'єктів господарювання. Базовим документом у цій сфері є Закон України «Про інформацію», який регламентує загальні принципи створення, використання, поширення та захисту інформації. У межах цього закону закріплено основні поняття, визначено права суб'єктів на доступ до інформації, а також класифіковано інформацію за режимами доступу, зокрема на відкриту та інформацію з обмеженим доступом, до якої належать конфіденційна, таємна та службова інформація [17].

Ключову роль у забезпеченні інформаційної безпеки в цифровому середовищі відіграє Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». Цей нормативний акт визначає порядок організації захисту інформації, що обробляється та передається в електронних системах, встановлює обов'язки власників інформаційних систем і операторів, регламентує вимоги до сертифікації засобів захисту інформації, а також передбачає заходи реагування на інциденти інформаційної безпеки. Його положення є основою для побудови систем захисту інформації в межах корпоративних інформаційних ресурсів підприємств [15].

Важливим елементом нормативного регулювання є Закон України «Про захист персональних даних», який визначає правові засади обробки, зберігання та передавання персональної інформації фізичних осіб. Для підприємств, що здійснюють діяльність із використанням клієнтських або кадрових баз даних,

дотримання вимог цього закону є обов'язковим. Зокрема, закон встановлює необхідність отримання згоди суб'єктів персональних даних на їх обробку, визначає вимоги до забезпечення безпеки баз даних, а також зобов'язує призначати відповідальних осіб за організацію захисту персональної інформації [16].

Положення щодо захисту інформації містяться також у Цивільному та Господарському кодексах України, де закріплено правовий режим комерційної таємниці та визначено відповідальність за її неправомірне розголошення. Згідно з цими актами, інформація, що має комерційну цінність і не є загальнодоступною, може бути віднесена до комерційної таємниці за умови вжиття підприємством відповідних заходів щодо збереження її конфіденційності [7; 50].

Кримінальний кодекс України доповнює систему правового захисту інформації, встановлюючи кримінальну відповідальність за незаконне втручання в роботу комп'ютерних систем і мереж, несанкціонований доступ до інформації, створення та розповсюдження шкідливого програмного забезпечення, а також порушення законодавства у сфері захисту персональних даних. Таким чином, національне законодавство створює комплексну правову основу для протидії загрозам інформаційній безпеці підприємств [30].

Разом із тим, в умовах глобалізації цифрових процесів і розширення міжнародної співпраці національних норм часто виявляється недостатньо для забезпечення належного рівня захисту інформаційних активів. Саме тому значна кількість підприємств орієнтується не лише на вимоги національного законодавства, а й на міжнародні стандарти управління інформаційною безпекою, які визначають уніфіковані підходи до ідентифікації, оцінювання та управління ризиками в інформаційному середовищі.

З метою обґрунтованого вибору підходів до управління інформаційною безпекою доцільно порівняти найбільш поширені на практиці стандарти та нормативні системи (рис. 1.2).

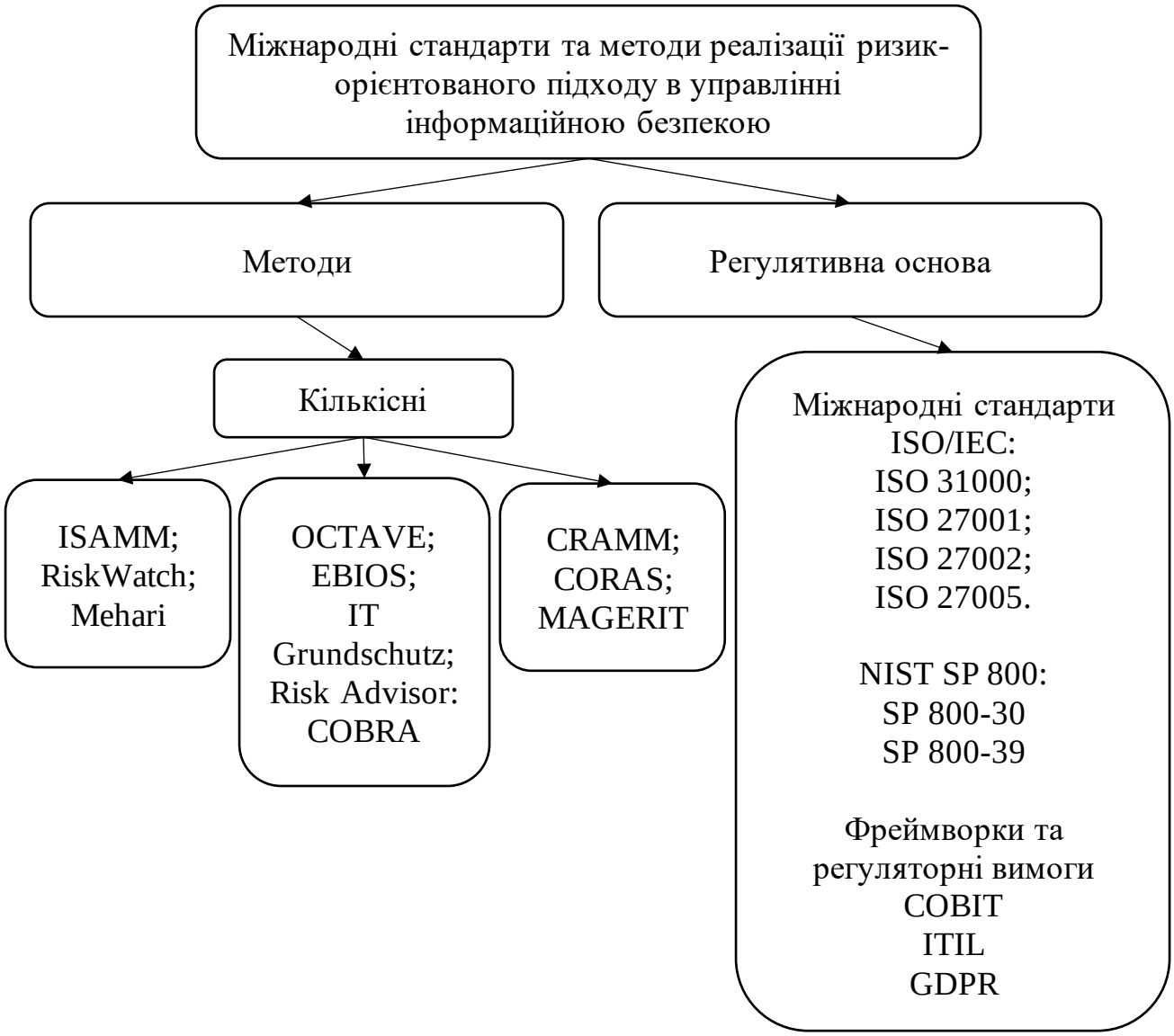

Рис. 1.2. Міжнародні стандарти та методи реалізації ризик-орієнтованого підходу в управлінні інформаційною безпекою [20]

Представлена схема відображає взаємозв'язок між методами оцінювання ризиків, міжнародними стандартами та управлінськими фреймворками, які у сукупності забезпечують реалізацію ризик-орієнтованого підходу до управління інформаційною безпекою підприємства.

Важливим нормативним орієнтиром у сфері управління ризиками, у тому числі ризиками інформаційної безпеки, є міжнародний стандарт ISO 31000:2018,

який визначає загальні принципи та керівні настанови з менеджменту ризиків для організацій будь-якого типу та сфери діяльності. Оновлена редакція цього стандарту акцентує увагу на інтеграції управління ризиками в усі управлінські процеси підприємства, посиленні ролі вищого керівництва та формуванні ризик-орієнтованого мислення на всіх рівнях управління. Стандарт визначає базові принципи управління ризиками, зокрема створення та захист цінностей, інтегрованість у діяльність організації, системність, динамічність, урахування людського фактору та безперервне вдосконалення, а також встановлює рамкову структуру і послідовний процес управління ризиками. Його застосування спрямоване на підвищення обґрунтованості управлінських рішень в умовах невизначеності та зростання ймовірності досягнення стратегічних цілей підприємства [55].

У контексті безпосереднього управління інформаційною безпекою ключове значення має стандарт ISO/IEC 27001:2022, який встановлює вимоги до створення, впровадження, підтримання та постійного вдосконалення системи управління інформаційною безпекою організації. Центральним елементом цього стандарту є управління ризиками інформаційної безпеки, яке передбачає систематичне виявлення, аналіз, оцінювання та обробку ризиків у межах планування та функціонування системи управління інформаційною безпекою (далі – СУІБ). Зокрема, положення пункту 6.1 ISO/IEC 27001:2022 регламентують необхідність формування плану обробки ризиків інформаційної безпеки з урахуванням прийнятного рівня ризику та бізнес-контексту підприємства. Важливо, що оновлена редакція стандарту узгоджена з принципами ISO 31000:2018 та методологічними рекомендаціями ISO/IEC 27005:2022, що забезпечує цілісність ризик-орієнтованого підходу. Стандарт ISO/IEC 27001 є нормативним і передбачає можливість сертифікації організацій, що підтверджує зрілість процесів управління інформаційною безпекою. В Україні чинним залишається ДСТУ ISO/IEC 27001:2015, ідентичний попередній редакції ISO/IEC 27001:2013, водночас нова

версія ISO/IEC 27001:2022 перебуває на етапі впровадження як національний стандарт [55; 56; 57; 58].

Додатковим елементом системи стандартів серії ISO/IEC 27000 є стандарт ISO/IEC 27002:2022, який має рекомендаційний характер і містить систематизований перелік передових практик та заходів безпеки для захисту інформаційних активів. Хоча цей стандарт безпосередньо не регламентує процедури оцінювання ризиків, він відіграє ключову роль у процесі їх обробки, оскільки слугує методичною основою для вибору та впровадження відповідних контролів на основі результатів ризик-аналізу. Оновлена редакція ISO/IEC 27002:2022 передбачає перегрупування контролів і впровадження атрибутів безпеки, що полегшує їх зіставлення з конкретними ризиками та сучасними цифровими загрозами. В українській практиці наразі застосовується ДСТУ ISO/IEC 27002:2015, ідентичний попередній міжнародній редакції, при цьому очікується адаптація оновленої версії стандарту на державному рівні. У сукупності ISO/IEC 27001 та ISO/IEC 27002 формують базис ризик-орієнтованого управління інформаційною безпекою, де перший визначає вимоги до процесу, а другий – практичні механізми його реалізації.

Окреме місце в системі міжнародних стандартів посідає ISO/IEC 27005:2022, який спеціалізується на управлінні ризиками інформаційної безпеки та надає розширені керівні вказівки щодо ідентифікації, аналізу, оцінювання та обробки ризиків. Цей стандарт методологічно узгоджений з ISO/IEC 27001:2022 і загальними принципами ISO 31000:2018, що забезпечує комплексний підхід до ризик-менеджменту. Суттєвими нововведеннями редакції 2022 року є впровадження концепції сценаріїв ризику, а також розмежування підходів до ідентифікації ризиків на основі активів і на основі подій. Такий підхід дає змогу підприємствам швидко адаптувати процес оцінювання ризиків відповідно до особливостей цифрової інфраструктури та характеру потенційних загроз. ISO/IEC 27005 не є сертифікаційним стандартом, однак широко використовується як

методологічна основа для підвищення ефективності управління ризиками інформаційної безпеки. В Україні йому відповідає ДСТУ ISO/IEC 27005:2023 «Настанова з керування ризиками інформаційної безпеки», що підтверджує актуальність і послідовність впровадження міжнародних підходів у національну практику [15; 58].

Також у міжнародній практиці управління ризиками інформаційної безпеки широко застосовуються рекомендації та нормативні документи сімейства NIST SP 800, розроблені Національним інститутом стандартів і технологій США. Зокрема, стандарт NIST SP 800-53 містить систематизований перелік заходів контролю безпеки для інформаційних систем і організацій, що охоплюють технічні, адміністративні та операційні аспекти захисту інформації. Його особливістю є чітка орієнтація на ризик-орієнтований підхід та можливість масштабування заходів безпеки залежно від рівня критичності інформаційних ресурсів і характеру загроз.

Поряд із цим, у межах сімейства NIST SP 800 застосовуються також інші методичні документи, зокрема NIST SP 800-30, який присвячений процесу оцінювання інформаційних ризиків, та NIST SP 800-39, що визначає інтегрований підхід до управління ризиками на рівні організації, бізнес-процесів і інформаційних систем. Важливим доповненням є Рамкова модель кібербезпеки NIST (NIST Cybersecurity Framework), яка надає універсальну структуру для ідентифікації, захисту, виявлення, реагування та відновлення після кіберінцидентів і активно використовується як у державному, так і в корпоративному секторі [59].

Окрім стандартів серії ISO та рекомендацій NIST, у практиці управління інформаційною безпекою широко застосовуються міжнародні фреймворки та регуляторні акти, які доповнюють ризик-орієнтований підхід організаційними й управлінськими інструментами. До таких належать COBIT, ITIL та GDPR, що орієнтовані на інтеграцію інформаційної безпеки в загальну систему корпоративного управління, управління IT-послугами та захист персональних даних відповідно.

Фреймворк COBIT використовується як інструмент управління та контролю інформаційних технологій на рівні підприємства і забезпечує узгодження процесів інформаційної безпеки з бізнес-цілями, управлінням ризиками та відповідальністю керівництва. Він не є стандартом інформаційної безпеки у вузькому розумінні, проте створює управлінське підґрунтя для впровадження та підтримки системи управління інформаційною безпекою.

Фреймворк ITIL доповнює управління інформаційною безпекою через процеси управління IT-послугами, зокрема інцидентами, проблемами, змінами та рівнем обслуговування. Його застосування сприяє зниженню операційних ризиків, підвищенню стабільності IT-інфраструктури та забезпеченню доступності й надійності інформаційних сервісів, що є важливими складовими інформаційної безпеки.

Регламент GDPR має нормативний характер і встановлює обов'язкові вимоги щодо захисту персональних даних, що безпосередньо впливає на побудову процесів інформаційної безпеки підприємств, які працюють із даними громадян Європейського Союзу. Його дотримання стимулює впровадження високих стандартів конфіденційності, прозорості та управління ризиками, пов'язаними з обробкою персональної інформації.

Для узагальнення підходів до управління ризиками інформаційної безпеки доцільно здійснити порівняльний аналіз ключових міжнародних стандартів, які найчастіше застосовуються у цій сфері, а саме ISO/IEC 27005, ISO 31000 та ISO/IEC 27001. Таке зіставлення дозволяє чітко окреслити їх призначення, нормативний статус, сферу застосування та логіку взаємодії у межах побудови системи управління інформаційною безпекою підприємства (Додаток А).

За результатами порівняльного аналізу можна зробити висновок, що ISO/IEC 27001 формує нормативну основу системи управління інформаційною безпекою, ISO/IEC 27005 забезпечує методичну підтримку процесів оцінювання та обробки ризиків ІБ, а ISO 31000 задає універсальні принципи управління ризиками, які

інтегруються в загальну систему менеджменту підприємства. Сукупне використання зазначених стандартів дозволяє вибудувати цілісний, узгоджений і ризик-орієнтований підхід до управління інформаційною безпекою в умовах цифрової трансформації.

В Україні поряд із міжнародними підходами до управління інформаційною безпекою діє національна система нормативного регулювання захисту інформації, ключовим елементом якої є Комплексна система захисту інформації (КСЗІ). Вона використовується переважно для забезпечення захисту даних в інформаційно-телекомунікаційних системах, що обробляють інформацію з обмеженим доступом, та визначає порядок організації, впровадження і контролю заходів інформаційної безпеки відповідно до вимог національного законодавства. Напрактиці управління ризиками інформаційної безпеки відповідні підходи також знаходять відображення у нормативно-правових актах. Зокрема, Закон України «Про основні засади забезпечення кібербезпеки України» визначає управління ризиками як один із базових принципів захисту критичної інформаційної інфраструктури [20].

Водночас, попри наявність національних регуляторних вимог, базисом для побудови практичних процесів управління інформаційною безпекою на підприємствах здебільшого залишаються міжнародні стандарти серій ISO/IEC 27000 та ISO 31000, які забезпечують уніфіковану термінологію, узгоджені підходи до оцінювання та обробки ризиків, а також можливість інтеграції управління інформаційною безпекою в загальну систему управління організацією.

Таким чином, нормативно-правові вимоги та міжнародні стандарти відіграють ключову роль у формуванні ефективної системи управління ризиками інформаційної безпеки підприємства в умовах цифрової трансформації. Національне законодавство України забезпечує базові правові рамки захисту інформації, визначає відповідальність за порушення вимог інформаційної безпеки та регламентує обробку інформації з обмеженим доступом, зокрема персональних даних і комерційної таємниці. Водночас ці норми мають переважно регуляторний

характер і потребують доповнення сучасними управлінськими та методологічними інструментами.

Міжнародні стандарти, насамперед серій ISO/IEC 27000 та ISO 31000, формують універсальну методологічну основу для впровадження ризик-орієнтованого підходу до управління інформаційною безпекою. Вони забезпечують системність, узгодженість і гнучкість процесів ідентифікації, оцінювання та обробки ризиків, дозволяють інтегрувати управління інформаційною безпекою в загальну систему менеджменту підприємства та адаптувати заходи захисту до змін цифрового середовища і характеру загроз. Особливу цінність у цьому контексті становить взаємодоповнюваність стандартів ISO/IEC 27001, ISO/IEC 27005 та ISO 31000, що дає змогу поєднати нормативні вимоги, практичні механізми реалізації та універсальні принципи ризик-менеджменту.

Висновки до розділу 1

У першому розділі розкрито науково-теоретичні підходи до управління інформаційною безпекою організації в умовах цифрової трансформації та обґрунтовано її роль як одного з ключових елементів сучасного менеджменту підприємства. Уточнено зміст поняття «інформаційна безпека» на рівні організації, узагальнено наявні підходи до його трактування та підкреслено комплексний характер цієї категорії, що формується під впливом технічних, організаційних, правових і управлінських чинників. Доведено, що інформаційна безпека не зводиться лише до застосування технічних засобів, а передбачає системну управлінську роботу, спрямовану на підтримання конфіденційності, цілісності та доступності інформації, захист інформаційних активів і забезпечення безперервності бізнес-процесів.

Окрему увагу приділено загрозам і вразливостям інформаційного середовища в цифровій інфраструктурі підприємства. Систематизовано ключові внутрішні й

зовнішні загрози, визначено їх можливі наслідки для функціонування організації та показано, що реальна реалізація загроз відбувається через наявні вразливості – слабкі місця технологій, процесів і людського фактору. Обґрунтовано доцільність класифікації загроз за масштабом шкоди та характером впливу на інформаційні системи, а також підкреслено динамічність сучасного цифрового середовища, у якому ризики швидко еволюціонують і потребують регулярного перегляду підходів до захисту.

Також розглянуто нормативні вимоги та стандартизовані підходи, що визначають правила і методологію управління ризиками інформаційної безпеки. Показано, що національна правова база формує обов’язкові рамки захисту інформації, регламентує обробку персональних даних і комерційної таємниці та встановлює відповідальність за порушення у цифровій сфері. Водночас міжнародні стандарти й рекомендації забезпечують уніфіковані, практично орієнтовані підходи до організації системи управління інформаційною безпекою та ризиками, дозволяють інтегрувати заходи безпеки в загальну систему управління підприємством і підвищувати керованість процесів захисту в умовах цифрових загроз.

РОЗДІЛ 2
МЕТОДИ ТА МОДЕЛІ ОЦІНЮВАННЯ СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

2.1. Методичні підходи до діагностики ризиків та якості системи захисту інформації

Перехід до практичних аспектів управління інформаційною безпекою зумовлює необхідність поглибленого аналізу методів і підходів, що дозволяють об’єктивно оцінити рівень захищеності інформаційних ресурсів організації та ефективність функціонування системи захисту інформації. В умовах цифрової трансформації підприємств зростає не лише кількість інформаційних активів, а й складність загроз, що унеможливлює використання фрагментарних або інтуїтивних рішень у сфері безпеки.

Оцінювання стану інформаційної безпеки виступає основою для прийняття управлінських рішень щодо вдосконалення заходів захисту, оптимального розподілу ресурсів та визначення пріоритетних напрямів реагування на загрози. Без системної діагностики неможливо визначити реальний рівень ризиків, виявити критичні вразливості інформаційної інфраструктури чи оцінити відповідність наявної системи захисту вимогам нормативних актів і міжнародних стандартів.

Ідентифікація ризиків передбачає виявлення інформаційних активів, потенційних загроз і вразливостей, а також опис можливих сценаріїв інцидентів і їх наслідків для організації. Результатом є реєстр ризиків, у якому фіксується зв’язок «актив – загроза – вразливість – наслідки», що формує основу для подальшого аналізу та пріоритезації.

Аналіз ризиків передбачає поглиблене дослідження ідентифікованих ризиків з метою розуміння їх природи та визначення рівня ризику. У межах цього етапу оцінюється імовірність виникнення небажаних подій і масштаби їх можливих

наслідків для організації. При цьому враховуються джерела і причини ризиків, можливі сценарії інцидентів, а також ефективність наявних заходів контролю, здатних зменшити ймовірність або вплив реалізації загроз.

У практиці оцінювання стану інформаційної безпеки використовуються різні підходи до аналізу ризиків, які відрізняються ступенем формалізації та глибиною кількісної оцінки. Якісний підхід ґрунтується на застосуванні описових шкал і експертних суджень, коли ймовірність реалізації загрози та рівень її впливу визначаються за категоріями «низький», «середній» або «високий». Такий підхід є доцільним за умов обмеженої статистичної інформації або на початкових етапах побудови СУІБ, оскільки дозволяє швидко визначити критичні ризики без складних розрахунків. Кількісний підхід орієнтований на отримання числових значень рівня ризику та базується на використанні ймовірнісних оцінок і фінансових показників, де наслідки інцидентів відображаються у грошовому еквіваленті очікуваних втрат. Водночас такий підхід потребує достовірних даних і відповідних аналітичних ресурсів, що не завжди є можливим для підприємств із обмеженою історією інцидентів. Напівкількісний підхід поєднує елементи якісного та кількісного аналізу й є найбільш поширеним у прикладних дослідженнях, оскільки дозволяє ранжувати ризики на основі умовних шкал і уніфікованих критеріїв без повної кількісної формалізації всіх параметрів.

Незалежно від обраного підходу, загальна логіка аналізу ризику ґрунтується на поєднанні двох базових складових – ймовірності реалізації загрози та рівня її наслідків. У спрощеному вигляді рівень ризику може бути представлений як функція зазначених параметрів:

$$R = Likelihood \times Impact, \tag{2.1}$$

де: Likelihood – оцінка ймовірності реалізації ризик-сценарію, Impact – оцінка наслідків (впливу) для організації.

Практичним інструментом узагальнення результатів такого аналізу є матриця ризику, яка дозволяє наочно зіставляти ризики шляхом розміщення їх у

двовимірному просторі координат «ймовірність – вплив». Кожна комірка матриці відповідає певному рівню ризику, що використовується для пріоритезації реагування: низькі ризики відносяться до «зеленої» зони, середні – до «жовтої», високі – до «червоної», що спрощує ухвалення управлінських рішень щодо черговості обробки ризиків (рис. 2.1).

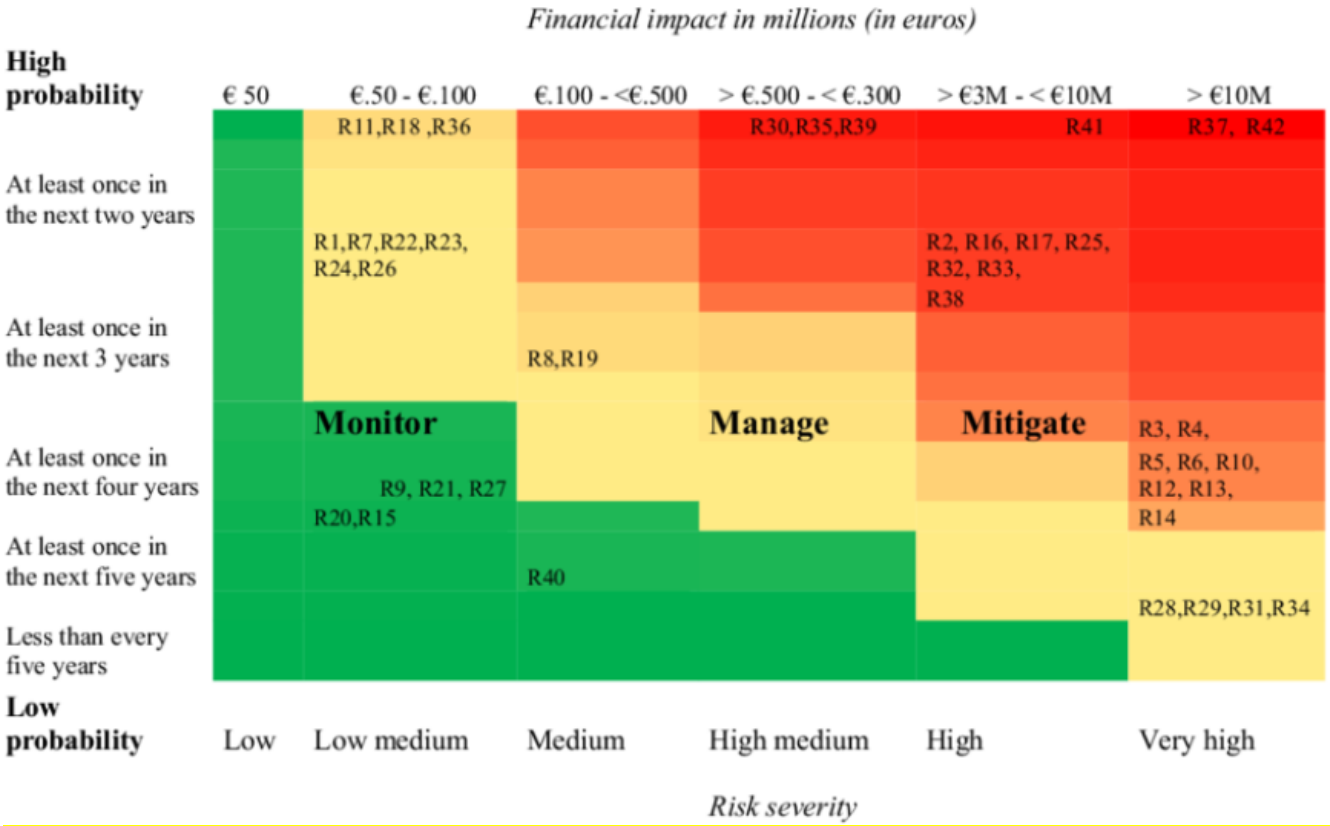

Рис. 2.1. Матриця ризиків, що відображає взаємозв'язок між імовірністю реалізації загрози та рівнем її впливу [55]

Для підвищення точності й об'єктивності аналізу організація має заздалегідь встановити єдині критерії оцінювання ймовірності та наслідків. Межі ймовірності можуть задаватися кількісно (наприклад, значення менше 5 % – низький рівень, 5–20 % – середній, понад 20 % – високий) або через якісні часові орієнтири («раз на кілька років», «кілька разів на рік», «майже неминуче»), що є доцільним за нестачі статистики. Паралельно визначаються критерії наслідків, які відображають можливий вплив інцидентів на діяльність організації: від мінімальних фінансових

втрат і локальних порушень окремих процесів до істотних економічних збитків, зупинки критичних бізнес-процесів або втрати довіри з боку клієнтів і партнерів. Джерелами для формування таких критеріїв виступають вимоги міжнародних стандартів, галузеві рекомендації, а також внутрішній досвід підприємства, зокрема рівень ризик-апетиту керівництва та результати аналізу попередніх інцидентів.

Порівняння та інтерпретація отриманих рівнів ризику передбачає визначення того, які ризики є прийнятними, а які потребують обов'язкової обробки. Для цього ризики впорядковуються за значущістю, що дозволяє зосередити управлінську увагу на загрозах, які перевищують допустимі межі, та формує основу для вибору управлінських дій (табл. 2.1).

Таблиця 2.1

Критерії прийнятності ризиків інформаційної безпеки [58]

Рівень ризику	Статус прийнятності	Рекомендовані управлінські дії
Низький (зелена зона)	Прийнятний	Рівень ризику перебуває в межах допустимого. Застосування додаткових заходів не є обов'язковим; підтримуються наявні механізми контролю.
Середній (жовта зона)	Терпимий за умови контролю	Потребує постійного моніторингу та, за можливості, поетапного посилення заходів захисту у середньо- та довгостроковій перспективі.
Високий (червона зона)	Неприйнятний	Вимагає невідкладного впровадження заходів зниження ризику. За неможливості ефективної обробки доцільно розглянути припинення або зміну діяльності, пов'язаної з таким ризиком.

Як результат, на етапі аналізу формується ранжований перелік ризиків, що дає змогу цілеспрямовано розподіляти ресурси та зосереджувати організаційні й технічні заходи на найбільш критичних загрозах. Водночас оцінювання ризиків не повинно зводитися лише до формальних числових показників, оскільки окремі ризики можуть мати помірний розрахунковий рівень за фінансовими критеріями, але суттєві репутаційні або стратегічні наслідки, що потребує додаткового експертного перегляду з урахуванням контексту діяльності та очікувань зацікавлених сторін.

Оцінювання ризиків є завершальним етапом процесу оцінки, на якому результати аналізу узагальнюються у вигляді пріоритетного переліку ризиків із визначенням черговості реагування. Пріоритезація здійснюється з урахуванням рівня ризику, а також стратегічних цілей організації, вимог законодавства і регуляторів та інтересів ключових зацікавлених сторін. На основі цього формується перелік ризиків, для яких у першу чергу мають бути визначені й реалізовані відповідні заходи реагування.

Для формалізації оцінювання застосовується напівкількісний підхід, у межах якого рівень ризику визначається як добуток очікуваних втрат від одноразового інциденту та показника середньорічної частоти реалізації загрози.

Аналітично рівень ризику може бути поданий у вигляді залежності:

$$R = L * P, \tag{2.2}$$

де R – рівень ризику, пов’язаного з реалізацією загрози, спрямованої на вразливість місця зберігання або обробки інформаційного активу;

L – величина фінансових втрат, що виникають унаслідок одноразової реалізації відповідної загрози;

P – показник середньорічної частоти реалізації загрози, який приймає дискретні значення залежно від інтенсивності та повторюваності інцидентів $(P \in \{1, 2, 3\})$ [31].

Зазначений підхід дозволяє кількісно зіставляти ризики між собою, визначати найбільш критичні з них та формувати пріоритети щодо впровадження заходів захисту. Критерії віднесення загроз до відповідного рівня середньорічної частоти їх реалізації визначаються з урахуванням мотивації та можливостей джерела загрози, рівня поширеності інформації про наявні вразливості, а також ефективності чинних засобів захисту і наявності статистичних даних щодо виникнення інцидентів. Застосування таких критеріїв дозволяє уніфікувати підхід до оцінювання ймовірності реалізації загроз, забезпечити порівнюваність отриманих результатів та

підвищити обґрунтованість висновків у процесі діагностики ризиків інформаційної безпеки підприємства (табл. 2.2).

Таблиця 2.2

Рівні середньорічної частоти реалізації загрози [31]

Рівень частоти реалізації загрози	Характеристика
Низький	Ймовірність реалізації загрози є незначною. Джерело загрози має слабку мотивацію або обмежені можливості. Наявні засоби захисту істотно ускладнюють реалізацію загрози. Відсутні статистичні дані чи інша інформація, що свідчить про можливість виникнення інциденту.
Середній	Джерело загрози є мотивованим, існують об'єктивні передумови для реалізації загрози. Відомості про наявну вразливість є загальнодоступними, однак для здійснення атаки потрібні спеціальні технічні знання або засоби.
Високий	Інформація про вразливість широко розповсюджена та доступна для потенційних порушників. Наявні статистичні дані або інші підтвердження, що свідчать про високу ймовірність реалізації загрози. Існують суттєві мотиви або причини для здійснення атаки на інформаційні активи підприємства.

Такий поділ дає змогу уніфікувати підхід до визначення ймовірності реалізації загроз і використовується для подальшого розрахунку рівня ризику та пріоритезації заходів інформаційної безпеки.

Величина фінансових збитків від одноразової реалізації загрози, спрямованої на вразливість місця зберігання інформаційного активу, визначається з урахуванням вартості відповідного активу та рівня наслідків порушення його основних властивостей. Для кількісної оцінки фінансових втрат використовується формула (2.3):

$$L = \sum(Cass * LR), \tag{2.3}$$

де:

L – фінансовий збиток від одноразової реалізації загрози, спрямованої на вразливість місця зберігання активу;

Cass – вартість інформаційного активу;

LR – рівень наслідків порушення конфіденційності, цілісності та доступності активу ($LR \in \{0 \dots 1\}$) [31].

Вартість інформаційного активу Cass виражається у грошових одиницях і залежить від його типу, ролі у діяльності підприємства та значущості для бізнес-процесів. При її визначенні доцільно враховувати такі складові: витрати на утримання активу, вартість його заміни або відновлення, фінансові втрати у разі недоступності активу, можливу шкоду діловій репутації організації, зниження річного доходу, втрату конкурентних переваг, зменшення ефективності бізнес-процесів, а також штрафи й санкції за порушення законодавчих норм і вимог.

Рівень наслідків порушення інформаційної безпеки активу визначається як максимальне значення шкоди, заподіяної порушенням однієї з базових властивостей інформації, та обчислюється за формулою (2.4):

$$LR = max\{ Cc, Ci, Ca \}, \quad (2.4)$$

де:

LR – інтегральний рівень наслідків порушення конфіденційності, цілісності та доступності інформаційного активу;

Cc – рівень наслідків шкоди у разі порушення конфіденційності;

Ci – рівень наслідків шкоди у разі порушення цілісності;

Ca – рівень наслідків шкоди у разі порушення доступності.

Використання максимального значення серед показників *Cc, Ci та Ca* дозволяє врахувати найбільш критичний сценарій реалізації загрози та забезпечує консервативний і обґрунтований підхід до оцінювання фінансових втрат у процесі діагностики ризиків інформаційної безпеки [31].

Оцінювання рівня наслідків шкоди, що виникає внаслідок порушення конфіденційності, цілісності або доступності інформаційних активів підприємства, здійснюється з використанням уніфікованої шкали значень. Такий підхід дає змогу кількісно визначити ступінь негативного впливу інцидентів інформаційної безпеки на фінансовий стан, стабільність бізнес-процесів та ділову репутацію організації, а

також сприяє зіставленню результатів оцінювання для різних активів і сценаріїв загроз (табл. 2.3).

Таблиця 2.3

Рівні наслідків порушення конфіденційності, цілісності та доступності інформаційного активу

Значення рівня наслідків	Характеристика наслідків
0	Порушення не призводять до відчутних негативних наслідків для діяльності підприємства
0,1–0,3	Незначні фінансові втрати; мінімальний вплив на бізнес-процеси; незначне погіршення ділової репутації та часткова втрата довіри окремих клієнтів і партнерів
0,4–0,6	Помірні фінансові збитки; відчутний вплив на окремі бізнес-процеси; помірне погіршення іміджу підприємства та зменшення довіри клієнтів і партнерів
0,7–0,9	Значні фінансові втрати; суттєве порушення функціонування більшості бізнес-процесів; істотне погіршення репутації та втрата довіри значної частини клієнтів і партнерів
1	Критичні фінансові втрати; повна або майже повна дестабілізація бізнес-процесів; критичне погіршення іміджу підприємства та масова втрата довіри клієнтів і партнерів

Для інтерпретації отриманого значення ризику від реалізації загрози R доцільно встановити порогові значення допустимих фінансових втрат, що відображають рівень ризик-апетиту підприємства. У межах даного дослідження граничним критерієм прийнятності ризику визначено рівень збитків, що становить 5 % від чистого прибутку підприємства. На основі цього підходу ризики інформаційної безпеки класифікуються за рівнем їх значущості залежно від величини можливих матеріальних втрат (табл. 2.4).

Таблиця 2.4

Класифікація ризиків за величиною фінансових збитків

Рівень ризику	Величина матеріального збитку
Високий	≥ 5 % від чистого прибутку підприємства
Середній	від 2 % до 5 % чистого прибутку підприємства
Низький	≤ 2 % чистого прибутку підприємства

У практиці управління інформаційною безпекою підприємство зосереджує основні управлінські та організаційні заходи на реагуванні й мінімізації ризиків із високим і середнім рівнем, оскільки їх реалізація може призвести до істотних фінансових втрат, порушення безперервності бізнес-процесів і погіршення репутації. Ризики низького рівня, як правило, визнаються прийнятними та контролюються шляхом регулярного моніторингу без впровадження додаткових витратних заходів захисту.

Таким чином, методичні підходи до діагностики ризиків інформаційної безпеки ґрунтуються на системному, ризик-орієнтованому та циклічному процесі, що охоплює ідентифікацію, аналіз і оцінювання ризиків з урахуванням специфіки інформаційних активів, характеру загроз і ефективності наявних заходів захисту. Використання кількісних і напівкількісних методів оцінювання дозволяє обґрунтовано визначати рівень ризиків, зіставляти їх між собою та формувати пріоритети управлінських рішень у сфері інформаційної безпеки.

Запропонований підхід забезпечує прозорість і порівнюваність результатів оцінювання, сприяє підвищенню якості управління системою захисту інформації та створює основу для подальшого вибору і впровадження ефективних заходів реагування. У контексті цифрової трансформації підприємств така методика діагностики ризиків є необхідною передумовою для забезпечення стійкості інформаційної інфраструктури та відповідності системи захисту сучасним вимогам безпеки.

2.2. Концептуальна модель системи управління інформаційною безпекою організації

Перехід від методів оцінювання ризиків інформаційної безпеки до формування цілісної системи управління ними зумовлює необхідність розгляду концептуальної моделі системи управління інформаційною безпекою організації.

Така модель визначає логіку взаємодії ключових елементів безпеки, місце процесів управління ризиками в загальній структурі управління та механізми інтеграції заходів захисту в діяльність підприємства. В умовах цифрової трансформації саме наявність формалізованої концептуальної моделі дозволяє забезпечити узгодженість управлінських рішень, адаптивність системи захисту до змін середовища та її відповідність міжнародним стандартам.

Система управління інформаційною безпекою розглядається не лише як сукупність технічних і організаційних заходів, а як комплексний управлінський механізм, орієнтований на досягнення стратегічних цілей організації шляхом зниження інформаційних ризиків до прийнятного рівня. Центральним елементом такої системи виступає ризик-орієнтований підхід, який забезпечує пріоритетність захисту найбільш критичних інформаційних активів і раціональний розподіл ресурсів.

Управління ризиками інформаційної безпеки є ключовою складовою системи управління інформаційною безпекою організації та визначає її функціональну спрямованість. Методологічну основу цього процесу формують міжнародні стандарти, зокрема ISO/IEC 27005:2022, який надає детальні рекомендації щодо менеджменту ризиків інформаційної безпеки та забезпечує практичну реалізацію вимог стандарту ISO/IEC 27001 щодо функціонування СУІБ. При цьому підхід ISO/IEC 27005 узгоджується із загальними принципами управління ризиками, закладеними в стандарті ISO 31000:2018 [28; 29; 30; 31].

Відповідно до положень ISO 31000, ризик трактується як вплив невизначеності на досягнення цілей організації, що може проявлятися у відхиленні від запланованих результатів як у негативному, так і в позитивному напрямі. Управління ризиками, у цьому випадку, спрямоване на систематичне виявлення, аналіз, оцінювання та зниження рівня невизначеності, що впливає на стабільність функціонування інформаційних систем і бізнес-процесів організації [55].

Стандарт ISO 31000:2018 визначає базові принципи ризик-менеджменту, які мають бути покладені в основу концептуальної моделі системи управління інформаційною безпекою. До таких компонентів належать інтегрованість управління ризиками в загальну систему менеджменту, структурованість і комплексність підходів, адаптація до контексту діяльності організації, залучення зацікавлених сторін, динамічність процесів, використання достовірної та актуальної інформації, урахування людських і культурних чинників, а також орієнтація на постійне вдосконалення. Дотримання зазначених компонентів забезпечує узгодженість процесів управління інформаційною безпекою на стратегічному, тактичному та операційному рівнях (рис. 2.2).

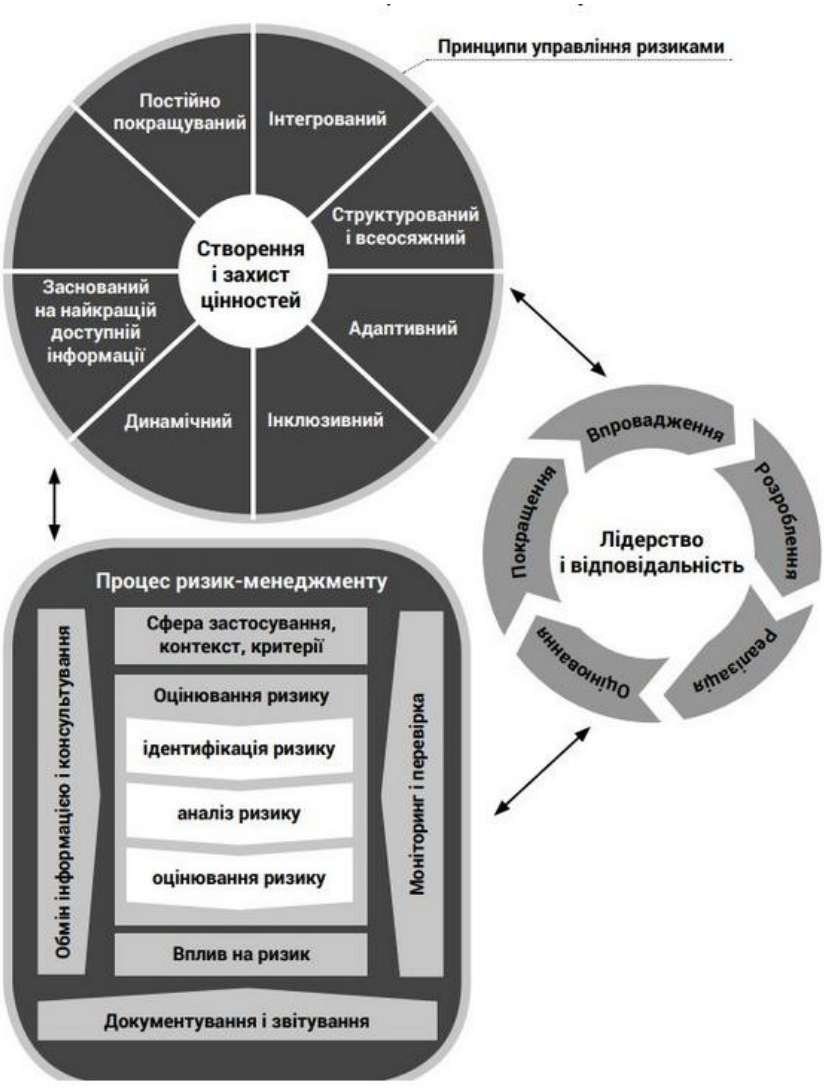

Рис. 2.2. Основні компоненти ризик-менеджменту ISO 31000:2018 [55]

ISO/IEC 27005:2022 конкретизує ці принципи з урахуванням специфіки інформаційної безпеки та пропонує концептуальну модель процесу управління ризиками ІБ, яка базується на загальній рамковій моделі ISO 31000. Відповідно до цього стандарту процес управління ризиками інформаційної безпеки включає послідовні взаємопов'язані етапи: встановлення контексту; оцінювання ризиків, що охоплює ідентифікацію, аналіз та оцінку; обробку ризиків; прийняття залишкових ризиків; комунікацію та консультування з питань ризику; а також моніторинг і перегляд результатів [57].

Зазначені етапи формують замкнутий ітеративний цикл, який постійно повторюється з метою забезпечення актуальності оцінок ризиків і ефективності впроваджених заходів захисту. Після реалізації заходів з обробки ризиків здійснюється повторне оцінювання залишкових ризиків, а за необхідності – коригування обраних управлінських рішень. Такий підхід дозволяє адаптувати систему управління інформаційною безпекою до змін у зовнішньому та внутрішньому середовищі організації, появи нових загроз і трансформації бізнес-процесів.

Узгодженість концептуальної моделі управління ризиками інформаційної безпеки з вимогами ISO/IEC 27001 забезпечує інтеграцію ризик-менеджменту в загальну систему управління організацією та підкріплюється активною роллю керівництва. Підтримка з боку топ-менеджменту, визначення чітких ролей і відповідальності, а також орієнтація на постійне поліпшення виступають необхідними умовами ефективного функціонування системи управління інформаційною безпекою в цілому [56].

Концептуальну модель процесу управління ризиками інформаційної безпеки в межах системи управління інформаційною безпекою організації представлено на рис. 2.3.

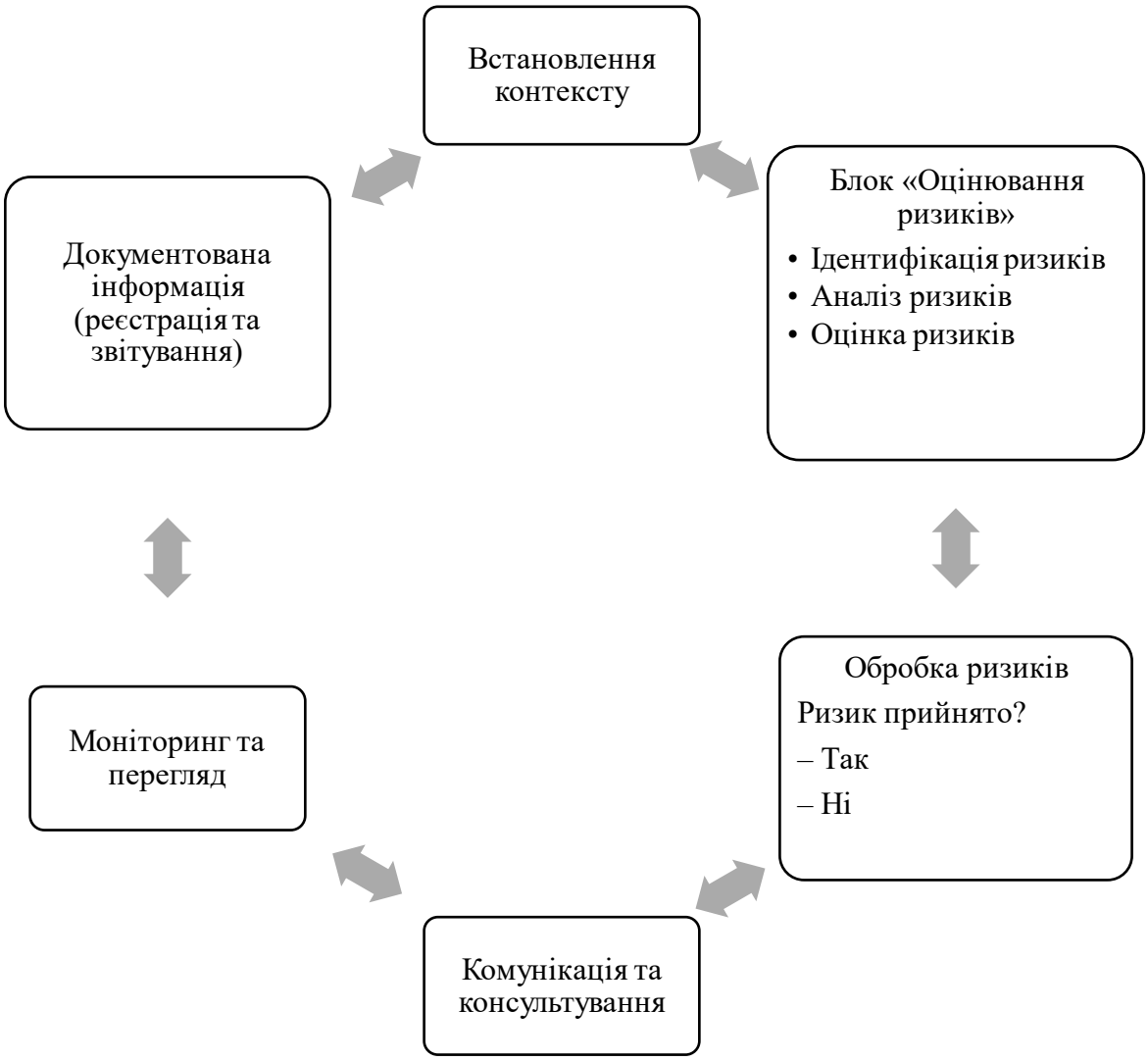

Рис. 2.3. Концептуальна модель процесу управління ризиками інформаційної безпеки в системі управління інформаційною безпекою організації [56]

Запропонована схема демонструє логічну послідовність і взаємозв'язок ключових етапів ризик-менеджменту, які реалізуються у вигляді безперервного циклу та забезпечують системність і адаптивність управління інформаційною безпекою в умовах цифрової трансформації.

Початковим етапом концептуальної моделі є встановлення контексту, в межах якого визначаються цілі інформаційної безпеки, межі застосування системи управління, критерії оцінювання ризиків і їх прийнятності, а також аналізуються внутрішні й зовнішні фактори, що впливають на рівень ризиків. До таких факторів

належать організаційна структура підприємства, особливості бізнес-процесів, нормативно-правові вимоги, рівень цифрової зрілості та актуальні загрози інформаційному середовищу.

Наступним блоком є оцінювання ризиків інформаційної безпеки, яке охоплює три взаємопов'язані підпроцеси. На етапі ідентифікації ризиків здійснюється виявлення інформаційних активів, джерел загроз, наявних вразливостей і можливих сценаріїв інцидентів. Аналіз ризиків спрямований на визначення рівня ризику шляхом оцінювання ймовірності реалізації загроз та масштабів можливих наслідків для діяльності організації. Оцінка ризиків полягає у зіставленні отриманих рівнів ризику з установленими критеріями прийнятності, що дозволяє ранжувати ризики та визначити пріоритети подальших дій.

За результатами оцінювання здійснюється перехід до етапу обробки ризиків, у межах якого обираються та впроваджуються відповідні варіанти реагування. До них належать зниження ризику шляхом впровадження заходів захисту, уникнення ризику через зміну або припинення певних процесів, передача ризику третім сторонам або прийняття ризику за умови його відповідності встановленому рівню допустимості. Після реалізації заходів управління здійснюється формальне прийняття залишкових ризиків на рівні керівництва організації.

Важливою особливістю концептуальної моделі є те, що процеси комунікації та консультування, а також моніторингу і перегляду ризиків супроводжують усі етапи управління ризиками інформаційної безпеки. Комунікація забезпечує своєчасне інформування зацікавлених сторін щодо рівня ризиків і прийнятих управлінських рішень, тоді як моніторинг і перегляд дозволяють відстежувати зміни у середовищі загроз, оцінювати ефективність впроваджених заходів і забезпечувати актуальність оцінок ризиків. Уся діяльність у межах управління ризиками підлягає обов'язковому документуванню та аналізу з боку керівництва, що сприяє прозорості й керованості системи управління інформаційною безпекою.

Запропонована концептуальна модель управління ризиками інформаційної безпеки узгоджується з вимогами стандарту ISO/IEC 27001, який встановлює обов'язковість оцінювання інформаційних ризиків, визначення критеріїв їх оцінки та документального підтвердження результатів у межах системи управління інформаційною безпекою. Водночас стандарт ISO/IEC 27005 забезпечує методичну підтримку цього процесу, деталізуючи порядок ідентифікації, аналізу та обробки ризиків. На етапі обробки ризиків концептуальна модель також взаємодіє зі стандартом ISO/IEC 27002, який надає структурований перелік заходів контролю для зниження і мінімізації ризиків інформаційної безпеки [57].

Таким чином, концептуальна модель системи управління інформаційною безпекою організації ґрунтується на ризик-орієнтованому підході та реалізується у вигляді безперервного циклу управління ризиками. Вона забезпечує логічну узгодженість між встановленням контексту, оцінюванням, обробкою та моніторингом ризиків, а також інтеграцію процесів управління інформаційною безпекою у загальну систему управління підприємством. Узгодженість стандартів ISO/IEC 27001, ISO/IEC 27005, ISO/IEC 27002 та ISO 31000 дозволяє сформувати цілісну й ефективну систему управління інформаційною безпекою, орієнтовану на постійне вдосконалення, адаптацію до змін цифрового середовища та забезпечення стійкості бізнес-процесів організації.

2.3. Моделі моніторингу та оцінювання стану інформаційної безпеки в цифровому середовищі

Функціонування системи управління інформаційною безпекою в цифровому середовищі не обмежується одноразовим оцінюванням ризиків на етапі її впровадження, а потребує їх постійного відстеження та переоцінювання з урахуванням динаміки загроз, змін інформаційної інфраструктури та зовнішніх регуляторних вимог. У цьому контексті особливого значення набувають моделі

моніторингу та оцінювання стану інформаційної безпеки, які забезпечують актуальність ризик-профілю організації та створюють підґрунтя для своєчасного коригування управлінських рішень. Такі підходи є складовою ризик-орієнтованої логіки СУІБ і інтегруються в її загальну архітектуру, забезпечуючи адаптивність і безперервність функціонування.

Моніторинг ризиків інформаційної безпеки полягає у систематичному збиранні, аналізі та інтерпретації інформації про чинники, здатні впливати на рівень ризику з плином часу. У цифровому середовищі ці чинники мають виражений динамічний характер і охоплюють як технічні, так і організаційні складові. До них належать поява нових загроз, зокрема поширення нових типів шкідливого програмного забезпечення, удосконалення методів кібератак, а також зміна тактик і мотивації потенційних порушників, що безпосередньо впливає на рівень ризиків для інформаційних активів.

Важливим елементом моніторингу є своєчасне виявлення нових вразливостей у програмному забезпеченні, апаратних компонентах і мережевій інфраструктурі. Інформація з відкритих джерел про вразливості, зокрема повідомлення типу CVE, рекомендації CERT та галузеві аналітичні огляди, повинна регулярно відслідковуватися і враховуватися під час актуалізації оцінок ризику. Не менш значущими є зміни у складі та характеристиках інформаційних активів організації, такі як впровадження нових інформаційних систем, використання хмарних сервісів, модернізація мережевої архітектури або трансформація бізнес-процесів, що змінює конфігурацію загроз і вразливостей.

Окрему групу факторів моніторингу становлять зміни у вимогах законодавства, нормативних документах і договірних зобов’язаннях у сфері інформаційної безпеки, а також результати внутрішніх і зовнішніх аудитів, тестувань на проникнення та перевірок ефективності засобів захисту. Аналіз інцидентів інформаційної безпеки, які мали місце як у межах організації, так і в інших суб’єктів відповідної галузі, дозволяє враховувати накопичений досвід і

використовувати його для уточнення ризик-оцінок та вдосконалення управлінських підходів.

У практиці управління інформаційною безпекою застосовуються різні моделі моніторингу, які доповнюють одна одну залежно від рівня зрілості СУІБ і складності цифрового середовища. Поряд із подієво-орієнтованим моніторингом, що базується на фіксації та аналізі інцидентів і подій безпеки, поширення набувають процесно-орієнтовані моделі, спрямовані на контроль дотримання політик, процедур і регламентів інформаційної безпеки. Такі моделі дозволяють оцінювати не лише наслідки порушень, а й стабільність функціонування процесів захисту інформації.

Окреме місце займають ризик-орієнтовані моделі моніторингу, у межах яких ключовим об’єктом спостереження є зміни рівнів ризиків і факторів, що на них впливають. У таких підходах акцент робиться на динамічному перегляді імовірності реалізації ризик-сценаріїв і масштабів можливих наслідків, що забезпечує своєчасну адаптацію заходів захисту. Доповненням до них є показникові моделі моніторингу, які базуються на системі кількісних і якісних індикаторів, що відображають стан захищеності, ефективність контролів і тенденції розвитку загроз.

Відповідно до рекомендацій ISO/IEC 27005:2022, моніторинг ризиків має здійснюватися на постійній основі з використанням формалізованих процедур і чітко визначених відповідальних ролей. Практична реалізація цього процесу передбачає ведення реєстрів подій і інцидентів інформаційної безпеки з подальшим аналізом тенденцій, призначення відповідальних осіб за відстеження зовнішніх джерел інформації про загрози, а також використання автоматизованих інструментів контролю. До таких інструментів належать системи класу SIEM, які забезпечують безперервний збір і кореляцію подій безпеки, виявлення аномальної активності та формування аналітичної інформації для підтримки управлінських рішень [58].

Поряд із постійним моніторингом, сучасні підходи до управління інформаційною безпекою передбачають регулярний перегляд ризиків і самої системи ризик-менеджменту. Такий перегляд може здійснюватися з визначеною періодичністю або ініціюватися настанням подій-тригерів, що істотно впливають на стан безпеки. У межах перегляду актуалізується контекст управління ризиками, уточнюється перелік ідентифікованих ризиків, переглядаються їх рівні з урахуванням нових даних та оцінюється ефективність впроваджених заходів захисту.

Позаплановий перегляд ризиків є необхідним у разі виникнення суттєвих інцидентів інформаційної безпеки, змін організаційної структури або значних трансформацій IT-ландшафту, таких як злиття компаній, впровадження нових інформаційних платформ або критичних цифрових сервісів. У таких умовах попередні оцінки ризику можуть втратити актуальність, що потребує повторного проходження ключових етапів процесу управління ризиками.

Моделі моніторингу та оцінювання стану інформаційної безпеки тісно пов’язані з вимогами ISO/IEC 27001 щодо оцінки результативності СУІБ і аналізу з боку керівництва. Організація має визначати показники моніторингу, які відображають стан управління ризиками, динаміку інцидентів і ефективність реалізації планів обробки ризиків. Отримані результати використовуються як інформаційна основа для прийняття управлінських рішень, спрямованих на підтримання прийнятного рівня ризику та раціональний розподіл ресурсів у сфері інформаційної безпеки.

Після формування переліку ризиків інформаційної безпеки наступним етапом є їх оцінювання, яке виступає ключовим інструментом визначення фактичного стану захищеності інформаційного середовища організації. Оцінювання ризиків дозволяє не лише охарактеризувати окремі ризики у якісній або кількісній формі, а й сформувати узагальнену картину рівня інформаційної безпеки в умовах функціонування цифрової інфраструктури підприємства.

Процес оцінювання ризиків включає аналіз ризиків і їх подальшу оцінку шляхом порівняння отриманих результатів із встановленими критеріями прийнятності. Основною метою цього процесу є визначення значущості кожного ризику для діяльності організації та встановлення пріоритетів реагування з урахуванням впливу ризиків на досягнення стратегічних і операційних цілей.

Відповідно до положень ISO/IEC 27005:2022, аналіз ризиків ґрунтується на оцінюванні імовірності реалізації ризик-сценаріїв і масштабів можливих наслідків для організації. Такий підхід узгоджується з вимогами ISO/IEC 27001:2022 і забезпечує формування інтегрального показника ризику, який може використовуватися для прийняття управлінських рішень у сфері інформаційної безпеки з урахуванням рівня зрілості СУІБ та доступності вихідних даних [56; 58].

Таким чином, моделі моніторингу та оцінювання стану інформаційної безпеки в цифровому середовищі забезпечують перехід організацій від реактивного реагування на інциденти до проактивного управління ризиками. Їх застосування дозволяє своєчасно виявляти нові загрози, підтримувати актуальність ризик-профілю, формувати обґрунтовану систему прийняття управлінських рішень і забезпечувати стійкість інформаційних активів в умовах зростаючої цифрової складності.

Висновки до розділу 2

У другому розділі розглянуто методи та підходи, що формують методичну основу оцінювання стану інформаційної безпеки організації в умовах цифрового середовища. Обґрунтовано, що результативне управління інформаційною безпекою неможливе без послідовної діагностики ризиків, яка забезпечує об’єктивне визначення рівня захищеності інформаційних активів, виявлення критичних вразливостей і підготовку управлінських рішень щодо вдосконалення системи захисту інформації.

Розкрито логіку процесу оцінювання ризиків через взаємопов’язані етапи ідентифікації, аналізу та оцінювання, а також показано значення уніфікованих критеріїв і шкал для забезпечення порівнюваності результатів і зменшення впливу суб’єктивності. Узагальнено практику використання якісного, кількісного та напівкількісного підходів, уточнено роль матриці ризику як інструмента візуалізації співвідношення “ймовірність – вплив” і обґрунтування пріоритетів реагування. Окремо акцентовано, що в межах дослідження формалізація оцінювання ґрунтується на поєднанні очікуваних фінансових втрат від одноразового інциденту та показника середньорічної частоти реалізації загрози, що дозволяє зіставляти ризики між собою та визначати черговість упровадження заходів безпеки.

Сформовано концептуальне бачення системи управління інформаційною безпекою як комплексного управлінського механізму, де управління ризиками виступає центральною функціональною складовою. Показано узгодженість ризик-орієнтованої рамки з вимогами ISO/IEC 27001, рекомендаціями ISO/IEC 27005 та принципами ISO 31000, а також доведено ітеративність і безперервність циклу управління ризиками як передумову адаптивності СУІБ до змін у цифровій інфраструктурі, бізнес-процесах і ландшафті загроз.

Узагальнено підходи до моніторингу та оцінювання стану інформаційної безпеки в цифровому середовищі як практичного механізму підтримання актуальності ризик-профілю організації. Визначено, що систематичне відстеження подій і інцидентів, контроль дотримання політик і процедур, ризик-орієнтований перегляд чинників ризику та використання показників результативності створюють інформаційну основу для своєчасного коригування управлінських рішень. У підсумку доведено, що поєднання регулярного моніторингу, перегляду ризиків, застосування критеріїв прийнятності та інструментів пріоритезації забезпечує перехід від реактивного реагування на інциденти до проактивного управління інформаційною безпекою в умовах зростаючої цифрової складності.

РОЗДІЛ 3
ПРАКТИЧНА КОНЦЕПЦІЯ ВДОСКОНАЛЕННЯ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ОРГАНІЗАЦІЇ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

3.1. Характеристика об’єкта дослідження та аналіз поточного стану інформаційної безпеки

Для проведення практичного дослідження було обрано підприємство ТОВ «ВСЕ ДЛЯ ЛЮДЕЙ 2024», яке здійснює господарську діяльність із використанням сучасних цифрових інструментів та інформаційних систем.

ТОВ «ВСЕ ДЛЯ ЛЮДЕЙ 2024» є відносно новим підприємством, зареєстрованим 24.07.2024 у Київській області (Бучанський район, с. Софіївська Борщагівка), яке здійснює діяльність у сфері роздрібної торгівлі продуктами харчування, а також здійснює операції з купівлі та продажу власного нерухомого майна та проводить діяльність у сфері рекламних агентств. Сукупність зазначених напрямів зумовлює обробку різнорідних інформаційних ресурсів, зокрема фінансової та облікової інформації, договірної документації, даних про контрагентів, клієнтів і персонал, а також комерційної інформації, що має безпосередній вплив на фінансову стабільність і конкурентні позиції підприємства.

За наявними фінансовими показниками за 2024 рік підприємство має значний дохід при відносно невеликому чистому прибутку, що підсилює актуальність питання захисту інформації, оскільки фінансовий результат є чутливим до будь-яких позапланових втрат. За таких умов навіть одиничний інцидент інформаційної безпеки, пов’язаний із витоком даних, порушенням цілісності інформації або збоєм у роботі інформаційних систем, здатен спричинити непропорційно великі економічні втрати та негативно вплинути на фінансову стабільність і стійкість підприємства (табл. 3.1).

Таблиця 3.1

Основні фінансові показники ТОВ «ВСЕ ДЛЯ ЛЮДЕЙ 2024» за 2024 рік [49]

Показники фінансової звітності	Значення, грн
Дохід	125 118 400
Чистий прибуток	684 700
Активи	42 746 300
Зобов'язання	41 431 300
Статутний капітал	800 000
Кількість працівників, осіб	82

Організаційна структура компанії є розгалуженою та орієнтованою на підтримку ключових бізнес-процесів торгівлі, логістики, закупівель і фінансового управління. Управління здійснюється генеральним директором у взаємодії з функціональними напрямами, серед яких важливе місце посідають IT-напрям і напрям безпеки, а також фінансовий блок, що працює з чутливими даними та формує основу управлінської звітності. Для підприємства такого типу характерна висока інтенсивність інформаційних потоків між підрозділами, а також постійна взаємодія з контрагентами, що підвищує вимоги до захисту даних і контролю доступу.

Критично важливими для компанії є інформаційні активи, пов'язані з фінансами та взаєморозрахунками, обліком товарних запасів, договорами, ціноутворенням, плануванням закупівель і звітністю. Саме ці дані мають найбільшу цінність з точки зору конкурентних переваг і водночас є найбільш привабливими для зловмисників. Практична вразливість таких активів посилюється тим, що вони зберігаються і обробляються на різних носіях і в різних середовищах – на робочих ПК працівників, у системі електронного документообігу, на паперових носіях, у системі обліку UniproRetail, а також у поштовій інфраструктурі та на сервері з даними про постачальників і фінансовою звітністю. За цих умов навіть часткове порушення конфіденційності або цілісності даних може вплинути на розрахунки, коректність управлінських рішень, виконання договірних зобов'язань і дотримання вимог законодавства.

Цифрова інфраструктура підприємства сформована як інтегроване поєднання локальних і віддалених сервісів, що забезпечує безперервність бізнес-процесів та гнучкість у роботі. До складу інфраструктури входять локальна мережа центрального офісу, серверні ресурси, робочі станції персоналу, віддалені канали доступу для працівників і філій, база даних клієнтів та замовлень, система електронного документообігу, CRM, електронна пошта та хмарні сховища. Використання сучасних хмарних платформ дозволяє масштабувати ресурси за потреби, оптимізувати зберігання та обробку даних, а також підвищувати продуктивність праці.

Така архітектура створює високий рівень операційної гнучкості та підтримує зростання бізнесу, проте водночас збільшує поверхню атак і ускладнює контроль безпеки через різні середовища обробки даних та різні категорії користувачів, які мають неоднакові потреби й рівні доступу. Для забезпечення захищеності інформаційних ресурсів застосовуються системи управління доступом, багаторівнева автентифікація користувачів, моніторинг подій безпеки та антивірусний захист, а також регулярні аудити та оцінка ризиків. Підприємство також впроваджує політики резервного копіювання та відновлення даних, що дозволяє мінімізувати наслідки потенційних інцидентів і гарантувати безперервність діяльності.

Для комплексної оцінки поточного стану інформаційної безпеки ТОВ «ВСЕ ДЛЯ ЛЮДЕЙ 2024» було застосовано підхід оцінювання рівня зрілості ключових процесів управління інформаційною безпекою, що ґрунтується на рекомендаціях стандартів ISO/IEC 27000–27005 та практиках Information Security Forum (ISF). Такий підхід дозволяє визначити не лише наявність окремих заходів захисту, а й ступінь їх формалізації, керованості та інтеграції в систему управління підприємством. Оцінювання виконувалося з урахуванням специфіки діяльності підприємства, використання централізованих облікових систем (зокрема UniproRetail), наявності виділених IT-функцій, серверної інфраструктури та

базових процедур контролю доступу, а також з урахуванням того, що компанія перебуває на початковому етапі свого розвитку.

Оцінювання поточного стану інформаційної безпеки здійснюється відповідно до критеріїв, відображених у табл. 3.2.

Таблиця 3.2

Критерії оцінки поточного стану інформаційної безпеки [41]

Рівень зрілості	**Позначення рівня зрілості**	**Опис**
0	Відсутній	Заходи з інформаційної безпеки фактично не застосовуються, процеси захисту інформації відсутні, ризики не ідентифікуються та не контролюються.
1	Низький	Окремі заходи інформаційної безпеки застосовуються епізодично та несистемно, без формалізованих процедур, відповідальності й контролю.
2	Початковий	Базові процеси інформаційної безпеки реалізуються на постійній основі, проте мають фрагментарний характер і переважно спираються на загальні практики та рекомендації без чіткої внутрішньої регламентації.
3	Формалізований	Процеси захисту інформації визначені та виконуються відповідно до встановлених правил, наявні відповідальні особи та організаційні ресурси для підтримки поточного рівня безпеки.
4	Керований	Стан інформаційної безпеки систематично контролюється, здійснюється аналіз подій безпеки, управління доступом і ризиками, а також регулярна оцінка ефективності впроваджених заходів.
5	Оптимізований	Інформаційна безпека інтегрована в систему управління організацією, її стан вимірюється кількісними показниками, а процеси захисту постійно вдосконалюються з урахуванням змін цифрового середовища та загроз.

Застосування зазначених критеріїв дозволяє не лише оцінити поточний стан процесів управління інформаційною безпекою, але й здійснити порівняльний аналіз з вимогами нормативних документів і міжнародними стандартами в цій сфері. Такий підхід дає змогу ідентифікувати слабкі місця в системі захисту інформаційних ресурсів, визначити пріоритетні напрями вдосконалення, а також обґрунтовано планувати заходи щодо підвищення ефективності управління безпекою та зменшення потенційних ризиків.

Систематизація рівнів зрілості процесів управління інформаційною безпекою, що відображає ключові ознаки та критерії кожного рівня, наведена в табл. 3.3.

Таблиця 3.3

Оцінка поточного стану процесів інформаційної безпеки ТОВ «ВСЕ ДЛЯ ЛЮДЕЙ 2024» [41]

№	Найменування процесу інформаційної безпеки	Рівень зрілості
1	Стратегія інформаційної безпеки	2
2	Усвідомлення керівництвом важливості інформаційної безпеки	3
3	Управління ризиками інформаційної безпеки	2
4	Управління відповідністю нормативним вимогам	2
5	Аудит інформаційної безпеки	1
6	Політика інформаційної безпеки	2
7	Управління доступом до інформаційних ресурсів	2
8	Управління вразливостями	2
9	Управління життєвим циклом інформаційних систем	2
10	Управління інформаційними активами	3
11	Управління змінами	2
12	Архітектура інформаційної безпеки	2
13	Управління каналами зв’язку	2
14	Управління зовнішніми контрагентами	2
15	Виявлення та аналіз загроз	2
16	Управління подіями інформаційної безпеки	1
17	Управління інцидентами інформаційної безпеки	1
18	Антикризове управління	1
19	Забезпечення безперервності бізнесу	2
20	Підвищення обізнаності персоналу з інформаційної безпеки	1
21	Безпека персоналу	2
Загальний рівень поточного стану інформаційної безпеки		2,05

Отримані результати оцінки свідчать, що поточний стан інформаційної безпеки ТОВ «ВСЕ ДЛЯ ЛЮДЕЙ 2024» характеризується початковим рівнем сформованості процесів із окремими елементами формалізації. Найбільш розвиненими є процеси, пов’язані з управлінням інформаційними активами та усвідомленням керівництвом важливості інформаційної безпеки, що пояснюється використанням централізованих систем обліку, зокрема програмного забезпечення UniproRetail, та наявністю базових управлінських практик.

Водночас значна частина процесів інформаційної безпеки перебуває на низькому або початковому рівні. Це стосується, зокрема, аудиту інформаційної безпеки, управління інцидентами, подіями безпеки, антикризового управління та підвищення обізнаності персоналу. Така ситуація є типовою для новостворених підприємств, у яких пріоритет на початковому етапі розвитку зосереджений на забезпеченні операційної діяльності, а системний підхід до управління інформаційною безпекою лише формується.

Загальний інтегральний показник на рівні 2,05 свідчить про наявність базових механізмів захисту інформації, проте їх фрагментарність і недостатня керованість створюють підвищені ризики в умовах цифрової трансформації. Це обумовлює необхідність переходу від реактивних і несистемних заходів до впровадження цілісної практичної концепції вдосконалення управління інформаційною безпекою.

Також межах аналізу поточного стану інформаційної безпеки ТОВ «ВСЕ ДЛЯ ЛЮДЕЙ 2024» було проведено кількісне оцінювання ризику, пов’язаного з можливим порушенням захищеності фінансової та облікової інформації, що обробляється в системі UniproRetail та зберігається на внутрішніх серверних ресурсах підприємства. Оцінювання здійснювалося відповідно до методики, наведеної в попередньому розділі, на основі визначення фінансових втрат від одноразової реалізації загрози та середньорічної частоти виникнення інцидентів інформаційної безпеки.

Як ключовий інформаційний актив розглядалася фінансова й облікова інформація підприємства, порушення конфіденційності, цілісності або доступності якої може призвести до зупинки облікових і торговельних процесів, необхідності відновлення даних, додаткового навантаження на бухгалтерський та IT-персонал, а також до можливих штрафних санкцій і локальних репутаційних втрат. З урахуванням зазначених чинників вартість відповідного інформаційного активу Cass прийнято на рівні 10% від чистого прибутку.

Оцінювання рівня наслідків порушення базових властивостей інформації здійснювалося відповідно до уніфікованої шкали значень. Для даного активу наслідки порушення конфіденційності оцінено – як помірні у зв'язку з можливим витоком фінансової інформації, наслідки порушення цілісності – як помірні через ризик спотворення облікових даних, а порушення доступності – як помірні з огляду на ймовірний тимчасовий простій системи. Відповідно, інтегральний рівень наслідків LR визначено на рівні 0,6 як максимальне значення серед показників конфіденційності, цілісності та доступності.

Фінансовий збиток від одноразової реалізації загрози було розраховано за формулою (2.3) і він становить:

$$L = Cass \times LR = 68\,470 \times 0{,}6 = 41\,082 \text{ грн.}$$

З урахуванням специфіки діяльності торговельного підприємства, характерних для нього загроз соціальної інженерії, фішингових атак, помилок персоналу та можливих збоїв у роботі інформаційних систем, середньорічну частоту реалізації загроз інформаційної безпеки оцінено як середню. Відповідно до прийнятої шкали значень показник частоти P прийнято рівним 3, що відповідає можливості виникнення інцидентів дотрьох разів на рік.

Інтегральний рівень ризику інформаційної безпеки визначався відповідно до формули (2.2) і становив:

$$R = L \times P = 41\,082 \times 3 = 123\,246 \text{ грн.}$$

Для інтерпретації отриманого результату інтегральний рівень ризику було зіставлено з фінансовими показниками діяльності підприємства. Чистий прибуток ТОВ «ВСЕ ДЛЯ ЛЮДЕЙ 2024» за 2024 рік становив 684 700 грн, що дозволяє визначити частку інтегрального ризику у чистому прибутку на рівні близько 18 %. Таке значення свідчить про підвищений рівень ризику інформаційної безпеки, який наближається до верхньої межі допустимого для підприємства та несе відчутну загрозу його фінансовій стабільності.

Отримані результати підтверджують, що поточний стан інформаційної безпеки ТОВ «ВСЕ ДЛЯ ЛЮДЕЙ 2024» характеризується наявністю суттєвих ризиків, пов’язаних із захистом фінансової та облікової інформації. Хоча зафіксований рівень ризику не є критичним, він перевищує комфортний для підприємства поріг і вимагає впровадження додаткових організаційних та технічних заходів захисту. Таким чином підтверджується необхідність подальшого вдосконалення системи управління інформаційною безпекою, особливо у сфері контролю доступу, адміністрування облікових записів та забезпечення стійкості ключових інформаційних ресурсів в умовах цифрової трансформації.

Доступ до інформаційних ресурсів ТОВ «ВСЕ ДЛЯ ЛЮДЕЙ 2024» здійснюється як через корпоративну мережу, так і через віддалені канали, а також через хмарні сервіси та мобільні застосунки. Виявлені практичні особливості доступу вказують на наявність суттєвих ризиків, пов’язаних із автентифікацією та контролем облікових записів. Зокрема, використання стандартного віддаленого доступу без додаткової перевірки особи, опора на паролі як основний бар’єр захисту, нерівномірність застосування шифрування у листуванні та відсутність єдиної політики поводження з вкладеннями створюють умови, за яких фішингові атаки, компрометація паролів або перехоплення даних можуть призвести до проникнення в критичні системи.

Поточний стан захисту характеризується наявністю базових заходів безпеки, однак аналіз виявляє слабкі місця, що мають системний характер. Проблемними зонами є використання слабких або повторюваних паролів, відсутність багаторівневої перевірки особи для критичних сервісів, недостатній контроль подій безпеки через обмежене логування спроб входу та змін у системах, відсутність шифрування даних на робочих і мобільних пристроях, а також недосконале адміністрування облікових записів, зокрема збереження активності записів працівників після звільнення. Додатковий ризик формують незахищені інтерфейси обміну даними між прикладними системами, оскільки це відкриває можливості для

перехоплення трафіку або підміни запитів у разі компрометації мережевого середовища.

Узагальнення ідентифікованих загроз для підприємства торговельної сфери показує, що найбільш імовірними є інциденти, пов'язані з людським фактором, соціальною інженерією та зловмисним програмним забезпеченням, а також сценарії несанкціонованого доступу через слабкі паролі, помилки налаштувань або недостатній розподіл прав доступу. Потенційні наслідки таких інцидентів для ТОВ «ВСЕ ДЛЯ ЛЮДЕЙ 2024» проявляються у фінансових втратах, репутаційних збитках, ризиках юридичної відповідальності та втраті конкурентних переваг через витік комерційної інформації, що є особливо критичним для компанії з відносно невеликою маржинальністю та високою залежністю від стабільності операційних процесів.

Таким чином, проведений аналіз засвідчив, що поточний стан інформаційної безпеки ТОВ «ВСЕ ДЛЯ ЛЮДЕЙ 2024» має переважно початковий рівень сформованості – із окремими елементами формалізації та усвідомленням важливості захисту з боку керівництва, але без достатньої керованості, регулярного аудиту, повноцінного моніторингу подій та відпрацьованих процедур реагування на інциденти. Результати кількісного оцінювання підтвердили, що ризик порушення захищеності фінансової та облікової інформації в середньому становить близько 18 % чистого прибутку, тобто є високим для підприємства за умов його відносно невеликої маржинальності та залежності від безперервності облікових і торговельних процесів. За таких обставин пріоритетом стає перехід від фрагментарних і переважно реактивних заходів до цілісного підходу, який поєднує організаційні рішення та технічні інструменти, забезпечує контроль доступу до ключових систем, уніфікує правила роботи з даними, підсилює захист облікової інфраструктури та формує послідовну програму підвищення рівня безпеки, орієнтовану на реальні загрози та потреби підприємства в умовах цифрової трансформації.

3.2. Формування стратегії та програми підвищення рівня інформаційної безпеки в умовах цифровізації бізнес-процесів

Сучасна діяльність ТОВ «ВСЕ ДЛЯ ЛЮДЕЙ 2024» здійснюється в умовах активної цифровізації бізнес-процесів, що проявляється у використанні централізованих облікових систем, електронного документообігу, серверних ресурсів, віддаленого доступу та цифрових каналів взаємодії з контрагентами. Такі трансформаційні процеси забезпечують підвищення операційної ефективності та керованості бізнесу, водночас істотно збільшують кількість потенційних загроз інформаційній безпеці та ускладнюють контроль за доступом до чутливих даних.

Проведений аналіз поточного стану інформаційної безпеки підприємства засвідчив наявність базових організаційних і технічних заходів захисту, однак виявив фрагментарність їх реалізації, недостатній рівень формалізації та обмежену керованість процесів безпеки. Отримані результати оцінювання рівня зрілості процесів управління інформаційною безпекою, а також кількісна оцінка ризиків, пов’язаних із захистом фінансової та облікової інформації, підтверджують необхідність переходу від реактивного реагування на інциденти до системного й проактивного підходу до управління інформаційною безпекою.

В умовах цифровізації бізнес-процесів підвищення рівня інформаційної безпеки не може обмежуватися окремими технічними рішеннями або локальними заходами захисту. Воно потребує формування цілісної стратегії, що поєднує організаційні, управлінські та технічні інструменти, узгоджені з бізнес-цілями підприємства, масштабами його діяльності та рівнем прийнятного ризику. Для новоствореного підприємства особливо важливим є поетапний характер впровадження такої стратегії, який дозволяє поступово підвищувати рівень захищеності без надмірного навантаження на ресурси.

З огляду на це, формування стратегії підвищення рівня інформаційної безпеки ТОВ «ВСЕ ДЛЯ ЛЮДЕЙ 2024» має ґрунтуватися на результатах ідентифікації

ключових загроз і вразливостей, пріоритезації ризиків, а також на врахуванні особливостей цифрової інфраструктури підприємства, зокрема використання облікових систем типу UniproRetail, серверних рішень і віддалених каналів доступу. Важливою складовою такої стратегії є розроблення практичної програми заходів, спрямованих на підвищення керованості доступу, посилення контролю дій користувачів, захист критичних інформаційних активів і формування культури інформаційної безпеки серед персоналу.

Результати аналізу ІТ-інфраструктури ТОВ «ВСЕ ДЛЯ ЛЮДЕЙ 2024» свідчать, що одним із найбільш уразливих елементів поточної системи захисту є механізми автентифікації та контролю доступу користувачів до інформаційних ресурсів. На практиці доступ до внутрішніх систем підприємства здебільшого базується на використанні класичної схеми «логін–пароль», яка в умовах сучасних кіберзагроз не забезпечує належного рівня захищеності. Використання слабких або повторюваних паролів, відсутність додаткових факторів перевірки особи та обмежений контроль за створенням і зміною облікових записів істотно підвищують ризик несанкціонованого доступу до критично важливої фінансової та облікової інформації.

Недостатній рівень захищеності процедур автентифікації посилюється відсутністю багаторівневої перевірки користувачів і криптографічного захисту автентифікаційних даних на ключових етапах доступу. За таких умов навіть часткова компрометація облікових даних унаслідок фішингових атак, соціальної інженерії або витоку інформації може призвести до порушення конфіденційності, цілісності та доступності внутрішніх інформаційних ресурсів підприємства. Це створює потенційну загрозу як для внутрішніх бізнес-процесів, так і для обробки комерційної та персональної інформації клієнтів і контрагентів.

З огляду на виявлені вразливості, одним із ключових напрямів підвищення рівня інформаційної безпеки підприємства є впровадження вдосконаленої багаторівневої системи авторизації, орієнтованої на поєднання організаційних і

технічних заходів захисту. Така система має забезпечувати не лише надійний технічний контроль доступу до ресурсів, а й формування єдиної політики автентифікації та управління правами користувачів відповідно до сучасних вимог кібербезпеки та масштабів діяльності підприємства.

В умовах зростання кількості атак соціальної інженерії та поширення фішингових схем доцільним є використання каскадного підходу до автентифікації, за якого доступ до інформаційних ресурсів надається лише після проходження кількох послідовних етапів перевірки особи. Це дозволяє суттєво знизити ймовірність успішного несанкціонованого доступу навіть у разі компрометації одного з рівнів захисту та підвищує загальну стійкість системи до зовнішніх і внутрішніх загроз.

Важливою складовою запропонованого підходу є використання сучасних криптографічних механізмів для захисту автентифікаційних даних, а також впровадження додаткових програмних факторів підтвердження особи під час доступу до критично важливої інформації або виконання чутливих операцій. Такий підхід дозволяє зменшити залежність безпеки системи від людського фактора та мінімізувати ризики, пов’язані з витоком облікових даних.

Для забезпечення централізованого й керованого доступу до підсистем інформаційної інфраструктури підприємства доцільним є застосування ролевої моделі керування доступом RBAC (Role-Based Access Control). Використання цієї моделі дає змогу призначати права доступу на основі функціональних ролей, що спрощує адміністрування, знижує ймовірність помилок у налаштуванні доступу та забезпечує прозорість політики безпеки. Застосування RBAC також створює умови для масштабування системи управління доступом у разі розширення діяльності підприємства або змін у його організаційній структурі.

З метою підвищення рівня захисту комерційної та облікової інформації ТОВ «ВСЕ ДЛЯ ЛЮДЕЙ 2024» пропонується впровадження багаторівневої системи

авторизації, побудованої за принципом послідовної перевірки користувача із застосуванням криптографічних механізмів і ролевого розмежування доступу.

Архітектура системи ґрунтується на використанні окремих логічних компонентів, ключовим з яких є графічний вебінтерфейс для введення облікових даних, контрольних параметрів і взаємодії користувача з повідомленнями безпеки. Обмін інформацією між клієнтською частиною та серверною логікою здійснюється через захищений канал зв'язку з використанням протоколу HTTPS, що мінімізує ризики перехоплення або підміни автентифікаційної інформації під час передавання. Графічний вебінтерфейс наведено на рисунку 3.1.

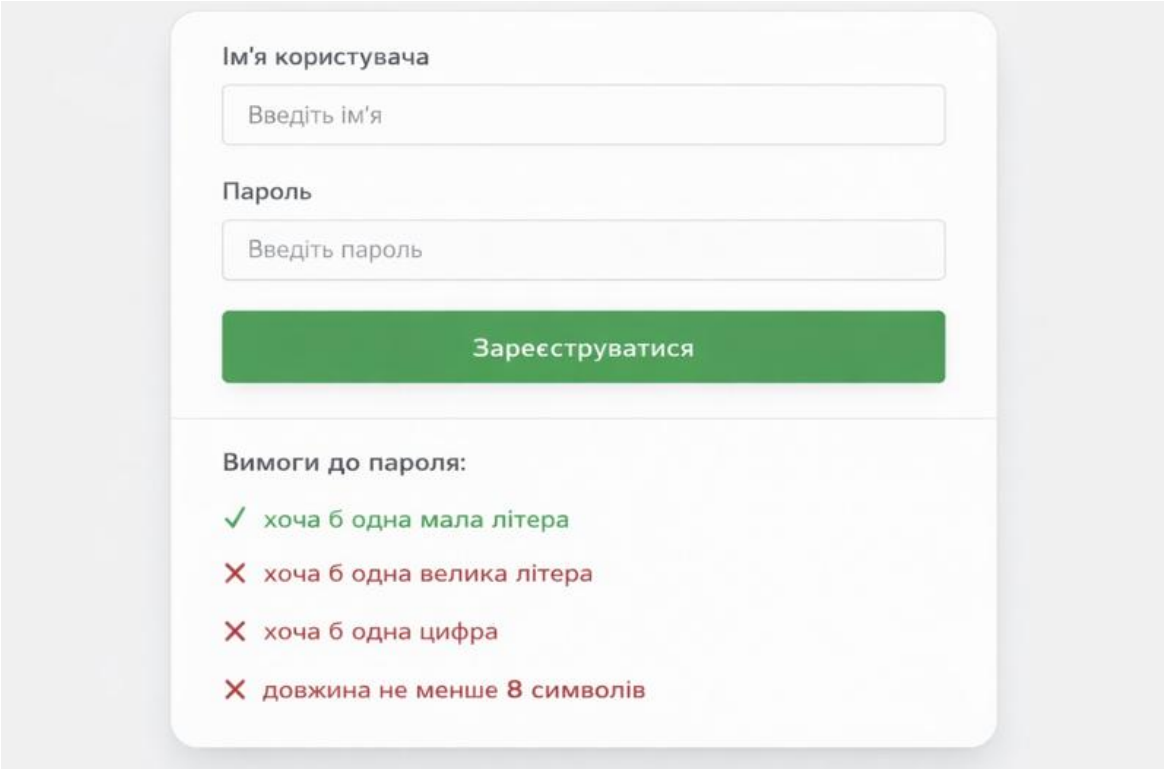

Рис. 3.1. Графічний вебінтерфейс

Процес авторизації реалізується у вигляді каскадної послідовності рівнів перевірки. На першому рівні користувач вводить основні облікові дані, після чого система виконує перевірку відповідності введеного пароля хеш-значенню, збереженому в базі даних. Для цього застосовуються стійкі алгоритми хешування, зокрема PBKDF2 або bcrypt, що відповідають сучасним вимогам криптографічного

захисту та ускладнюють відновлення початкового значення пароля. Схему першого рівня зображено на рисунку 3.2.

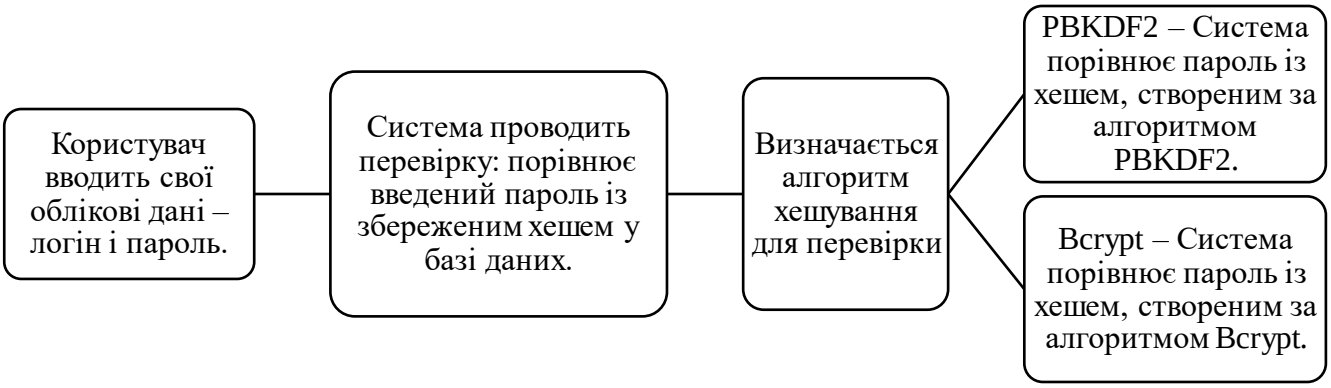

Рис. 3.2. Схема першого рівня

Другий рівень передбачає додаткову перевірку шляхом повторного введення пароля або використання окремого автентифікаційного значення. Перевірка здійснюється за аналогічним принципом, проте з використанням іншого криптографічного ключа або солі, що підвищує стійкість системи до атак у разі часткового витоку інформації з бази даних. Схему другого рівня зображено на рисунку 3.3.

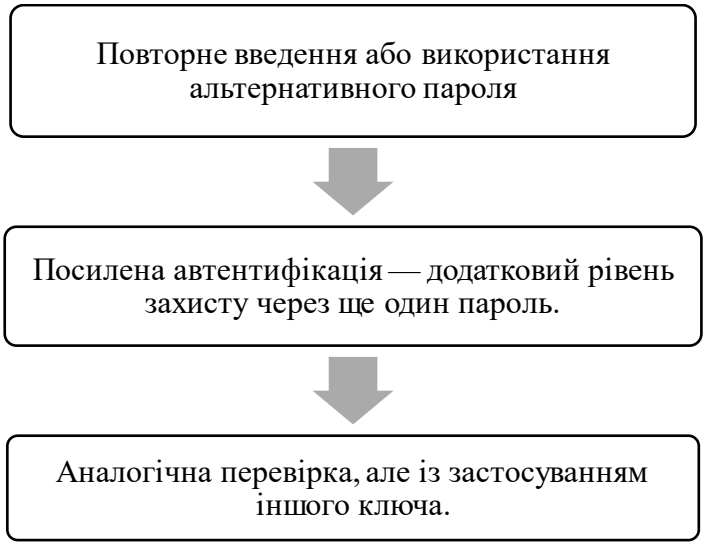

Рис. 3.3. Схема другого рівня

На третьому рівні реалізується посилений механізм захисту, який ґрунтується на двоступеневій криптографічній обробці введеного значення. Пароль шифрується

із застосуванням симетричного алгоритму AES-256 з внутрішнім ключем системи, після чого отриманий результат перетворюється у двійкове представлення та порівнюється з еталонним значенням, збереженим на сервері. Такий підхід істотно ускладнює використання атак типу перебору або словникових атак навіть у разі компрометації зашифрованих даних. Схему рівня 3 зображено на рисунку 3.4

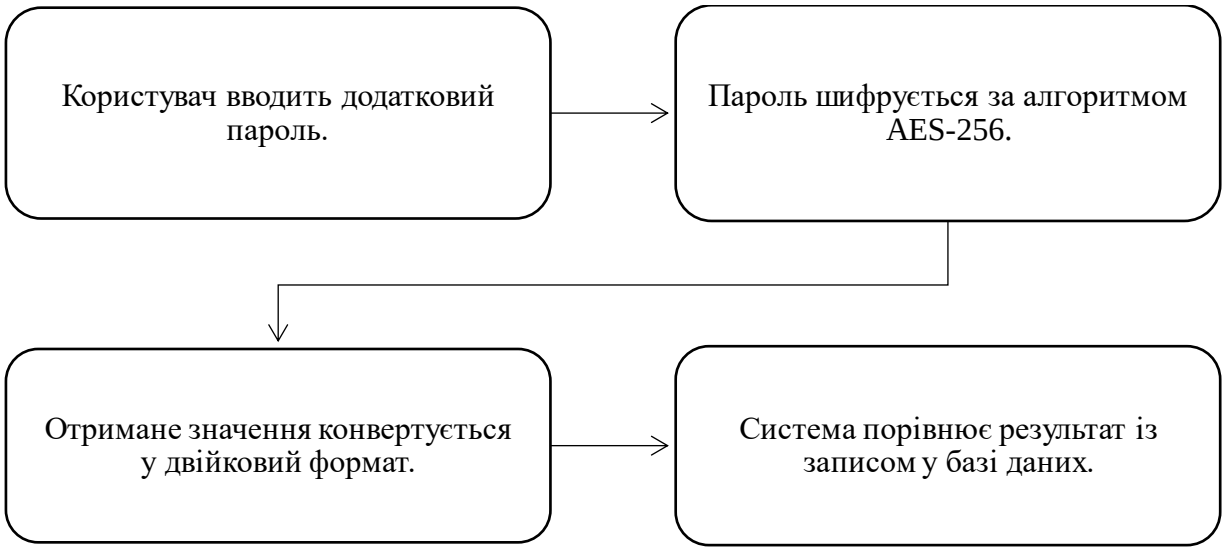

Рис. 3.4. Схема третього рівня

Четвертий рівень авторизації передбачає використання контрольної фрази, яка задається користувачем під час реєстрації та виступає додатковим програмним фактором підтвердження особи. Після введення контрольної фрази система здійснює її криптографічну обробку за схемою подвійного шифрування, аналогічною до застосованої на попередньому рівні, з подальшою перевіркою відповідності збереженому еталонному значенню. Такий механізм дозволяє суттєво підвищити рівень захищеності доступу до фінансової та облікової інформації, а також може застосовуватися під час виконання критично важливих операцій або відновлення доступу до облікового запису. Схему рівня 4 зображено на рисунку 3.5

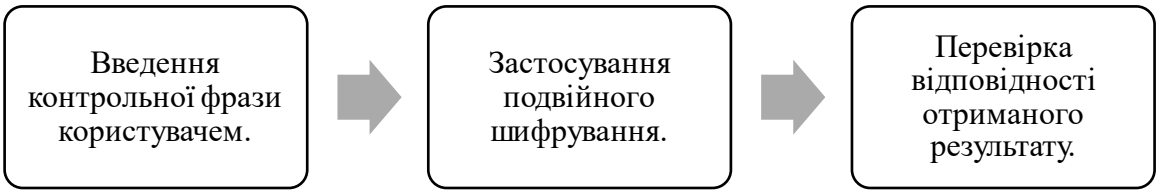

Рис. 3.5. Схема четвертого рівня

Лише після успішного проходження всіх рівнів автентифікації формується токен доступу, який передається до RBAC-модуля для визначення ролі користувача та обсягу його повноважень у системі. Використання ролевої моделі керування доступом забезпечує централізоване та прозоре призначення прав, спрощує адміністрування облікових записів, знижує ризик помилок у налаштуваннях доступу та створює умови для масштабування системи в разі розширення діяльності підприємства або змін у його організаційній структурі.

Повна архітектура системи контролю доступу побудована за модульним принципом і передбачає чіткий розподіл функцій між ключовими компонентами. Центральним елементом є сервер автентифікації, який приймає запити на доступ та координує процес перевірки користувача (рис. 3.6).

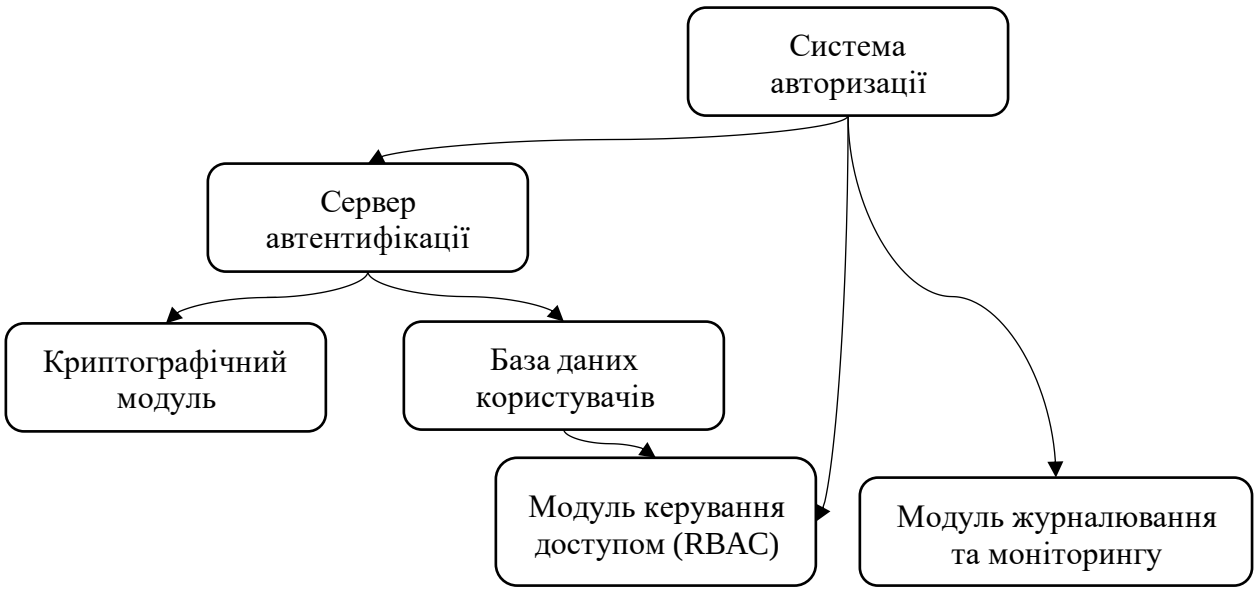

Рис. 3.6. Архітектура системи захисту доступу

У межах автентифікації сервер взаємодіє з криптографічним модулем, що відповідає за обробку облікових даних із використанням алгоритмів шифрування, а також із базою даних облікових записів, у якій зберігаються еталонні значення для перевірки.

Після успішного підтвердження особи ініціюється етап авторизації, під час якого формується інформація про права доступу користувача. Для цього використовується модуль RBAC, який визначає допустимі дії на основі призначеної ролі та забезпечує централізоване керування повноваженнями.

Усі події автентифікації та авторизації фіксуються в модулі журналювання та моніторингу, що дозволяє здійснювати контроль активності користувачів, аналіз безпекових подій і підтримувати аудит доступу до інформаційних ресурсів. Така архітектура забезпечує розмежування відповідальності між компонентами, підвищує керованість системи доступу та створює умови для її масштабування й подальшого вдосконалення.

Таким чином, сформована стратегія підвищення рівня інформаційної безпеки ТОВ «ВСЕ ДЛЯ ЛЮДЕЙ 2024» орієнтована на поєднання організаційних і технічних заходів захисту в умовах цифровізації бізнес-процесів. Запропонована програма ґрунтується на результатах аналізу поточного стану безпеки та спрямована на усунення ключових вразливостей, пов’язаних із контролем доступу до фінансової та облікової інформації. Реалізація багаторівневої системи автентифікації з використанням криптографічних механізмів і ролевої моделі керування доступом забезпечує підвищення керованості процесів безпеки, зменшення ризиків несанкціонованого доступу та створює надійну основу для подальшого розвитку системи управління інформаційною безпекою підприємства відповідно до масштабів його діяльності та стратегічних цілей.

3.3. Оцінювання результативності запропонованих заходів та напрями подальшого розвитку системи інформаційної безпеки

Реалізація комплексу заходів з підвищення рівня інформаційної безпеки має системний вплив на організаційну та операційну діяльність ТОВ «ВСЕ ДЛЯ ЛЮДЕЙ 2024». Насамперед це проявляється у зростанні керованості доступу до фінансової, облікової та управлінської інформації, що є критично важливою для стабільного функціонування торговельного підприємства з високою інтенсивністю інформаційних потоків.

Застосування багаторівневої системи авторизації дозволяє зменшити залежність захисту інформаційних ресурсів від одного автентифікаційного фактора та істотно обмежити ймовірність несанкціонованого доступу, зумовленого людськими помилками, використанням методів соціальної інженерії або компрометацією облікових даних. У результаті підвищується стійкість ключових цифрових бізнес-процесів і знижується ризик порушення безперервності операційної діяльності.

Для підприємства з відносно невеликою маржинальністю та значними обсягами обороту такий ефект є особливо важливим, оскільки навіть короткочасні збої в доступності або цілісності облікової інформації можуть призводити до порушень у процесах продажу, розрахунках із постачальниками та формуванні управлінської звітності. Посилення механізмів автентифікації у поєднанні з ролевим керуванням доступом мінімізує подібні ризики та сприяє стабільній роботі ключових бізнес-процесів.

З організаційної точки зору використання ролевої моделі керування доступом забезпечує впорядкування внутрішніх процедур роботи з інформаційними ресурсами. Для ТОВ «ВСЕ ДЛЯ ЛЮДЕЙ 2024» це означає чітке розмежування повноважень між працівниками відповідно до їх функціональних обов’язків, спрощення процесів надання та перегляду прав доступу, а також зменшення

ймовірності накопичення надлишкових або неконтрольованих повноважень. У підсумку підвищується прозорість управління доступом і знижується адміністративне навантаження на систему.

Разом із тим реалізація зазначених рішень потребує відповідних витрат, що зумовлює необхідність оцінювання їх економічної доцільності. Для ТОВ «ВСЕ ДЛЯ ЛЮДЕЙ 2024», як новоствореного підприємства, важливим є забезпечення раціонального співвідношення між обсягом фінансових ресурсів, спрямованих на інформаційну безпеку, та очікуваним ефектом у вигляді зниження рівня ризиків і підвищення стабільності діяльності.

Основні витрати, пов’язані з реалізацією багаторівневої системи авторизації та ролевого керування доступом, мають переважно організаційно-технічний характер і не потребують значних капітальних вкладень у апаратну інфраструктуру. Орієнтовна структура витрат на реалізацію заходів підвищення рівня інформаційної безпеки наведена в таблиці 3.4.

Таблиця 3.4

Орієнтовні витрати на реалізацію заходів підвищення інформаційної безпеки ТОВ «ВСЕ ДЛЯ ЛЮДЕЙ 2024»

Стаття витрат	Характер витрат	Орієнтовна сума, грн
Розроблення та налаштування багаторівневої системи авторизації	Одноразові	35 000
Налаштування ролевої моделі доступу (RBAC)	Одноразові	18 000
Інтеграція з обліковою системою UniproRetail	Одноразові	12 000
Організація журналювання та контролю подій безпеки	Одноразові	8 000
Навчання персоналу з питань інформаційної безпеки	Одноразові	7 000
Технічний супровід і підтримка (протягом року)	Поточні	10 000
Загальна орієнтовна сума витрат		90 000

Запропонований рівень витрат є помірним і відповідає фінансовим можливостям підприємства. З урахуванням раніше визначеного інтегрального рівня ризику інформаційної безпеки, який оцінюється приблизно у 100 000 грн на рік,

реалізація зазначених заходів дозволяє досягти економічно обґрунтованого ефекту у вигляді зменшення потенційних втрат від інцидентів інформаційної безпеки.

Узагальнюючи результати оцінювання, можна стверджувати, що запропонований комплекс рішень сприяє зниженню ймовірності несанкціонованого доступу до фінансової та облікової інформації, підвищенню керованості дій користувачів і формуванню відповідального ставлення персоналу до питань захисту інформації. У сукупності це позитивно впливає на стабільність бізнес-процесів та зменшує ризики порушення безперервності діяльності підприємства.

Таким чином, реалізація розробленої програми підвищення рівня інформаційної безпеки є доцільною як з організаційної, так і з економічної точки зору та створює надійну основу для подальшого розвитку системи управління інформаційною безпекою ТОВ «ВСЕ ДЛЯ ЛЮДЕЙ 2024» в умовах цифровізації бізнес-процесів.

Висновки до розділу 3

У третьому розділі сформовано практичну концепцію вдосконалення управління інформаційною безпекою організації в умовах цифрової трансформації на прикладі ТОВ «ВСЕ ДЛЯ ЛЮДЕЙ 2024». Окреслено специфіку діяльності підприємства та визначено ключові інформаційні активи, пов’язані з фінансами, обліком товарних запасів, договірною документацією, ціноутворенням і взаємодією з контрагентами, що в сукупності формують підвищені вимоги до захисту даних у середовищі інтенсивних інформаційних потоків і розгалуженої цифрової інфраструктури.

Проведено оцінювання поточного стану інформаційної безпеки за підходом зрілості процесів, що базується на рекомендаціях ISO/IEC 27000–27005 та практиках ISF. Отримані результати засвідчили початковий рівень сформованості

процесів із наявністю окремих елементів формалізації, водночас виявлено недостатню керованість у сферах аудиту, моніторингу подій, реагування на інциденти, антикризового управління та підвищення обізнаності персоналу. Підтверджено, що за таких умов збереження фрагментарних і переважно реактивних заходів створює ризики для безперервності облікових і торговельних процесів та фінансової стійкості підприємства.

У межах практичної частини виконано кількісне оцінювання ризику порушення захищеності фінансової та облікової інформації, що обробляється в UniproRetail і зберігається на внутрішніх серверних ресурсах. Визначено, що інтегральний рівень ризику є відчутним у співвідношенні з чистим прибутком підприємства, що обґрунтовує необхідність посилення контролю доступу, уніфікації правил роботи з даними та підвищення стійкості ключових ресурсів. Додатково ідентифіковано системні проблемні зони в управлінні доступом і обліковими записами, зокрема залежність від паролів як основного бар’єра, відсутність багаторівневої перевірки особи для критичних сервісів, обмежене логування, недосконале адміністрування облікових записів і нерівномірність застосування шифрування, що підсилює ризики фішингу, соціальної інженерії та несанкціонованого доступу.

На основі виявлених вразливостей сформовано стратегію та програму підвищення рівня інформаційної безпеки, зорієнтовану на поєднання організаційних і технічних заходів із урахуванням цифровізації бізнес-процесів і ресурсних обмежень новоствореного підприємства. Центральним напрямом визначено впровадження багаторівневої системи авторизації з використанням сучасних криптографічних механізмів, захищеного обміну даними та ролевого розмежування доступу RBAC, що забезпечує зниження ймовірності несанкціонованого доступу, підвищує керованість прав користувачів і створює умови для масштабування системи безпеки в разі розвитку підприємства. Запропонована модульна архітектура з виділенням сервера автентифікації,

криптографічного блоку, бази облікових записів, RBAC-модуля та підсистеми журналювання забезпечує прозорість контролю, підтримку аудиту доступу та можливість подальшого розширення засобів моніторингу.

Оцінено результативність і економічну доцільність запропонованих заходів, зокрема через зіставлення орієнтовних витрат на реалізацію програми з очікуваними втратами від інцидентів інформаційної безпеки. Показано, що запропонований рівень витрат має помірний характер, а впровадження багаторівневої автентифікації, RBAC і журналювання подій формує практичний ефект у вигляді зниження ймовірності інцидентів, підвищення стійкості ключових бізнес-процесів і зміцнення дисципліни доступу до критичних інформаційних ресурсів. Результати дослідження підтверджують, що впровадження програми є доцільним і забезпечує комплексний ефект, який охоплює організаційні та економічні складові, водночас формуючи основу для подальшого розвитку системи управління інформаційною безпекою в умовах цифрової трансформації.

ВИСНОВКИ

З урахуванням поставленої мети було розкрито теоретичні засади управління інформаційною безпекою в умовах цифрової трансформації як безперервного, ризик-орієнтованого управлінського процесу, що поєднує організаційні рішення, технічні засоби та нормативні вимоги. Обґрунтовано, що в цифровому середовищі захист інформації має забезпечувати не лише протидію окремим інцидентам, а й стійкість бізнес-процесів завдяки інтеграції безпекових процедур у систему менеджменту та регулярному перегляду ризиків відповідно до сучасних міжнародних підходів.

У межах виконання завдання щодо аналізу методів та інструментарію оцінювання стану інформаційної безпеки систематизовано підходи до діагностики ризиків і результативності захисту, які дозволяють отримувати порівнювані результати та формувати пріоритети реагування. Показано доцільність використання уніфікованих шкал і критеріїв для інтерпретації ризиків, а також застосування кількісних і напівкількісних оцінок на основі поєднання величини потенційних втрат і частоти реалізації загроз. Це забезпечує практичну придатність оцінювання для підприємств, які не мають великої історії інцидентів, але потребують обґрунтованих управлінських рішень.

Поточний рівень захищеності обраної організації було досліджено на прикладі ТОВ «ВСЕ ДЛЯ ЛЮДЕЙ 2024» з урахуванням масштабів діяльності та структури інформаційних активів. Зафіксовано, що за наявності значного обороту підприємство має відносно невеликий чистий прибуток, що підвищує чутливість до навіть одиничних інцидентів і робить питання захисту даних економічно критичним.

Результати прикладного оцінювання ризику для фінансової та облікової інформації показали інтегральне значення 123 246 грн, що становить близько 18 % чистого прибутку, тобто створює відчутну загрозу фінансовій стабільності та

підтверджує необхідність посилення організаційних і технічних заходів, насамперед у частині контролю доступу й керованості облікових записів.

Практичні рекомендації з удосконалення управління інформаційною безпекою сформовано з фокусом на усунення найбільш уразливих ланок доступу до критичних ресурсів. Запропоновано впровадження багаторівневої автентифікації із застосуванням криптографічної обробки облікових даних та ролевого розмежування прав доступу (RBAC), а також організацію журналювання і контролю подій безпеки та навчання персоналу. Такий комплекс рішень спрямований на зменшення імовірності несанкціонованого доступу, підвищення прозорості дій користувачів і зниження впливу людського фактора, що є типовим джерелом ризиків для торговельних підприємств.

Результативність запропонованих заходів оцінено з позицій організаційного ефекту та економічної доцільності. Показано, що орієнтовні витрати на реалізацію комплексу становлять 90 000 грн і є співставними з оцінюваним рівнем потенційних втрат від ризику, що підтверджує раціональність інвестицій у посилення контролю доступу та супровідних процедур.

У якості напрямів подальшого розвитку системи інформаційної безпеки визначено підвищення зрілості процесів реагування на інциденти, регулярного аудиту та моніторингу подій безпеки, формування сталих політик роботи з даними й розширення практик підготовки персоналу, що дозволить закріпити перехід від переважно реактивних дій до системного проактивного управління ризиками в умовах цифровізації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Андріяш В. Управління інформаційною безпекою : навч. посіб. – Київ : Вид-во НАУ, 2018. – 324 с.

2. Василенко С. А. Інноваційні технології в інформаційній безпеці // Вісник економічної науки України. – 2018. – № 2. – С. 142–145.

3. Верескун М. В. Методичне забезпечення системи інформаційної безпеки промислових підприємств / М. В. Верескун // Економіка і організація управління. – 2014. – Вип. 1-2. – С. 54-60.

4. Воронін Д. В. Ризик-орієнтований підхід в управлінні інформаційною безпекою: міжнародні стандарти та український досвід // Інформаційні технології та захист інформації. – 2020. – № 4(20). – С. 77–85.

5. Герасименко О. В. Інформаційна безпека підприємства: поняття та методи її забезпечення / О. В. Герасименко, А. В. Козак // 2015. – № 2.

6. Гладченко, Т. М. Індикатори економічної безпеки підприємницької діяльності. Донецьк: ДонДАУ. Менеджер. 2000. №12. С.111-113.

7. Господарський кодекс України // Відомості Верховної Ради України. 2003. № 18, № 19–20, № 21–22. Ст. 144. URL: https://zakon.rada.gov.ua/laws/show/436-15#Text (дата звернення: 06.12.2025).

8. Гусєв А. В. Інформаційна безпека: сучасні виклики та загрози // Інформаційна безпека. – 2019. – № 4. – С. 21–27.

9. Дейнега О. Інформаційна безпека підприємств в умовах глобалізації / О. Дейнега // Економіка та суспільство. – 2019. – Вип. 20. – С. 70–79.

10. Дробот О. В. Інформаційні ризики та методи їх аналізу : навч. посіб. – Київ : Талком, 2019. – 340 с.

11. Дубина М. М. Методи захисту інформації в умовах цифрової трансформації // Економіка і прогнозування. – 2019. – № 2. – С. 38–44.

12. Дячков Д. В. Формування моделі політики інформаційної безпеки на основі концепції «глибинного захисту» // Підприємництво і торгівля. – 2019. – № 25. – С. 116–121.

13. Єфименко В. В. Забезпечення інформаційної безпеки в умовах глобалізації // Проблеми економіки. – 2020. – № 7. – С. 123–127.

14. Забродський, В. А., Кізім, Н. А., Янов, Л. І. Сучасні методи організації та управління промисловим виробництвом. Харків: АТ «Бізнес-Інформ», 1997. 64.

15. Закон України «Про захист інформації в інформаційно-комунікаційних системах» // Відомості Верховної Ради України. 1994. № 31. Ст. 286. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 06.12.2025).

16. Закон України «Про захист персональних даних» // Відомості Верховної Ради України. 2010. № 34. Ст. 481. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 06.12.2025).

17. Закон України «Про інформацію» // Відомості Верховної Ради України. 1992. № 48. Ст. 650. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 06.12.2025).

18. Закон України «Про основні засади забезпечення кібербезпеки України» // Відомості Верховної Ради України. 2017. № 45. Ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 06.12.2025).

19. Закон України «Про телекомунікації» № 1089-IX від 16.12.2020. ВВР 2020.

20. Інформаційна безпека. Підручник. Під ред. В.В. Остроухова. К.: Видавництво Ліра-К, 2021. 412 с.

21. Камлик, М. І. Економічна безпека підприємницької діяльності. Економіко-правовий аспект [Текст] : навч. посіб. К. : Атіка, 2005. 432 с.

22. Кириченко О. В. Роль людського фактора в інформаційній безпеці // Інформаційні технології і засоби навчання. – 2019. – № 1. – С. 35–40.

23. Клименко О. А. Методи оцінки ризиків інформаційної безпеки підприємства // Вісник НАУ. – 2018. – № 3. – С. 34–41.

24. Козак В. І. Інформаційна безпека: проблеми та перспективи // Вісник Київського національного університету технологій та дизайну. – 2022. – № 2. – С. 23–28.

25. Козачок В. А., Гайдур, Г. І., Гахов, С. О., Хмелевський, Р. М., Чумак, Н. С. Політики безпеки. Навчальний посібник для студентів вищих навчальних закладів. Київ: ДУТ ННІЗІ, 2020.167 с.

26. Концепція інформаційної безпеки України. URL: https://www.osce.org/sites/default/files/f/documents/0/2/175056.pdf (дата звернення: 06.12.2025).

27. Костюченко В. В. Особливості організації інформаційної безпеки сучасної інформаційної системи та її економічна доцільність / В. В. Костюченко, К. О. Шиковець // Економіка і суспільство. – 2017. – № 10. – С. 89-93.

28. Кравченко Н. М. Інформаційна безпека в умовах цифрової трансформації // Економічний аналіз. – 2021. – № 6. – С. 75–81.

29. Краснова М. В. Основи оцінки ризиків інформаційної безпеки : навч. посіб. – Київ : Алерта, 2020. – 216 с.

30. Кримінальний кодекс України // Відомості Верховної Ради України. 2001. № 25–26. Ст. 131. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 06.12.2025).

31. Лекція «Ризик як оцінка, оцінка як необхідність» (2014). URL: https://surl.li/qhmsls (дата звернення: 06.12.2025).

32. Литвиненко А. О. Інформаційна безпека як складовий елемент системи економічної безпеки суб’єкта підприємництва / А. О. Литвиненко, Є. М. Іполітов // Стратегічні пріоритети розвитку підприємництва, торгівлі та біржової діяльності : матеріали IV Міжнар. наук.-практ. конф., 10–11 травня 2023 р. – Запоріжжя, 2023. – С. 74–75.

33. Маркіна І. А. Інформаційна безпека підприємства та організаційні заходи її забезпечення / І. А. Маркіна, Ю. М. Гарічев // Український журнал прикладної економіки. – 2019. – Т. 4. – № 4. – С. 209–215.

34. Маркіна І. А. Основи формування системи менеджменту інформаційної безпеки підприємства / І. А. Маркіна, Д. В. Дячков // Проблеми і перспективи розвитку підприємництва. – 2016. – № 3(1). – С. 80–88.

35. Мельник М. О. Аналіз побудови моделі політики інформаційної безпеки підприємства // Системи обробки інформації. – 2017. – Вип. 2(148). – С. 126–128.

36. Михайлова Л. В. Стратегії управління інформаційною безпекою в умовах глобалізації // Вісник економіки транспорту і промисловості. – 2020. – № 6. – С. 132–137.

37. Могильний, А. І., Безчастний, В. М., Винокуров, Ю. О. Основи безпеки бізнесу. Донецьк: Регіон, 2000. 130 с.

38. Ніколаюк, С. І., Никифорчук, Д. Й. Безпека суб'єктів підприємницької діяльності [Текст] курс лекцій К. : КНТ, 2005. 320 с.

39. Олійник, О. В. Принципи забезпечення інформаційної безпеки України. Науковий вісник Ужгородського університету. 2012. Випуск 18. С. 170-173.

40. Онищенко С.В. Управління інформаційною безпекою стратегічно важливих підприємств в умовах викликів й загроз / С.В. Онищенко, О.П. Ківшик // Економіка і регіон. – 2022. – № 3 (86). – С. 80-85. DOI: https://doi.org/10.26906/EiR.2022.3(86).2817. (дата звернення: 06.12.2025).

41. Остроухов В.В. Інформаційна безпека: Підручни. Київ: Ліра-К, 2021. – 412 с.

42. Панченко В. Управління інформаційною безпекою держави та підприємств: правові та організаційні аспекти / В. Панченко // Актуальні проблеми правознавства. – 2020. – № 1 (21). – С. 103-109.

43. Попов О. А. Моделі управління ризиками інформаційної безпеки // Економічний часопис. – 2021. – № 15. – С. 65–70.

44. Романюк А. Управління ризиками інформаційних технологій : монографія. – Львів : Тріада плюс, 2020. – 392 с.

45. Савельєва Т. В. Аналіз методів і засобів реалізації ризик-орієнтованого підходу в контексті забезпечення інформаційної безпеки підприємства / Т. В. Савельєва, О. М. Панаско, О. М. Пригодюк // Вісник Черкаського державного технологічного університету. Серія: Технічні науки. – 2018. – № 1. – С. 81–88.

46. Соколова А. П. Інформаційна безпека в умовах цифрової трансформації // Вісник Київського національного торговельно-економічного університету. – 2020. – № 19. – С. 98–103.

47. Супрун І. В. Інформаційна безпека: сучасні виклики та технології // Вісник Чернігівського державного технологічного університету. – 2022. – № 21. – С. 113–118.

48. Терещенко М. І. Управління інформаційною безпекою: теорія та практика // Науковий вісник Одеського національного економічного університету. – 2019. – № 22. – С. 84–89.

49. ТОВ «ВСЕ ДЛЯ ЛЮДЕЙ 2024» : інформація про діяльність підприємства. URL: https://opendatabot.ua/c/45580200 (дата звернення: 06.12.2025).

50. Цивільний кодекс України // Відомості Верховної Ради України. 2003. №№ 40–44. Ст. 356. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text (дата звернення: 06.12.2025).

51. Шевчук В. В. Методики проведення ризик-аналізу інформаційних систем / В. В. Шевчук, М. Ю. Гончаренко // Кібербезпека та захист інформації. – 2021. – № 2(8). – С. 56–65.

52. Шульга, В. І. Сучасні підходи до трактування поняття інформаційна безпека. Ефективна економіка № 4, 2015. Режим доступу: http://www.economy.nayka.com.ua/?op=1&z=5514 (дата звернення: 06.12.2025).

53. Якименко, Ю. М., Савченко, В. А., Легомінова, С. В. Системний аналіз інформаційної безпеки: сучасні методи управління: підручник. Київ: Державний університет телекомунікацій, 2022. 308 с.

54. Information security management – definition & overview// URL: https://www.sumologic.com/glossary/information-security-management. (дата звернення: 06.12.2025).

55. ISO 31000:2018 Risk management – Guidelines. – International Organization for Standardization, 2018. URL: https://zakon.isu.net.ua/sites/default/files/normdocs/dstu_iso_31000_2018.pdf (дата звернення: 06.12.2025).

56. ISO/IEC 27001:2022. URL: https://www.iso.org/ru/standard/27001 (дата звернення: 06.12.2025).

57. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls. – International Organization for Standardization/International Electrotechnical Commission, 2022. URL: https://www.iso.org/ru/standard/75652.html (дата звернення: 06.12.2025).

58. ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection – Guidance on information security risk management. – International Organization for Standardization/International Electrotechnical Commission, 2022. URL: https://www.karlancer.com/api/file/1683114859-CH6u.pdf (дата звернення: 06.12.2025).

59. National Institute of Standards and Technology (NIST). Special Publications 800 Series. URL: https://csrc.nist.gov/publications/sp800 (дата звернення: 06.12.2025).

60. What is Information Security Management? URL: https://www.checkpoint.com/cyber-hub/network-security/what-is-security-management/what-is-information-security-management (дата звернення: 06.12.2025).

ДОДАТКИ

Додаток А

Таблиця А.1

Порівняльна характеристика міжнародних стандартів управління ризиками інформаційної безпеки

Характеристика	ISO/IEC 27005:2022 – управління ризиками ІБ	ISO 31000:2018 – менеджмент ризиків	ISO/IEC 27001:2022 – система управління ІБ
Статус документа	Настановчий стандарт (guidance), рекомендаційний, не передбачає сертифікації	Настановчий стандарт (guidelines) загального призначення	Нормативний стандарт (requirements), містить обов'язкові вимоги, сертифікаційний
Сфера застосування	Управління ризиками інформаційної безпеки в організаціях, що впроваджують або підтримують СУІБ	Універсальний – застосовується до будь-яких видів ризиків (фінансових, операційних, безпекових тощо)	Побудова, впровадження, функціонування та підтримка системи управління інформаційною безпекою
Основна мета та фокус	Надання детальних рекомендацій щодо ідентифікації, аналізу та обробки ризиків ІБ; методична підтримка виконання вимог ISO/IEC 27001	Формування принципів ефективного управління ризиками, рамкової структури та процесу прийняття рішень в умовах невизначеності	Встановлення вимог до процесів управління інформаційною безпекою, включно з управлінням ризиками, у межах комплексного захисту інформаційних активів
Підхід до управління ризиками	Ітеративний процес управління ризиками ІБ, узгоджений з ISO 31000; використання сценаріїв ризику, підходів на основі активів або подій	Системний і безперервний процес управління ризиками: встановлення контексту, ідентифікація, аналіз, оцінювання, реагування та моніторинг	Управління ризиками визначено на рівні обов'язкових вимог: встановлення критеріїв ризику, регулярна оцінка, планування та реалізація заходів обробки ризиків
Гнучкість методів оцінювання	Дозволяє застосування різних підходів і методик оцінки ризиків залежно від контексту організації	Не регламентує конкретні методи, орієнтуючись на принципи та інтеграцію в систему управління	Не встановлює конкретної методики оцінювання, але вимагає досягнення визначених критеріїв прийнятності ризиків

Продовження табл. А.1

Взаємозв'язок з іншими стандартами	Доповнює ISO/IEC 27001 (роз'яснює виконання вимог щодо ризиків) та узгоджується з принципами ISO 31000	Є базовим високорівневим стандартом, на основі якого розроблено галузеві документи, зокрема ISO/IEC 27005	Є центральним елементом сімейства ISO/IEC 27000; використовує ISO/IEC 27002, ISO/IEC 27005 та інші супровідні стандарти
Статус впровадження в Україні	Прийнятий як ДСТУ ISO/IEC 27005:2023 (ідентичний переклад)	Прийнятий як ДСТУ ISO 31000:2018	В Україні чинною є версія ДСТУ ISO/IEC 27001:2015; редакція 2022 року перебуває на етапі впровадження