Міністерство освіти і науки України

Одеський національний технологічний університет

Кафедра економічної безпеки, права та соціальних процесів

КВАЛІФІКАЦІЙНА РОБОТА

на тему*: «*Інформаційна безпека як фактор забезпечення економічної стійкості суб'єктів господарювання»

ШИФР ЕБПтаСП.1.599.03-2.2

Здобувач _____ Мальцев Вячеслав Сергійович
4 курсу ФЕБ-313с
Керівник _____ к.ю.н., доц. Шишлюк В.Р.

Кваліфікаційна робота допускається до захисту
Рішення кафедри від «09» червня 2026 р., протокол № 11

Завідувачка кафедри економічної безпеки,
права та соціальних процесів _____к.е.н., доц. Згадова Н.С.

Одеса-2026

ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

ННІ економіки, управління і бізнесу ім. Г. Е. Вейнштейна
Кафедра економічної безпеки, права та соціальних процесів
Ступінь вищої освіти – перший (бакалавр)
Спеціальність *051 «Економіка»*
Освітня програма *«Економічна та продовольча безпека»*

ЗАТВЕРДЖУЮ

«___»_____2025р.

_____

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧА

Мальцева Вячеслава Сергійовича

1. Тема роботи: «Інформаційна безпека як фактор забезпечення економічної стійкості суб'єктів господарювання», затверджена наказом від 30.10.2025 р. № 599-03.

2. Термін здачі здобувачем закінченої роботи 12 червня 2026 р. Вихідні дані до роботи: звітні дані про діяльність підприємств.

3. Перелік питань, які потрібно розробити: Теоретичні основи формування інформаційної безпеки в контексті економічної безпеки підприємства. Сучасні загрози інформаційній безпеці в контексті економічної безпеки підприємств. Система стратегічного забезпечення інформаційної безпеки як складова економічної безпеки підприємства. Висновки та пропозиції.

4. Перелік графічного матеріалу: таблиць – 7

5. Дата видачі завдання 30 жовтня 2025 року.

Керівник_____ к.ю.н., доц. Шишлюк В.Р.

Завдання прийняв до виконання _____ Мальцев В. С.

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Вибір теми, обґрунтування її актуальності і призначення наукового керівника кваліфікаційної роботи	30.10.2025 – 06.12.2025	Виконано
2	Отримання завдання на проведення наукового дослідження та підготовка календарного плану виконання кваліфікаційної роботи, затвердження його керівником	07.12.2025 – 24.12.25	Виконано
3	Збір та узагальнення статистичного матеріалу за темою роботи.	25.12.2025 – 25.01.26	Виконано
4	Написання розділу 1. Теоретичні основи формування інформаційної безпеки в контексті економічної безпеки підприємства.	27.01.2026 – 27.02.26	Виконано
5	Написання розділу 2. Сучасні загрози інформаційній безпеці в контексті економічної безпеки підприємств.	28.02.2026 – 30.03.26	Виконано
6	Написання розділу 3. Система стратегічного забезпечення інформаційної безпеки як складова економічної безпеки підприємства	01.05.2026 – 22.05.26	Виконано
7	Подання роботи на перевірку науковому керівникові та доопрацювання тексту роботи і висновків. Завершення оформлення роботи та розробка висновків і пропозицій	25.05.2026 – 02.06.26	Виконано
9	Оформлення кваліфікаційної роботи	03.06.2026 – 05.06.26	Виконано
10	Перевірка роботи на плагіат. Підготовка до захисту кваліфікаційної роботи на засіданні Екзаменаційної комісії: доповідь, демонстраційні матеріали, попередній захист, подання текстової і графічної частини роботи до е-архіву кафедри та університету	12.06.2026	Виконано
11	Захист кваліфікаційної роботи згідно затвердженого графіку роботи ЕК спеціальності 051 «Економіка»	22.06.2026	Виконано

Здобувач_____ Мальцев В. С.

Керівник роботи_____ к.ю.н., доц. Шишлюк

Несу відповідальність за ідентичність електронного та друкованого варіантів кваліфікаційної роботи, даю згоду на обробку персональних даних та не заперечую проти розміщення кваліфікаційної роботи на офіційних web-ресурсах ОНТУ.

Підтверджую, що в кваліфікаційній роботі відсутні порушення норм академічної доброчесності.

Здобувач-дипломник_____ Мальцев В. С.

АНОТАЦІЯ

кваліфікаційної роботи бакалавра ***Мальцева Вячеслава Сергійовича***

«Інформаційна безпека як фактор забезпечення економічної стійкості суб'єктів господарювання»

Мета дослідження – здійснення комплексного теоретичного та практичного аналізу інформаційної безпеки як складової економічної безпеки суб'єктів господарювання, визначення її ролі у забезпеченні стабільного функціонування підприємства та розроблення практичних рекомендацій щодо вдосконалення механізмів захисту інформаційних ресурсів.

Кваліфікаційна робота складається з трьох розділів.

У першому розділі розкрито теоретичні та методологічні засади інформаційної безпеки у структурі економічної безпеки суб'єктів господарювання. Досліджено сутність інформаційної безпеки, її основні складові, принципи та механізми забезпечення, а також визначено місце інформаційної безпеки в системі економічної безпеки підприємства.

У другому розділі проведено аналіз сучасних загроз інформаційній безпеці підприємств та їх впливу на рівень економічної безпеки суб'єктів господарювання.

У третьому розділі розроблено практичні рекомендації щодо вдосконалення системи інформаційної безпеки у структурі економічної безпеки суб'єктів господарювання. Запропоновано заходи щодо підвищення ефективності управління інформаційними ризиками.

У висновках узагальнено результати дослідження та сформульовано авторські пропозиції щодо підвищення рівня захищеності інформаційних ресурсів підприємства.

Кваліфікаційна робота містить: текстової частини – 70 стор., 6 таблиць.

Ключові слова: інформаційна безпека, економічна безпека, суб'єкти господарювання, інформаційні ресурси, кібербезпека, кіберзагрози, інформаційні ризики, захист інформації, управління ризиками, цифрова трансформація.

ABSTRACT

of the Bachelor's Qualification Thesis by ***Viacheslav Maltsev***

« Information security as a factor in ensuring the economic stability of business entities »

The purpose of the study is to conduct a comprehensive theoretical and practical analysis of information security as a component of the economic security of business entities, to determine its role in ensuring the stable functioning of an enterprise, and to develop practical recommendations for improving mechanisms for the protection of information resources.

The qualification thesis consists of three chapters.

The first chapter reveals the theoretical and methodological foundations of information security within the structure of the economic security of business entities. The essence of information security, its main components, principles, and mechanisms are investigated, and the place of information security within the enterprise economic security system is determined.

The second chapter analyzes contemporary threats to enterprise information security and their impact on the level of economic security of business entities.

The third chapter develops practical recommendations for improving the information security system within the structure of the economic security of business entities. Measures aimed at enhancing the effectiveness of information risk management are proposed.

The conclusions summarize the results of the research and present the author's recommendations for increasing the level of protection of enterprise information resources.

The qualification thesis contains: 70 pages of text and 6 tables.

Keywords: information security, economic security, business entities, information resources, cybersecurity, cyber threats, information risks, information protection, risk management, digital transformation.

ЗМІСТ

ВСТУП

Актуальність теми дослідження. У сучасних умовах цифрової трансформації економіки, розвитку інформаційно-комунікаційних технологій та глобалізації бізнес-процесів інформація перетворилася на один із найцінніших ресурсів суб'єктів господарювання. Ефективність функціонування підприємств, їх конкурентоспроможність, фінансова стійкість та здатність до розвитку значною мірою залежать від рівня захищеності інформаційних ресурсів, інформаційних систем і технологій. У зв'язку з цим інформаційна безпека набуває особливого значення як невід'ємна складова системи економічної безпеки підприємства.

Особливої актуальності дослідження набуває в умовах воєнного стану в Україні, коли суттєво зростає кількість кіберзагроз, інформаційних атак, спроб несанкціонованого доступу до корпоративних інформаційних систем та випадків витоку конфіденційної інформації.

Водночас процеси цифровізації бізнесу, автоматизації управлінських процесів, впровадження хмарних технологій, систем електронного документообігу та штучного інтелекту створюють не лише нові можливості для підвищення ефективності діяльності підприємств, але й формують додаткові ризики для їх економічної безпеки. Зростання залежності від інформаційної інфраструктури обумовлює необхідність розроблення ефективних механізмів захисту інформаційних активів, управління інформаційними ризиками та забезпечення безперервності бізнес-процесів.

Аналіз наукових досліджень свідчить, що економічна безпека підприємства є складною багаторівневою системою, яка включає фінансову, кадрову, техніко-технологічну, правову, екологічну, силову та інформаційну складові. При цьому саме інформаційна безпека забезпечує належний рівень захищеності інформаційних ресурсів підприємства, підтримує стабільність управлінських процесів та сприяє прийняттю ефективних управлінських рішень. Незважаючи на значну кількість наукових праць, присвячених питанням економічної та інформаційної безпеки, потребують подальшого

дослідження теоретичні та практичні аспекти визначення місця інформаційної безпеки у структурі економічної безпеки суб'єктів господарювання, а також механізми її забезпечення в умовах зростання кіберзагроз.

Таким чином, дослідження інформаційної безпеки як складової економічної безпеки суб'єктів господарювання є актуальним як з наукової, так і з практичної точки зору, оскільки спрямоване на пошук ефективних інструментів захисту інформаційних ресурсів, підвищення стійкості підприємств до інформаційних загроз та забезпечення їх стабільного розвитку в сучасному цифровому середовищі.

Мета та завдання дослідження. Метою кваліфікаційної роботи є комплексне дослідження теоретичних та практичних аспектів інформаційної безпеки у структурі економічної безпеки суб'єктів господарювання, визначення її ролі у забезпеченні стабільного функціонування підприємства та розроблення рекомендацій щодо вдосконалення механізмів захисту інформаційних ресурсів.

Для досягнення поставленої мети в роботі передбачено розв'язання таких завдань:

– дослідити теоретичні підходи до визначення сутності інформаційної безпеки підприємства;

– розкрити зміст та основні складові інформаційної безпеки суб'єктів господарювання;

– визначити місце інформаційної безпеки у структурі економічної безпеки підприємства;

– узагальнити наукові підходи до класифікації інформаційних загроз та ризиків;

– дослідити організаційно-економічні механізми забезпечення інформаційної безпеки підприємства;

– проаналізувати сучасні загрози інформаційній безпеці суб'єктів господарювання;

– здійснити оцінку впливу інформаційних загроз на рівень економічної безпеки підприємства;

– визначити основні напрями вдосконалення системи інформаційної безпеки в структурі економічної безпеки суб'єктів господарювання;

– розробити практичні рекомендації щодо підвищення ефективності управління інформаційними ризиками на підприємстві.

Об'єкт дослідження – система економічної безпеки суб'єктів господарювання.

Предмет дослідження – теоретичні, організаційно-економічні та практичні аспекти забезпечення інформаційної безпеки як складової економічної безпеки суб'єктів господарювання.

Методи дослідження. У процесі виконання кваліфікаційної роботи використано комплекс загальнонаукових і спеціальних методів дослідження, зокрема: діалектичний метод – для дослідження сутності інформаційної та економічної безпеки; системний підхід – для визначення місця інформаційної безпеки у структурі економічної безпеки підприємства; методи аналізу і синтезу – для узагальнення наукових підходів та теоретичних положень; порівняльний аналіз – для дослідження сучасних механізмів забезпечення інформаційної безпеки; економіко-статистичні методи – для аналізу впливу інформаційних загроз на діяльність підприємств; графічно-аналітичні методи – для наочного відображення результатів дослідження; метод узагальнення – для формування висновків та практичних рекомендацій.

Теоретичною та інформаційною основою дослідження є праці вітчизняних і зарубіжних учених з питань економічної та інформаційної безпеки підприємств, серед яких такі науковці як Близнюк І. М., Братель О. Р., Бондаренко В. О., Бучило І. Л., Горбатюк О. М., Гуцалюк М. О., Ляшенко О. М., Камлик М. І., Козаченко Г. В., Остроухов В. В., Пономарьов В. П., Стрельцов А. А., Расторгуев С. П., Цимбалюк В. Л., Чубарук Т. І., Щербина В. М. та багатьох інших. Однак, незважаючи на значну кількість наукових

праць, інформаційна безпека як складова економічної безпеки підприємств залишається недостатньо дослідженою.

Наукова новизна дослідження полягає в обґрунтуванні ролі інформаційної безпеки як ключової складової економічної безпеки суб'єктів господарювання та розробленні практичних рекомендацій щодо вдосконалення механізмів захисту інформаційних ресурсів в умовах цифровізації економіки та зростання кіберзагроз.

Практичне значення отриманих результатів полягає в можливості використання розроблених рекомендацій у діяльності суб'єктів господарювання для підвищення рівня захищеності інформаційних ресурсів, мінімізації інформаційних ризиків, удосконалення системи економічної безпеки та забезпечення стабільного функціонування підприємства в умовах цифрового середовища.

Апробація результатів дослідження. Основні положення та результати кваліфікаційної роботи були апробовані у наукових доповідях та опубліковані у матеріалах студентських науково-практичних конференцій.

Мальцев В. С. Місце інформаційної безпеки в системі економічної безпеки підприємства. Наукова конференція здобувачів вищої освіти ОНТУ. 24-27 березня 2026 року. Одеса: Одеський національний технологічний університет.

Мальцев В. С. Місце інформаційної безпеки в системі економічної безпеки підприємства. Актуальні аспекти соціально-економічного розвитку України: погляд молоді. Матеріали VIII Всеукраїнської студентської науково-практичної конференції 16-17 квітня 2026 року. Одеса: Одеський національний технологічний університет, 2026. С. 703-705.

Структура кваліфікаційної роботи. Кваліфікаційна робота складається зі вступу, трьох розділів, що включають вісім підрозділів, висновків, списку використаних джерел та додатків.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ФОРМУВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КОНТЕКСТІ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

1.1. Теоретичне визначення та сутнісна характеристика інформаційної безпеки підприємства

В умовах сучасного соціально-економічного розвитку України, що характеризується високим рівнем нестабільності зовнішнього та внутрішнього середовища, суб'єкти господарювання змушені формувати адаптивні стратегії забезпечення економічної стійкості, значною мірою спираючись на використання інформаційних технологій. Інформаційні технології сьогодні виступають одним із ключових факторів підвищення конкурентоспроможності підприємств, забезпечуючи прискорення інформаційного обміну, оптимізацію управлінських процесів та розширення можливостей прийняття ефективних рішень. Водночас їх активне впровадження супроводжується появою нових загроз, які безпосередньо впливають на рівень економічної безпеки підприємств та можуть спричиняти зниження стабільності їх фінансово-економічної діяльності.

Інформація в сучасних умовах трансформувалася з допоміжного ресурсу управління у стратегічний актив підприємства та інструмент конкурентної боротьби. Володіння достовірною та своєчасною інформацією забезпечує суб'єктам господарювання не лише отримання економічних переваг, але й формування довгострокової стійкості розвитку. Це підтверджує загальновизнане положення: «Хто володіє інформацією, той володіє світом». За таких умов захист інформаційної складової економічної безпеки набуває критичного значення для забезпечення стабільного функціонування підприємств.

У зв'язку з цим дедалі більше суб'єктів господарювання впроваджують комплексні корпоративні системи інформаційної безпеки як елемент загальної системи економічної безпеки. Основною метою таких систем є

захист інформаційних ресурсів підприємства від несанкціонованого доступу, витоку, модифікації або знищення, а також мінімізація впливу загроз, що можуть негативно впливати на економічну стійкість організації.

Ефективна система інформаційної безпеки має забезпечувати зниження рівня інформаційних ризиків при оптимальних витратах на її впровадження та функціонування, а також володіти достатнім рівнем гнучкості для адаптації до змін зовнішнього та внутрішнього середовища підприємства.

Інформаційна безпека є багатогранною економіко-управлінською категорією, що охоплює сукупність організаційних, технічних і правових заходів, спрямованих на захист інформації, яка створюється, зберігається, обробляється та передається в межах діяльності підприємства, від внутрішніх і зовнішніх загроз. З огляду на те, що інформація виступає стратегічним ресурсом, її порушення або компрометація можуть призвести до суттєвих фінансових, репутаційних та правових втрат, що безпосередньо впливають на рівень економічної безпеки суб’єкта господарювання.

У науковій літературі існують різні підходи до трактування сутності інформаційної безпеки підприємства. Так, за визначенням українського науковця О. В. Антонюка, інформаційна безпека підприємства розглядається як стан захищеності інформаційних ресурсів, що забезпечує їх цілісність, конфіденційність і доступність під час зберігання, обробки та передачі [1]. Дане трактування акцентує увагу на базових властивостях інформації, порушення яких створює прямі ризики для стабільності функціонування підприємства та його економічної безпеки.

Інший підхід запропонований В. В. Шереметом, який розглядає інформаційну безпеку не лише з технічної, але й з організаційно-управлінської точки зору. На його думку, інформаційна безпека є сукупністю політик, процедур і технічних рішень, спрямованих на мінімізацію ризиків несанкціонованого доступу, витоку або зміни інформації, що використовується підприємством [2]. Такий підхід підкреслює необхідність

комплексного управління інформаційними ризиками в системі економічної безпеки суб’єктів господарювання.

Міжнародні стандарти, зокрема ISO/IEC 27001, також пропонують системне трактування інформаційної безпеки, відповідно до якого вона охоплює процеси управління ризиками, пов’язаними з конфіденційністю, цілісністю та доступністю інформації, та спрямована на забезпечення стійкого функціонування інформаційних систем підприємства [3]. Такий підхід базується на формалізованих процедурах управління безпекою, що дозволяє інтегрувати інформаційну безпеку в загальну систему економічної безпеки підприємства.

Як зазначалося вище, інформаційна безпека як складова економічної безпеки суб’єктів господарювання базується на трьох фундаментальних характеристиках: конфіденційності, цілісності та доступності інформації.

1. Конфіденційність передбачає забезпечення доступу до інформаційних ресурсів виключно уповноваженим особам, яким надано відповідні права доступу. Реалізація цього принципу здійснюється шляхом застосування механізмів автентифікації користувачів, систем управління доступом, а також криптографічного захисту даних.

У наукових дослідженнях Л. С. Грищенко підкреслюється, що конфіденційність інформації виступає базовою умовою забезпечення економічної безпеки підприємства. Недотримання вимог конфіденційності підвищує ризик витоку стратегічно важливих даних, що може призвести до втрати конкурентних переваг та погіршення ринкових позицій суб’єкта господарювання [4].

2. Цілісність означає властивість інформації зберігати свою точність, повноту та незмінність у процесі її зберігання, обробки та передачі. Забезпечення цілісності реалізується через використання механізмів контролю змін, цифрового підпису, журналювання операцій та інших засобів захисту від несанкціонованого втручання.

Як зазначає А. В. Гончаров, саме цілісність інформації є критично важливою умовою прийняття обґрунтованих управлінських рішень на підприємстві. Використання недостовірних або спотворених даних може призвести до помилкових управлінських рішень, що негативно впливає на фінансово-економічні результати діяльності підприємства [5].

3. Доступність характеризує можливість уповноважених користувачів отримувати необхідну інформацію у визначений час. Важливими елементами забезпечення доступності є резервне копіювання, системи відновлення даних та забезпечення безперервності функціонування інформаційних систем.

Відповідно до досліджень І. В. Довгань, порушення доступності інформаційних ресурсів, зокрема внаслідок кібератак типу DDoS, може призводити до суттєвих фінансових втрат та тимчасового або повного припинення діяльності підприємства [6].

З урахуванням зазначених характеристик, забезпечення інформаційної безпеки в системі економічної безпеки підприємства передбачає комплексне застосування технічних, організаційних та правових заходів.

До технічних заходів належать програмно-апаратні засоби захисту інформації, зокрема міжмережеві екрани, системи виявлення та запобігання вторгненням, засоби криптографічного захисту, резервного копіювання та моніторингу інформаційних систем.

Організаційні заходи охоплюють формування внутрішніх політик інформаційної безпеки, регламентацію доступу до інформаційних ресурсів, розподіл повноважень користувачів та впровадження процедур контролю інформаційних потоків на підприємстві.

Правові заходи передбачають дотримання норм національного та міжнародного законодавства у сфері захисту інформації, включаючи положення щодо захисту персональних даних та вимоги відповідних стандартів інформаційної безпеки (зокрема GDPR у разі роботи з даними громадян ЄС).

Водночас забезпечення інформаційної безпеки суб’єктів господарювання супроводжується низкою проблем і викликів. Насамперед, це зростання кіберзагроз, оскільки сучасні атаки стають дедалі складнішими та більш цілеспрямованими. Як зазначає Є. М. Ковальчук, поширення шкідливого програмного забезпечення, фішингових атак та експлойтів істотно підвищує ризики порушення інформаційної безпеки підприємств [7].

Другою суттєвою проблемою є нестача кваліфікованих кадрів у сфері кібербезпеки, що ускладнює формування ефективної системи захисту інформаційних ресурсів.

Крім того, значним обмежувальним фактором виступає фінансове забезпечення, оскільки впровадження сучасних комплексних рішень інформаційної безпеки потребує значних інвестицій, які не завжди є доступними для підприємств різного масштабу.

Таким чином, інформаційна безпека як складова економічної безпеки суб’єктів господарювання охоплює не лише технічні аспекти захисту даних, але й організаційні та правові механізми їхнього забезпечення. Її головною метою є гарантування конфіденційності, цілісності та доступності інформаційних ресурсів, що є критично важливими для стабільного функціонування підприємства. З огляду на зростання кіберзагроз та ускладнення інформаційного середовища, інформаційна безпека набуває статусу одного з ключових елементів системи економічної безпеки суб’єктів господарювання.

Для забезпечення належного рівня інформаційної безпеки в системі економічної безпеки суб’єктів господарювання важливим є дотримання міжнародних стандартів і практик. Одним із найбільш поширених є стандарт ISO/IEC 27001, який встановлює вимоги до системи управління інформаційною безпекою (ISMS). Його застосування дозволяє підприємствам формувати, впроваджувати, підтримувати та постійно вдосконалювати комплексну систему захисту інформаційних ресурсів [6].

Важливе значення має також NIST Cybersecurity Framework, який пропонує структурований і комплексний підхід до управління кіберризиками на підприємстві. Як зазначається у дослідженні І. В. Довгань, впровадження зазначених міжнародних стандартів сприяє суттєвому зниженню рівня кіберзагроз та підвищенню стійкості суб'єктів господарювання до зовнішніх і внутрішніх кібератак [7].

Одним із ключових викликів сучасного етапу розвитку інформаційної безпеки є постійна еволюція технологій та відповідне ускладнення кіберзагроз. Це зумовлює необхідність безперервного вдосконалення та адаптації систем захисту інформації відповідно до нових умов цифрового середовища. На думку С. О. Климчука, у перспективі значно зростатиме роль технологій штучного інтелекту як інструменту підвищення ефективності систем інформаційної безпеки та виявлення кіберзагроз [8].

Таким чином, інформаційна безпека є невід'ємною складовою системи економічної безпеки суб'єктів господарювання. Вона охоплює сукупність технічних, організаційних і правових заходів, спрямованих на захист інформаційних ресурсів від внутрішніх і зовнішніх загроз. В умовах трансформації інформації у стратегічний ресурс підприємств її захист набуває ключового значення для забезпечення конкурентоспроможності, фінансової стійкості та довгострокового розвитку суб'єктів господарювання.

1.2. Організаційно-економічні механізми забезпечення інформаційної безпеки підприємства

Організаційно-економічні механізми забезпечення інформаційної безпеки підприємства є важливою складовою системи економічної безпеки суб'єктів господарювання, оскільки спрямовані на формування стійкого захисту інформаційних ресурсів від внутрішніх і зовнішніх загроз. У сучасних умовах інформаційна безпека розглядається не лише як технічна функція захисту даних, а як комплексна система управлінських, економічних,

правових та організаційних заходів, що забезпечують стабільність функціонування підприємства.

Інформаційна безпека в межах діяльності суб'єктів господарювання може бути визначена як рівень захищеності їх інформаційного середовища, що охоплює ключові бізнес-процеси, управлінські рішення, фінансові потоки та інші стратегічно важливі ресурси, від деструктивних інформаційних впливів. Такі впливи можуть призводити до порушення нормального функціонування підприємства, зниження його конкурентоспроможності та погіршення показників економічної стійкості.

З позиції системного підходу інформаційна безпека підприємства передбачає здатність його інформаційної інфраструктури виявляти, попереджати та нейтралізувати потенційні загрози. Це включає реалізацію заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації як базових характеристик її захищеності. Водночас інформаційна безпека охоплює не лише технологічний рівень, але й організаційні структури управління, економічні інструменти регулювання та правове забезпечення.

Джерелами інформаційних загроз для підприємств можуть виступати як внутрішні суб'єкти (працівники, підрозділи), так і зовнішні агенти (конкуренти, кіберзлочинці, сторонні організації). Сукупність таких факторів формує широкий спектр ризиків, що впливають на інформаційну складову економічної безпеки підприємства та можуть призводити до фінансових втрат, витоку комерційної таємниці або порушення безперервності бізнес-процесів.

Важливо враховувати, що інформаційна безпека має динамічний характер і змінюється під впливом розвитку інформаційно-комунікаційних технологій. Сучасні технологічні рішення водночас виступають як інструмент посилення захисту інформаційних систем, так і як джерело нових загроз, пов'язаних із кіберзлочинністю, несанкціонованим доступом та

інформаційними атаками. Таким чином, підприємства змушені постійно адаптувати свої системи захисту до нових умов цифрового середовища.

У цьому контексті забезпечення інформаційної безпеки потребує формування комплексних організаційно-економічних механізмів, які поєднують технічні засоби захисту, управлінські процедури, економічні стимули та правові інструменти регулювання. До таких механізмів належать політики інформаційної безпеки, системи управління ризиками, внутрішній контроль, регламентація доступу до інформаційних ресурсів, а також оцінка економічної ефективності заходів захисту.

Окрему роль у забезпеченні інформаційної безпеки відіграє формування корпоративної культури безпеки, що передбачає підвищення рівня обізнаності працівників, проведення навчання з питань кіберзахисту та дотримання внутрішніх регламентів. Крім того, важливим елементом є правове забезпечення, яке базується на дотриманні національного законодавства та міжнародних стандартів у сфері захисту інформації.

Таким чином, організаційно-економічні механізми забезпечення інформаційної безпеки підприємства виступають невід'ємною складовою системи економічної безпеки суб'єктів господарювання. Вони забезпечують комплексний захист інформаційних ресурсів, сприяють мінімізації ризиків та створюють умови для стабільного функціонування та розвитку підприємства в умовах зростаючих інформаційних загроз.

Таблиця 1.1 . Організаційно-економічні механізми забезпечення інформаційної безпеки підприємства

Група механізмів	Сутність	Основні інструменти	Економічний ефект для підприємства
Організаційні	Формування внутрішньої системи управління інформаційною безпекою	Політики безпеки, регламенти доступу, розподіл ролей і відповідальності, внутрішній аудит	Зменшення ризику витоку інформації, підвищення керованості процесів
Технічні	Захист інформаційних систем і ресурсів за допомогою технологій	Антивірусні системи, міжмережеві екрани, шифрування, резервне копіювання	Зниження ймовірності кібератак і простоїв систем
Економічні	Оптимізація витрат на забезпечення інформаційної безпеки	Бюджетування, оцінка ризиків, страхування кіберризиків, інвестиції в IT-	Підвищення ефективності використання ресурсів і

		захист	мінімізація фінансових втрат
Правові	Нормативне забезпечення захисту інформації	Дотримання законодавства, договори про конфіденційність (NDA), стандарти ISO/IEC 27001	Зменшення юридичних ризиків і штрафних санкцій
Кадрові	Формування культури інформаційної безпеки серед персоналу	Навчання, інструктажі, контроль доступу, підвищення кваліфікації	Зниження ризику людського фактора та помилок персоналу

Одним із ключових елементів системи національної безпеки є забезпечення інформаційної безпеки суб'єктів господарювання, оскільки саме підприємницька діяльність сьогодні значною мірою залежить від якості, своєчасності та достовірності інформації. У сучасних умовах інформація виступає повноцінним фактором виробництва та стратегічним ресурсом розвитку економічних систем. Паралельно з ускладненням інформаційних технологій, засобів автоматизації та цифровізації бізнес-процесів зростає рівень залежності підприємств від безпеки інформаційно-комунікаційних систем, що вони використовують [9, С. 205].

У загальному розумінні інформаційна безпека може розглядатися як стан захищеності інформаційного середовища, який забезпечує його функціонування та розвиток відповідно до економічних інтересів суб'єктів господарювання, суспільства та держави. Під інформаційним середовищем при цьому розуміють сукупність взаємопов'язаних процесів і елементів, що забезпечують створення, обробку, зберігання та використання інформаційних ресурсів у межах діяльності підприємств.

Структурно інформаційне середовище суб'єкта господарювання доцільно розглядати як систему взаємопов'язаних компонентів, кожен з яких має значення для формування рівня інформаційної безпеки.

По-перше, процес формування та поширення первинної й вторинної інформації. Йдеться про створення інформаційних даних у результаті аналітичної, виробничої або дослідницької діяльності підприємства. Первинна інформація формується безпосередньо з джерел, тоді як вторинна є

результатом її обробки та інтерпретації. Від достовірності та якості таких даних залежить ефективність подальших управлінських рішень.

По-друге, формування інформаційних ресурсів та створення інформаційних продуктів. На цьому етапі відбувається систематизація та структурування даних, що дозволяє формувати інформаційні бази, аналітичні звіти, програмні рішення та інші інформаційні продукти, які використовуються в управлінні підприємством. Також важливим елементом є надання інформаційних послуг, що забезпечують підтримку процесів обробки та використання даних.

По-третє, процес споживання інформації. Він охоплює використання інформаційних ресурсів керівництвом та персоналом підприємства для прийняття управлінських, фінансових і стратегічних рішень. Доступність інформації для уповноважених користувачів є ключовою умовою ефективного функціонування системи економічної безпеки.

По-четверте, створення та застосування інформаційних систем і технологій. Інформаційні системи являють собою сукупність технічних і програмних засобів, які забезпечують збір, обробку, зберігання та передачу даних. Їх використання є базовою умовою цифрової трансформації підприємств та підвищення ефективності управління бізнес-процесами.

По-п’яте, формування та впровадження механізмів інформаційної безпеки. У сучасних умовах зростання кіберзагроз цей компонент набуває особливої значущості. Він передбачає розробку та застосування технічних, організаційних і правових інструментів захисту інформації від несанкціонованого доступу, втрати, спотворення або блокування. До таких інструментів належать системи шифрування, політики доступу, засоби кіберзахисту, а також навчання персоналу принципам інформаційної безпеки.

Таким чином, інформаційна безпека підприємства є комплексним та багаторівневим процесом, який охоплює всі етапи життєвого циклу інформації – від її створення до використання. Вона не лише забезпечує захист інформаційних ресурсів, але й безпосередньо впливає на ефективність

функціонування суб’єктів господарювання, виступаючи важливим елементом їх економічної безпеки. Отже, належний рівень інформаційної безпеки є необхідною умовою стабільного розвитку підприємств в умовах цифрової трансформації економіки.

Важливо підкреслити, що задоволення інформаційних потреб у будь-якій формі сприяє накопиченню та розширенню знань про навколишнє середовище та процеси, які в ньому відбуваються. У результаті цього підвищується рівень інформованості як окремих осіб, так і суспільства та держави в цілому, що безпосередньо впливає на ефективність прийняття рішень у різних сферах діяльності [10, С. 46–48].

Концептуальні засади інформаційної безпеки держави являють собою систематизовану сукупність теоретичних положень і практичних підходів до забезпечення захищеності інформаційного простору. У межах цієї концепції здійснюється класифікація основних дестабілізуючих факторів та інформаційних загроз, що впливають на безпеку особистості, суспільства та держави, а також визначаються ключові напрями організації системи інформаційної безпеки і механізми її реалізації [10, С. 24–25].

У контексті забезпечення інформаційної безпеки держави суттєве значення має інформаційна безпека суб’єктів підприємницької діяльності, оскільки саме підприємства є одними з основних носіїв і продуцентів критично важливої інформації. До основних загроз інформаційній безпеці сучасних підприємств належать: протиправні дії окремих економічних суб’єктів у сфері створення, обробки та поширення інформації; порушення встановлених регламентів роботи з інформаційними ресурсами; як умисні, так і ненавмисні дії персоналу інформаційних систем; помилки на етапах проєктування інформаційної інфраструктури; а також відмови технічних засобів і збої програмного забезпечення в інформаційно-телекомунікаційних системах [10, С. 28].

Джерела негативного впливу на інформаційну безпеку підприємства є багатокомпонентними та можуть бути згруповані за різними ознаками.

Зокрема, першу групу становлять дії окремих фізичних осіб і суб'єктів господарювання, які можуть як свідомо, так і несвідомо впливати на стан захищеності інформаційних ресурсів. До цієї категорії належать представники органів державної влади, міжнародних структур, а також конкуренти, дії яких можуть проявлятися у формі як прямих кібератак, так і непрямих впливів, зокрема через нормативне регулювання або інформаційні кампанії.

Друга група охоплює впливи, що виникають унаслідок об'єктивних економічних, технологічних або соціально-політичних умов. До них належать зміни кон'юнктури ринку, технологічні інновації, науково-технічний прогрес, а також форс-мажорні обставини, зокрема природні катастрофи або кризові явища. Такі фактори мають зовнішній характер і часто є неконтрольованими з боку підприємства, однак суттєво впливають на рівень його інформаційної безпеки.

Залежно від природи походження негативні впливи доцільно поділяти на об'єктивні та суб'єктивні. Об'єктивні впливи виникають незалежно від діяльності підприємства та його персоналу і зумовлені зовнішніми умовами функціонування економічної системи. Натомість суб'єктивні чинники пов'язані з внутрішніми управлінськими процесами, рівнем організації інформаційної безпеки та людським фактором. До них належать недоліки в управлінні інформаційними ресурсами, недостатній рівень підготовки персоналу, а також несвоєчасне оновлення засобів захисту інформації, що створює додаткові уразливості для підприємства.

Таким чином, негативні впливи на інформаційну безпеку суб'єктів господарювання мають комплексний характер і потребують системного підходу до їх ідентифікації, аналізу та мінімізації, що передбачає поєднання зовнішнього моніторингу середовища та вдосконалення внутрішніх механізмів управління безпекою.

Основною метою інформаційної безпеки підприємства є забезпечення його стабільного та безперервного функціонування, а також створення умов

для довгострокового розвитку в умовах високої невизначеності та зростання кіберзагроз. У сучасному динамічному бізнес-середовищі захист інформаційних ресурсів набуває стратегічного значення як ключовий елемент системи економічної безпеки суб'єктів господарювання.

Одним із ключових джерел загроз для інформаційної складової економічної безпеки суб'єктів господарювання є постійне ускладнення інформаційних систем та телекомунікаційних мереж, які сьогодні виступають критично важливою інфраструктурою для забезпечення стабільного функціонування економіки та суспільства в цілому. Такі системи забезпечують безперервність бізнес-процесів підприємств, виконують функції обробки та передачі даних і водночас є складовою частиною національної безпеки [11, С. 19-20].

Загрози у сфері інформаційної безпеки підприємств можуть мати різний характер і походження. Вони можуть бути наслідком як умисних дій, зокрема кібератак, несанкціонованого доступу або промислового шпигунства, так і ненавмисних помилок персоналу, що виникають через недостатній рівень кваліфікації або порушення встановлених регламентів роботи з інформаційними системами. Крім того, суттєвими є технічні ризики, пов'язані з відмовами апаратного та програмного забезпечення, які можуть призводити до порушення функціонування інформаційної інфраструктури підприємства.

Окрему групу становлять загрози, що формуються з боку кримінальних структур та кіберзлочинних угруповань, які використовують вразливості інформаційних систем для досягнення протиправних цілей. Об'єктами таких впливів часто стають інформаційні системи підприємств, що забезпечують функціонування критично важливих сфер економіки, зокрема енергетики, транспорту, фінансового сектору та логістики.

Вразливість зазначених систем може призводити до суттєвих негативних наслідків для економічної безпеки як окремих підприємств, так і економіки в цілому. Зокрема, порушення роботи енергетичних або

транспортних систем спричиняє зупинку або уповільнення бізнес-процесів, фінансові втрати та зниження рівня довіри з боку споживачів і контрагентів.

У цьому контексті інформаційна безпека підприємства виступає не лише внутрішнім елементом системи управління, а й важливим фактором забезпечення загальної економічної безпеки суб'єкта господарювання. Її ефективне забезпечення потребує комплексного підходу, що включає постійний моніторинг інформаційних ризиків, аналіз загроз, підвищення кваліфікації персоналу, а також впровадження сучасних технологічних рішень захисту інформаційних ресурсів. Реалізація таких заходів дозволяє мінімізувати ризики та забезпечити стабільність функціонування підприємства в умовах цифрової трансформації економіки.

Окрему загрозу становить концентрація засобів масової інформації у руках обмеженого кола власників, що створює ризики інформаційного впливу на суспільну свідомість. Такі процеси можуть проявлятися у формі маніпуляції громадською думкою щодо соціально-економічних та політичних подій, а також у трансформації ціннісних орієнтирів суспільства шляхом нав'язування певних моделей поведінки.

Додатковим суттєвим джерелом загроз є зростання масштабів вітчизняної та міжнародної кіберзлочинності. Вона може проявлятися у вигляді шахрайських операцій із використанням інформаційно-телекомунікаційних систем, відмивання коштів, отриманих незаконним шляхом, несанкціонованого доступу до фінансової та банківської інформації, а також її подальшого використання з корисливою метою [11, С. 19-20].

Окрім внутрішніх чинників, істотний вплив на стан інформаційної безпеки підприємства мають зовнішні джерела загроз, які можуть істотно впливати на його функціонування та рівень економічної стійкості. Умовно такі загрози доцільно поділити на кілька основних груп, що відрізняються за характером походження та механізмами впливу.

По-перше, суттєвим джерелом ризиків є несприятлива державна економічна політика. Зміни у валютному регулюванні, податковій системі,

митних тарифах та інших інструментах державного регулювання можуть вступати в протиріччя з діючими бізнес-моделями підприємств і негативно впливати на їх економічну безпеку. Додаткові ризики формуються внаслідок адміністративного втручання органів державної влади у господарську діяльність суб'єктів бізнесу, зокрема через обмеження товарно-грошових операцій, надмірне регуляторне навантаження або неправомірне втручання у фінансово-господарські процеси підприємств. У міжнародному середовищі подібні загрози можуть посилюватися через протекціоністську або дискримінаційну економічну політику інших держав.

По-друге, значним зовнішнім джерелом загроз є діяльність інших суб'єктів господарювання, насамперед у формі недобросовісної конкуренції. У науковій та практичній площині вона охоплює низку деструктивних практик, серед яких: імітація діяльності конкурентів з метою введення споживачів в оману; поширення недостовірної або викривленої інформації щодо діяльності інших компаній з метою їх дискредитації; а також неправомірне використання комерційних позначень, торговельних марок та інших елементів ідентифікації, що може призводити до порушення прав інтелектуальної власності та економічних інтересів підприємств.

У цьому контексті забезпечення інформаційної безпеки виступає важливим інструментом захисту економічних інтересів суб'єктів господарювання та реалізується через комплекс організаційних, технічних і правових механізмів. Зокрема, формування ефективної системи інформаційного захисту потребує належного нормативного закріплення процедур та правил функціонування підсистем безпеки на підприємстві.

Однією з форм організаційного забезпечення інформаційної безпеки є інформаційний патронат, який передбачає підтримку державою та уповноваженими структурами процесів захисту інформаційного середовища підприємств. Такий підхід охоплює як забезпечення інформацією щодо потенційних загроз і дестабілізуючих факторів, так і безпосередній захист критично важливих інформаційних ресурсів суб'єктів господарювання [12].

Оскільки система економічної безпеки підприємства є інтегрованою та взаємопов’язаною, більшість завдань у сфері інформаційної безпеки реалізується у взаємодії з іншими її підсистемами. Технічна складова забезпечує виявлення та запобігання витокам інформації, а також захист інформаційних активів від несанкціонованого доступу як з боку зовнішніх, так і внутрішніх порушників. Організаційний компонент спрямований на регламентацію поведінки працівників щодо роботи з конфіденційною інформацією та формування відповідних внутрішніх процедур безпеки.

Дозвільно-регуляторний компонент системи інформаційної безпеки передбачає класифікацію інформаційних ресурсів за рівнями доступу та визначення прав користувачів, що дозволяє мінімізувати ризики витоку або неправомірного використання даних. Водночас важливу роль відіграє превентивний (попереджувальний) компонент, який забезпечує раннє виявлення потенційних загроз, аналіз каналів витоку інформації та їх блокування. Правовий компонент, у свою чергу, спрямований на захист інтересів підприємства у правовому полі, зокрема шляхом закріплення режиму комерційної таємниці у внутрішніх документах та договорах.

Сучасні підходи до побудови системи захисту інформації не завжди повною мірою враховують комплексність завдань, що постають перед підприємствами в умовах цифрової трансформації економіки. У цьому контексті ключовими завданнями системи інформаційної безпеки є: організація контролю за обігом конфіденційної документації; виявлення та блокування каналів витоку інформації; розробка внутрішніх нормативних документів щодо роботи з комерційною таємницею; захист інформації в інформаційно-комунікаційних системах; впровадження технічних засобів захисту даних; правовий супровід спорів, пов’язаних із порушенням інформаційних прав; а також підвищення рівня обізнаності персоналу у сфері інформаційної безпеки.

Важливо підкреслити, що ефективна система інформаційної безпеки ґрунтується на поєднанні превентивних, організаційних, технічних і

правових заходів, що реалізуються в межах загальної системи економічної безпеки підприємства. Такий підхід передбачає комплексне управління ризиками та орієнтацію на недопущення витоку стратегічно важливої інформації.

У сучасних умовах функціонування підприємств ключовим принципом забезпечення інформаційної безпеки виступає системність і превентивність заходів, а також достатній рівень поінформованості суб'єктів безпеки щодо потенційних загроз. Це створює необхідність подальшого розвитку механізмів інформаційної безпеки та їх адаптації до умов цифрової економіки, що визначає актуальність удосконалення відповідних організаційно-економічних підходів у діяльності суб'єктів господарювання.

1.3. Інформаційна безпека як складова системи економічної безпеки підприємства

У сучасних умовах функціонування суб'єктів господарювання особливої актуальності набуває проблема забезпечення надійного захисту їх економічних інтересів, а також обґрунтування та реалізації ефективних управлінських і стратегічних рішень. Активізація процесів європейської інтеграції та глобалізації висуває перед українськими підприємствами нові вимоги, що пов'язані з необхідністю адаптації до зростаючого рівня конкуренції, підвищенням невизначеності зовнішнього середовища та необхідністю мінімізації ризиків, що виникають унаслідок економічної нестабільності та конфліктності ринкових відносин.

Водночас сучасні наукові дослідження у сфері економічної безпеки підприємств не завжди забезпечують цілісне та системне розуміння механізмів її формування й функціонування. Зокрема, недостатньо опрацьованими залишаються питання забезпечення економічної безпеки суб'єктів господарювання в умовах високої турбулентності зовнішнього середовища, цифровізації економіки та посилення глобальних ризиків. Це створює суттєві труднощі у формуванні ефективних систем захисту

економічних інтересів підприємств, що безпосередньо впливає на рівень стійкості національної економіки в цілому.

Основною метою системи економічної безпеки підприємства є формування комплексного механізму протидії як потенційним, так і реальним загрозам його діяльності. Це передбачає розроблення та впровадження превентивних заходів, спрямованих на мінімізацію ризиків і забезпечення стабільного функціонування підприємства в умовах нестабільного зовнішнього та внутрішнього середовища. У цьому контексті економічна безпека повинна охоплювати комплекс взаємопов'язаних складових, серед яких важливе місце займають фінансова, кадрова, техніко-технологічна, екологічна, соціальна, фізична та інформаційна безпека.

Інформаційна безпека в сучасних умовах виступає одним із ключових елементів системи економічної безпеки підприємства, що зумовлено стрімким розвитком інформаційних технологій та цифровізацією бізнес-процесів. Наприкінці XX – на початку XXI століття відбулися глибокі трансформаційні зміни, які сприяли формуванню глобального інформаційного простору та становленню інформаційного суспільства як нової соціально-економічної реальності. Водночас активне використання інформаційного простору як інструменту конкурентної боротьби призвело до зростання вразливості інформаційної сфери до кібернетичних впливів, які можуть мати як навмисний, так і випадковий або техногенний характер [13].

У таких умовах інформаційна безпека набуває статусу стратегічного елемента управління підприємством і є невід'ємною складовою його економічної безпеки. Вона спрямована на захист інформаційних ресурсів, комерційної таємниці, управлінських даних та інших критично важливих відомостей від несанкціонованого доступу, викрадення, спотворення або знищення.

Зростання значущості інформаційної безпеки також обумовлене підвищенням ризиків, пов'язаних із використанням інсайдерської інформації та кіберзагрозами, що походять як із зовнішнього, так і з внутрішнього

середовища підприємства. Якщо раніше ці питання розглядалися переважно у контексті діяльності великих корпорацій та міжнародних компаній, то сьогодні вони стають актуальними і для середнього та малого бізнесу в Україні, який поступово усвідомлює критичну важливість захисту власних інформаційних активів.

Таким чином, інформаційна безпека є невід'ємною складовою системи економічної безпеки суб'єктів господарювання, що забезпечує стабільність їх функціонування, підвищення конкурентоспроможності та захист стратегічно важливих ресурсів у сучасному цифровому середовищі.

Зовнішні та внутрішні інформаційні впливи можуть істотно порушувати такі базові властивості інформації, як конфіденційність, цілісність, доступність і достовірність, що, у свою чергу, створює передумови для виникнення значних ризиків у діяльності суб'єктів господарювання. Наслідки таких порушень мають комплексний характер і безпосередньо впливають на рівень економічної безпеки підприємства.

Серед основних негативних наслідків доцільно виділити такі:

1. **Порушення функціонування систем управління технологічними та організаційними процесами.** Дестабілізація інформаційних потоків може призводити до зниження ефективності управління ресурсами підприємства, порушення координації підрозділів та затримок у виробничо-господарській діяльності.

2. **Розголошення комерційної таємниці та іншої конфіденційної інформації.** Втрата контролю над захищеними даними негативно впливає на рівень конкурентоспроможності підприємства та послаблює його ринкові позиції.

3. **Порушення достовірності фінансової та управлінської звітності.** Викривлення або несанкціонована зміна фінансових даних знижує рівень довіри з боку інвесторів, кредиторів та ділових партнерів.

4. **Несанкціонований доступ до інформаційних баз даних підприємства.** Подібні інциденти можуть призводити до втрати або

викрадення критично важливої інформації, що становить основу функціонування бізнесу.

5. **Спотворення публічної та репутаційної інформації про підприємство.** Поширення недостовірних або маніпулятивних відомостей негативно впливає на ділову репутацію компанії та її імідж на ринку.

Наслідки порушення цілісності та достовірності інформації можуть мати довгостроковий і системний характер, зокрема:

зниження ринкової вартості капіталу підприємства через втрату довіри інвесторів;

ускладнення процесу залучення інвестиційних ресурсів;

погіршення або розрив ділових відносин із контрагентами та партнерами;

зрив переговорних процесів і втрата потенційно вигідних контрактів;

прийняття неефективних управлінських рішень унаслідок використання викривленої інформації;

втрата можливостей правового захисту результатів інтелектуальної та науково-технічної діяльності;

зниження обсягів реалізації продукції або падіння попиту;

погіршення ділової репутації та зменшення рівня довіри до підприємства;

посилення вимог фінансових установ щодо кредитування та збільшення вартості позикового капіталу;

ускладнення логістичних процесів і взаємодії з постачальниками через втрату довіри до підприємства.

Таким чином, інформаційні загрози мають мультиплікативний вплив на діяльність суб’єктів господарювання, оскільки їх наслідки виходять за межі суто інформаційної сфери та безпосередньо трансформуються у фінансові, організаційні та репутаційні втрати. Це підтверджує необхідність розгляду інформаційної безпеки як ключового елемента системи економічної безпеки підприємства.

У разі критичного порушення принципів інформаційної безпеки можливі ситуації, що призводять до повної втрати бізнесу або суттєвого його занепаду, що підкреслює стратегічну важливість системного захисту інформаційних ресурсів підприємства.

Концептуально інформаційну безпеку доцільно розглядати у декількох взаємопов'язаних площинах. По-перше, як стан захищеності інформаційного середовища, що забезпечує його формування, використання та розвиток відповідно до інтересів суб'єктів господарювання, суспільства та держави. По-друге, як стан забезпечення інформаційних потреб економічних суб'єктів і суспільства, за якого гарантується стабільне функціонування та розвиток незалежно від впливу внутрішніх і зовнішніх деструктивних чинників.

У контексті економічної безпеки підприємства ключові інтереси у сфері інформаційної безпеки, що стосуються інформаційних ресурсів, інформаційних систем та інформаційних технологій, традиційно структуровані навколо трьох базових властивостей: доступності, цілісності та конфіденційності.

1. *Доступність інформації* визначає здатність користувачів отримувати необхідні інформаційні ресурси або сервіси у встановлений час без необґрунтованих обмежень. Забезпечення цього параметра є критично важливим для безперервності бізнес-процесів, оперативного управління та своєчасного прийняття рішень.

2. *Цілісність інформації* характеризує її повноту, точність та несуперечливість у процесі зберігання, обробки та передачі. Порушення цілісності призводить до викривлення даних, що може стати причиною прийняття неефективних управлінських рішень та формування хибних економічних оцінок діяльності підприємства.

3. *Конфіденційність інформації* передбачає обмеження доступу до даних для несанкціонованих користувачів і забезпечення захисту комерційно чутливої інформації, персональних даних та інших критично важливих відомостей підприємства.

З позиції інформаційних технологій інформаційна безпека розглядається як сукупність методів, засобів і процедур, спрямованих на виявлення вразливостей інформаційно-комунікаційних систем підприємства, ідентифікацію потенційних загроз та їх нейтралізацію.

Під загрозою інформаційної безпеки розуміють подію або дію, яка потенційно здатна порушити нормальне функціонування інформаційної системи підприємства, зокрема шляхом спотворення, знищення або несанкціонованого використання інформаційних ресурсів. Реалізація таких загроз може спричиняти як операційні збої, так і значні фінансово-економічні втрати.

Ймовірність реалізації загроз безпосередньо залежить від рівня вразливості інформаційної системи. Вразливості формуються під впливом специфіки бізнес-процесів, характеру оброблюваної інформації, а також особливостей апаратно-програмного забезпечення, що використовується на підприємстві. Важливу роль також відіграє ефективність впроваджених засобів захисту, які визначають загальний рівень стійкості інформаційної інфраструктури.

У цьому контексті забезпечення інформаційної безпеки повинно базуватися на інтегрованому підході, що поєднує технічні та організаційні заходи. До технічних належать засоби криптографічного захисту, міжмережеві екрани, антивірусні системи та інші інструменти кіберзахисту. Організаційні заходи охоплюють розробку політик доступу, регламентів роботи з інформацією, а також системне навчання персоналу щодо правил інформаційної безпеки.

Таким чином, ефективна система інформаційної безпеки є невід’ємним елементом загальної системи економічної безпеки підприємства, оскільки забезпечує захист критично важливих інформаційних активів і мінімізує ризики, що виникають у цифровому середовищі.

Аналіз теоретичних підходів і практики забезпечення інформаційної безпеки свідчить про доцільність виокремлення двох ключових груп загроз,

що впливають на інформаційні ресурси підприємства: ненавмисні (випадкові) та навмисні.

До *ненавмисних або випадкових загроз* належать ризики, що виникають унаслідок недосконалості організації процесів захисту інформації, помилок управлінського характеру або людського фактора. Такі ситуації можуть бути спричинені недостатнім рівнем кваліфікації персоналу, недотриманням регламентів безпеки або відсутністю належного контролю за інформаційними процесами. Типовими прикладами є випадкове видалення або пошкодження даних, некоректна конфігурація інформаційних систем, а також помилки користувачів, які можуть призводити до порушення стабільності функціонування підприємства.

Навмисні загрози є результатом цілеспрямованих дій, спрямованих на порушення конфіденційності, цілісності або доступності інформаційних ресурсів. До них відносяться несанкціонований доступ до інформаційних систем, викрадення або модифікація даних, а також використання інформаційних ресурсів з метою отримання неправомірної вигоди. Подібні дії можуть здійснюватися як зовнішніми зловмисниками (зокрема кіберзлочинцями), так і внутрішніми користувачами, які мають легітимний доступ до систем підприємства. У другому випадку особливу небезпеку становить зловживання службовими повноваженнями з метою розголошення або комерційного використання конфіденційної інформації.

Додатково класифікація загроз може здійснюватися за ознакою джерела їх виникнення, що дозволяє виокремити внутрішні та зовнішні загрози.

Внутрішні загрози формуються в межах самого підприємства та пов’язані з діями або бездіяльністю працівників. Вони можуть мати як ненавмисний, так і навмисний характер. Особливість внутрішніх загроз полягає в тому, що вони реалізуються в умовах наявного доступу до інформаційних ресурсів, що суттєво ускладнює їх виявлення та нейтралізацію. До них належать як порушення внутрішніх політик безпеки

через людський фактор, так і свідомі дії, спрямовані на завдання шкоди підприємству.

Зовнішні загрози виникають поза межами організації та реалізуються через вплив сторонніх суб'єктів або інформаційних середовищ. Найпоширенішими формами таких загроз є кібератаки, фішингові схеми, використання шкідливого програмного забезпечення, соціальна інженерія та інші методи несанкціонованого впливу на інформаційні системи.

Окрему групу становлять загрози, пов'язані з навмисними деструктивними діями, що можуть виникати за межами підприємства. До них, зокрема, належать [13, 14]:

– несанкціонований доступ до інформаційних ресурсів;

– заперечення або спотворення інформаційних операцій, що призводить до порушення цілісності даних;

– впровадження в програмне забезпечення прихованих деструктивних елементів («логічних бомб»), які активуються за певних умов;

– розробка та поширення шкідливого програмного забезпечення (вірусів);

– недбалість у розробці, супроводі та експлуатації програмних продуктів, що спричиняє збої в роботі систем;

– підробка електронних підписів та модифікація цифрової інформації;

– несанкціоноване перехоплення інформаційних потоків;

– відмова у наданні інформаційних послуг або блокування доступу до них.

Водночас, слід зазначити, що на сучасному етапі відсутній єдиний уніфікований підхід до класифікації загроз інформаційній безпеці, що зумовлено значною різноманітністю інформаційних систем, їх функціональним призначенням та специфікою оброблюваних даних.

У зв'язку з цим ефективне забезпечення інформаційної безпеки потребує застосування адаптивних підходів до ідентифікації та класифікації загроз, які враховують особливості конкретних інформаційних систем, а

також динаміку технологічного середовища та зміну характеру кіберризиків. Такий підхід дозволяє більш точно оцінювати рівень загроз та формувати ефективні механізми їх нейтралізації в межах системи економічної безпеки підприємства.

РОЗДІЛ 2. СУЧАСНІ ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ В КОНТЕКСТІ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ

2.1. Структура та характеристика загроз інформаційній безпеці підприємств

На сучасному етапі цифрової трансформації економіки загрози інформаційній безпеці підприємств набувають дедалі більш комплексного та динамічного характеру. Зростання обсягів цифрових даних, автоматизація бізнес-процесів і широке використання інформаційно-комунікаційних технологій формують нові умови функціонування суб’єктів господарювання, у яких інформаційні активи виступають ключовим фактором конкурентоспроможності. У таких умовах будь-яке порушення конфіденційності, цілісності чи доступності інформації здатне спричинити суттєві економічні втрати, погіршення ділової репутації та зниження ринкових позицій підприємства.

Однією з найбільш критичних загроз сучасного цифрового середовища є кіберзлочинність, яка охоплює сукупність протиправних дій, що реалізуються із використанням комп’ютерних мереж та інформаційних технологій. Основними цілями кіберзлочинців є несанкціонований доступ до корпоративних систем, викрадення конфіденційних даних, компрометація баз даних, а також отримання фінансової вигоди шляхом шантажу або продажу інформації. Стрімке зростання цифровізації бізнесу сприяє збільшенню кількості таких інцидентів та розширенню їх масштабів.

Сучасні методи кіберзлочинців постійно вдосконалюються і стають більш складними. Поряд із традиційними фішинговими атаками активно використовуються методи соціальної інженерії, автоматизовані інструменти злому та шкідливе програмне забезпечення нового покоління. Особливу небезпеку становить маніпулювання поведінкою користувачів з метою отримання доступу до захищених інформаційних систем. За оцінками міжнародних досліджень, значна частина компаній щорічно стикається з

кіберінцидентами, що підтверджує високий рівень ризиків у цій сфері [15, С. 18].

Окремим поширеним інструментом реалізації кіберзагроз є використання бот-мереж (botnet), які формуються шляхом зараження великої кількості пристроїв шкідливим програмним забезпеченням. Такі мережі можуть використовуватися для проведення DDoS-атак, масового розсилання спаму або інших деструктивних дій, при цьому власники інфікованих пристроїв часто не усвідомлюють їх участі в атаках.

Для протидії кіберзлочинності підприємствам необхідно впроваджувати комплексні заходи захисту, що включають регулярне оновлення програмного забезпечення, використання систем виявлення аномалій, фільтрацію мережевого трафіку та застосування сучасних антивірусних рішень. Важливим елементом є також впровадження моделей керування доступом, зокрема рольової моделі (RBAC), яка обмежує доступ до критично важливих інформаційних ресурсів відповідно до службових обов’язків працівників [16, С. 27-28].

Серед найбільш деструктивних кіберзагроз слід виокремити атаки типу DoS (Denial of Service) та DDoS (Distributed Denial of Service), які спрямовані на перевантаження інформаційних систем підприємства з метою порушення їх працездатності. Такі атаки можуть призводити до тимчасової або повної недоступності онлайн-сервісів, що безпосередньо впливає на операційну діяльність підприємства та спричиняє фінансові втрати.

Статистичні дані свідчать про стабільне зростання кількості DDoS-атак щороку, що підтверджує посилення загроз у кіберпросторі. Крім того, подібні атаки часто використовуються як відволікаючий маневр для реалізації інших кіберзлочинів, зокрема викрадення даних або впровадження шкідливого програмного забезпечення [17].

Фішингові атаки та соціальна інженерія залишаються одними з найпоширеніших методів отримання несанкціонованого доступу до інформаційних ресурсів підприємств. Їх сутність полягає у психологічному

впливі на користувача з метою добровільного розкриття конфіденційної інформації. Особливо небезпечною формою є цільовий фішинг (spear phishing), який базується на попередньому зборі інформації про конкретну організацію або особу [18].

Ефективними заходами протидії таким загрозам є систематичне навчання персоналу, підвищення рівня цифрової грамотності та впровадження багатофакторної автентифікації, що суттєво знижує ризик несанкціонованого доступу навіть у разі компрометації облікових даних.

Важливою складовою загроз інформаційній безпеці є також шкідливе програмне забезпечення (malware), яке використовується для отримання контролю над інформаційними системами, викрадення даних або їх пошкодження. До основних видів такого ПЗ належать комп'ютерні віруси, троянські програми, шпигунське програмне забезпечення та програми-вимагачі (ransomware).

Особливу небезпеку становлять програми-вимагачі, які блокують доступ до інформаційних ресурсів до моменту сплати викупу. У сучасній практиці такі атаки демонструють значне зростання та завдають суттєвих збитків підприємствам, особливо малим і середнім, які часто не мають достатнього рівня резервування даних і ресурсів для швидкого відновлення систем [19, С. 172].

Загалом ransomware-атаки реалізуються через заражені електронні листи, шкідливі вкладення або скомпрометовані вебресурси. Відсутність резервного копіювання та належної політики кіберзахисту значно підвищує ризики критичних втрат інформації та порушення безперервності бізнес-процесів.

Таким чином, сучасні загрози інформаційній безпеці підприємств мають багаторівневий характер і охоплюють як технічні, так і соціально-психологічні аспекти. Це зумовлює необхідність комплексного підходу до побудови системи захисту інформації в межах загальної системи економічної безпеки підприємства.

У сучасних умовах цифровізації економіки характер і масштаби загроз інформаційній безпеці підприємств суттєво ускладнилися. Інформаційні ресурси суб'єктів господарювання, що охоплюють комерційні, технологічні, фінансові та управлінські дані, сьогодні виступають ключовим елементом формування їх конкурентних переваг. Відповідно, забезпечення їх захисту набуває стратегічного значення, оскільки будь-яке порушення конфіденційності, цілісності або доступності інформації здатне спричинити фінансові втрати, репутаційні ризики та зниження ринкових позицій підприємства.

Однією з найбільш масштабних і динамічних загроз виступає кіберзлочинність, яка охоплює сукупність протиправних дій, реалізованих із використанням інформаційно-комунікаційних технологій. Основними цілями таких атак є несанкціоноване отримання конфіденційних даних, порушення функціонування корпоративних систем, компрометація баз даних, а також викрадення фінансової та комерційної інформації. Інтенсивний розвиток цифрових технологій і розширення онлайн-середовища призводять до постійного зростання кількості подібних інцидентів.

Методи кіберзлочинців постійно еволюціонують – від класичних фішингових схем до складних механізмів соціальної інженерії та використання шкідливого програмного забезпечення. Зловмисники часто експлуатують людський фактор, змушуючи користувачів добровільно надавати доступ до захищених систем. Відповідно до міжнародних досліджень, понад 60% компаній щороку стикаються з кіберінцидентами, що підтверджує високий рівень загроз у цій сфері [15, С. 18].

Сучасний етап розвитку інформаційної безпеки характеризується також активним використанням бот-мереж (botnet), які складаються із заражених пристроїв, що підконтрольні зловмисникам. Такі мережі часто застосовуються для реалізації DDoS-атак, розповсюдження шкідливого контенту та організації масованих кібератак, при цьому власники пристроїв можуть навіть не усвідомлювати їх участь у злочинній діяльності.

З метою протидії кіберзагрозам підприємствам необхідно впроваджувати комплекс технічних і організаційних заходів: регулярне оновлення програмного забезпечення, використання систем виявлення аномальної активності, фільтрацію мережевого трафіку, а також застосування сучасних антивірусних рішень. Важливим елементом є впровадження рольової моделі доступу (RBAC), яка дозволяє обмежити доступ до критично важливої інформації лише уповноваженим працівникам [16, С. 27–28].

Окрему групу кіберзагроз становлять атаки типу DoS та DDoS, що спрямовані на перевантаження інформаційних систем і виведення їх з ладу. Наслідком таких атак є тимчасова або повна недоступність сервісів підприємства, що особливо критично для компаній, які функціонують у цифровому середовищі. Статистичні дані свідчать про щорічне зростання кількості DDoS-атак на 10–15%, що підтверджує їх високу актуальність [17].

Серед поширених загроз також слід виділити фішингові атаки та соціальну інженерію. Їх сутність полягає у маніпулюванні користувачами з метою отримання конфіденційної інформації. Особливо небезпечним є spear-фішинг, який передбачає індивідуалізовані атаки на конкретних працівників чи організації [18]. Для мінімізації таких ризиків доцільним є підвищення рівня цифрової грамотності персоналу та використання багатофакторної автентифікації.

Важливою загрозою інформаційній безпеці виступає шкідливе програмне забезпечення (malware), яке включає віруси, троянські програми, шпигунські модулі та ransomware. Особливо небезпечними є програми-вимагачі, що блокують доступ до даних і вимагають викуп за їх відновлення. У 2021 році зафіксовано значне зростання таких атак, що підтверджує їх високу ефективність для кіберзлочинців і значну небезпеку для підприємств, особливо малого та середнього бізнесу [19, С. 172].

Для захисту від ransomware критично важливим є регулярне створення резервних копій даних та їх зберігання на ізольованих носіях або у захищених хмарних середовищах. Додатковим заходом є своєчасне

оновлення програмного забезпечення для усунення вразливостей, які можуть використовуватися зловмисниками.

Окремою проблемою є витоки даних, що можуть виникати як через зовнішні атаки, так і внаслідок внутрішніх помилок персоналу. За оцінками, значна частка інцидентів пов’язана саме з людським фактором або недостатнім рівнем контролю доступу. У зв’язку з цим важливу роль відіграє впровадження багаторівневих систем управління доступом і регулярне навчання співробітників принципам інформаційної безпеки [20].

Не менш значущими є вразливості програмного забезпечення, які виникають через помилки розробки, недостатнє тестування або несвоєчасне оновлення систем. Такі недоліки створюють потенційні точки входу для зловмисників. Згідно з дослідженнями, близько 25% кіберінцидентів пов’язані саме з експлуатацією програмних вразливостей [21, С. 94].

Додатково слід враховувати ризики, пов’язані з використанням застарілого або неперевіреного програмного забезпечення, яке може містити критичні дефекти безпеки [22, С. 105]. Ефективним механізмом протидії є впровадження політики регулярного оновлення та використання систем виявлення вторгнень (IDS).

Внутрішні загрози становлять окремий клас ризиків, оскільки вони виникають у межах організації та часто пов’язані з доступом працівників до критичної інформації. Такі загрози можуть бути як ненавмисними (помилки, недбалість), так і умисними (зловживання доступом, витік даних). Для їх мінімізації використовуються системи моніторингу поведінки користувачів та аналізу аномальної активності [23].

Зростаюче використання хмарних технологій і мобільних пристроїв створює додаткові ризики інформаційної безпеки. Недостатній рівень захисту хмарних сервісів або використання незахищених мереж може призводити до перехоплення даних. У цьому контексті важливими є технології шифрування, VPN та політики BYOD, які регламентують використання особистих пристроїв у корпоративному середовищі [24].

Інтеграція технологій штучного інтелекту (ШІ) та методів машинного навчання у сучасні системи інформаційної безпеки підприємств суттєво підвищує ефективність виявлення та нейтралізації кіберзагроз. Використання таких технологій забезпечує можливість оперативного опрацювання значних масивів даних і виявлення нетипових патернів у поведінці користувачів або мережевому трафіку, які можуть свідчити про наявність потенційних атак. Системи, побудовані на основі ШІ, здатні автоматично ідентифікувати підозрілі події та здійснювати швидке реагування на інциденти інформаційної безпеки [25].

Окремого значення набуває застосування алгоритмів штучного інтелекту для прогнозування можливих сценаріїв розвитку кіберзагроз. Аналіз історичних даних про атаки дозволяє формувати моделі потенційних загроз і завчасно впроваджувати відповідні захисні механізми. Крім того, технології глибокого навчання активно застосовуються для виявлення фішингових ресурсів, а також для ідентифікації та блокування шкідливого програмного забезпечення на ранніх етапах його проникнення в інформаційні системи.

Таким чином, спектр загроз інформаційній безпеці підприємств охоплює як зовнішні та внутрішні навмисні дії, так і випадкові помилки персоналу, що можуть призводити до порушення цілісності інформаційних процесів. У зв’язку з цим забезпечення належного рівня захисту інформаційних ресурсів потребує комплексного підходу, який поєднує технічні, організаційні та освітні інструменти.

Практична реалізація ефективної системи інформаційної безпеки передбачає впровадження сучасних засобів моніторингу, криптографічного захисту, багаторівневого контролю доступу, а також систематичне підвищення кваліфікації персоналу у сфері кібербезпеки. Додатково важливим є використання адаптивних технологій, зокрема систем поведінкового аналізу та інтелектуальних механізмів виявлення аномалій.

Отже, сучасний рівень розвитку інформаційних технологій зумовлює необхідність безперервного вдосконалення підходів до забезпечення інформаційної безпеки підприємств. Лише поєднання технологічних інновацій, зокрема штучного інтелекту, із організаційними заходами дозволяє формувати ефективну систему захисту, здатну мінімізувати ризики втрати або компрометації критично важливої інформації та забезпечити стабільність функціонування підприємства.

2.2. Ідентифікація та аналіз вразливостей інформаційних систем у контексті економічної безпеки підприємств

У сучасних умовах цифрової трансформації економіки інформаційні системи виступають базовим елементом забезпечення ефективного функціонування підприємств. Саме через них здійснюється обробка, зберігання та передача критично важливої інформації, яка формує основу управлінських рішень і забезпечує конкурентні переваги суб'єктів господарювання. До таких процесів належать управління фінансовими потоками, клієнтськими базами, логістикою, складськими ресурсами, маркетинговою аналітикою та іншими бізнес-функціями.

Разом із розширенням обсягів даних, кількості користувачів і каналів доступу до інформаційних ресурсів зростає і рівень уразливості інформаційних систем. Це створює додаткові ризики для економічної безпеки підприємств, оскільки будь-яка технічна або організаційна слабкість може бути використана зловмисниками для несанкціонованого доступу, викрадення даних або порушення працездатності систем.

Актуальність дослідження вразливостей інформаційних систем зумовлена не лише динамічним зростанням кількості кіберзагроз, але й посиленням вимог до захисту інформації з боку регуляторних органів та міжнародних стандартів. Для підприємств, що працюють із конфіденційними даними, належний рівень інформаційної безпеки є невід'ємною складовою

загальної системи економічної безпеки, а також важливим чинником збереження ділової репутації та довіри партнерів.

Інформаційні системи підприємств мають складну багаторівневу структуру, що включає апаратне забезпечення, програмні компоненти, телекомунікаційні мережі та інформаційні ресурси. Кожен із цих елементів може містити потенційні вразливості, які визначаються як слабкі місця системи, здатні бути використаними для реалізації кіберзагроз. Відповідно до сучасних підходів у сфері кібербезпеки, такі вразливості доцільно класифікувати на технічні, організаційні, фізичні та операційні, що дозволяє систематизувати підходи до їх виявлення та усунення [26, С. 53].

Найбільш поширеною групою є технічні вразливості, які виникають унаслідок недосконалості програмного або апаратного забезпечення, а також помилок у процесі його розробки чи експлуатації. Вони становлять значну частку кіберризиків, оскільки сучасні інформаційні системи є складними та багатокомпонентними [27]. До основних типів технічних вразливостей належать:

1. *Недоліки програмного забезпечення* – помилки у вихідному коді, логічні дефекти або відсутність належних механізмів захисту. Найпоширенішими прикладами є SQL-ін’єкції, які дозволяють зловмисникам виконувати несанкціоновані запити до баз даних, що може призвести до витоку або зміни інформації.

2. *Вразливості протоколів передачі даних* – недоліки у криптографічних або мережевих протоколах (наприклад, SSL/TLS), які можуть створювати умови для перехоплення або підміни інформації під час її передачі між користувачем і сервером.

3. *Незахищені API-інтерфейси* – недостатній рівень захисту програмних інтерфейсів, що використовуються для інтеграції систем, може відкривати несанкціонований доступ до внутрішніх ресурсів підприємства. У таких випадках можливе обходження механізмів автентифікації та авторизації.

4. *Слабкі механізми автентифікації* – використання простих або повторюваних паролів, а також відсутність багатофакторної автентифікації суттєво підвищує ризик несанкціонованого доступу до інформаційних систем [28].

Таблиця 2.1. Класифікація вразливостей інформаційних систем

Тип вразливості	Характеристика	Приклади
Технічні	Недоліки ПЗ та обладнання	баги, застарілі системи
Організаційні	Недосконалі політики	відсутність контролю доступу
Фізичні	Доступ до обладнання	крадіжка серверів
Операційні	Помилки процесів	збій моніторингу

Таким чином, ідентифікація та аналіз вразливостей інформаційних систем є ключовим етапом формування ефективної системи інформаційної безпеки підприємства. Виявлення слабких місць дозволяє не лише знизити рівень кіберризиків, але й забезпечити стабільність функціонування підприємства в контексті його економічної безпеки.

Технічні вразливості потребують постійного контролю, регулярного оновлення програмно-апаратних компонентів інформаційних систем, а також застосування автоматизованих засобів виявлення та усунення потенційних недоліків. Їх своєчасна ідентифікація є критично важливою умовою забезпечення стабільного функціонування інформаційної інфраструктури підприємства.

Організаційні вразливості безпосередньо пов’язані з людським фактором, внутрішніми політиками безпеки та рівнем управління персоналом. Вони виникають унаслідок недостатньо ефективної системи управління інформаційною безпекою на рівні підприємства, а також через відсутність належної культури кібербезпеки серед працівників. До основних організаційних вразливостей належать:

1. Недосконалі або формальні політики безпеки – відсутність чітко визначених регламентів щодо роботи з інформацією призводить до хаотичного доступу до даних та використання ненадійних практик їх обробки.

2. Низький рівень обізнаності персоналу – працівники, які не володіють базовими знаннями з інформаційної безпеки, стають вразливим елементом системи, що підвищує ризик успішних фішингових атак і соціальної інженерії та, як наслідок, витоку конфіденційних даних.

3. Недостатня готовність до реагування на інциденти – відсутність відпрацьованих процедур дій у кризових ситуаціях ускладнює оперативне реагування на кібератаки та може суттєво збільшити їх негативні наслідки для підприємства [29].

Зниження рівня організаційних вразливостей досягається шляхом системного навчання працівників, впровадження внутрішніх політик інформаційної безпеки та регулярного проведення навчальних тренувань із реагування на інциденти.

Фізичні вразливості пов’язані з можливістю фізичного доступу до приміщень, обладнання та інфраструктури, де здійснюється зберігання й обробка інформації. До основних фізичних ризиків належать:

1. Несанкціонований доступ до службових приміщень – недостатній контроль доступу до офісів, серверних або архівів створює ризик фізичного втручання у роботу інформаційних систем.

2. Вплив природних та техногенних факторів – пожежі, затоплення, аварії чи інші надзвичайні події можуть призвести до втрати або пошкодження критично важливого обладнання та даних.

3. Крадіжка технічних засобів – викрадення ноутбуків, серверного або мобільного обладнання може спричинити витік конфіденційної інформації, що зберігається локально [30].

Мінімізація фізичних вразливостей передбачає впровадження систем контролю доступу, охорони об’єктів, а також використання резервного копіювання даних із їх розміщенням у захищених або віддалених середовищах.

Операційні вразливості формуються внаслідок недоліків в організації бізнес-процесів та управлінні інформаційною безпекою. Вони охоплюють:

1. Неефективне управління правами доступу – відсутність чіткої системи розмежування доступу до інформаційних ресурсів може призводити до надмірних привілеїв і несанкціонованого використання даних.

2. Недостатній рівень моніторингу безпеки – відсутність постійного контролю за подіями в інформаційних системах ускладнює виявлення аномальної активності та своєчасне реагування на інциденти.

3. Неналежна організація резервного копіювання – відсутність систематичного створення резервних копій значно ускладнює або унеможливлює відновлення інформації після кібератак, зокрема атак із використанням програм-вимагачів [31, С. 306].

Таким чином, комплексне врахування технічних, організаційних, фізичних та операційних вразливостей є необхідною умовою формування ефективної системи інформаційної безпеки підприємства в контексті забезпечення його економічної безпеки.

Операційні вразливості можуть бути суттєво знижені завдяки систематичному аналізу ризиків, безперервному моніторингу інформаційних процесів, а також регулярному перегляду та вдосконаленню процедур управління інформаційною безпекою. Такий підхід дозволяє своєчасно виявляти відхилення у роботі системи та запобігати виникненню інцидентів, що можуть вплинути на стабільність діяльності підприємства.

Загалом, запропонована класифікація вразливостей інформаційних систем на технічні, організаційні, фізичні та операційні створює методологічну основу для ідентифікації слабких місць, які потенційно можуть бути використані зловмисниками. Вона також сприяє формуванню комплексного підходу до побудови системи кіберзахисту підприємства. Кожна з визначених груп вразливостей потребує окремих управлінських, технічних та організаційних рішень, що дозволяє розробити цілісну та ефективну стратегію інформаційної безпеки.

У сучасних умовах цифрової трансформації розвиток інформаційних технологій одночасно створює нові можливості для бізнесу та формує

додаткові ризики. Вразливості інформаційних систем безпосередньо впливають на економічну стійкість підприємств, оскільки будь-які інциденти у сфері кібербезпеки можуть призводити до значних фінансових втрат. До таких наслідків належать витрати на відновлення систем, втрати інформаційних ресурсів, зниження ділової репутації, судові витрати та штрафні санкції, що в сукупності формують суттєве фінансове навантаження на підприємство.

З економічної точки зору класифікація вразливостей дозволяє підприємствам більш обґрунтовано оцінювати рівень ризиків та планувати заходи щодо їх мінімізації. Різні типи вразливостей мають неоднаковий характер впливу на фінансові результати діяльності підприємства, що зумовлює необхідність диференційованого підходу до управління ними.

Технічні вразливості, зокрема недоліки програмного забезпечення та інформаційних систем, характеризуються найбільш відчутними економічними наслідками, оскільки саме вони найчастіше стають причиною кіберінцидентів і прямого фінансового збитку. Основні економічні наслідки технічних вразливостей включають:

1. Витрати на відновлення інформаційних систем. Усунення наслідків експлуатації технічних вразливостей потребує залучення кваліфікованих фахівців, оновлення програмного забезпечення та відновлення даних. У випадках масштабних інцидентів вартість відновлення може сягати значних сум, включаючи витрати на аудит, модернізацію та усунення наслідків атак [32].

2. Втрати продуктивності та доходів. Порушення роботи інформаційних систем призводить до простоїв у діяльності підприємства, що безпосередньо впливає на рівень доходів. Особливо критичними такі наслідки є для підприємств, які надають цифрові або онлайн-послуги [33].

3. Зростання страхових витрат. Підвищення рівня кіберризиків змушує компанії активніше використовувати кіберстрахування, що, у свою

чергу, збільшує регулярні витрати на забезпечення безпеки інформаційних активів.

4. Регуляторні штрафи та санкції. У разі витоку або компрометації даних підприємство може нести фінансову відповідальність відповідно до чинного законодавства. Наприклад, у межах GDPR штрафи можуть досягати до 4% річного обороту компанії [34].

Організаційні вразливості, що пов’язані з управлінням персоналом та внутрішніми політиками безпеки, також мають значний вплив на економічну ефективність підприємства. Основні наслідки включають:

1. Втрати через неефективне управління доступом. Відсутність належної системи розмежування прав доступу підвищує ризик інсайдерських загроз, які часто мають значні фінансові наслідки та потребують складного розслідування [35].

2. Витрати на навчання персоналу. Формування належного рівня кіберобізнаності потребує регулярних інвестицій у навчальні програми, тренінги та підвищення кваліфікації працівників.

3. Збитки від соціальної інженерії та фішингових атак. Успішні атаки цього типу призводять до витоку конфіденційної інформації, фінансових втрат та додаткових витрат на відновлення систем і репутації [36].

Фізичні вразливості, пов’язані з доступом до приміщень і технічної інфраструктури, також мають прямий економічний вимір:

1. Витрати на фізичний захист інфраструктури. Забезпечення охорони приміщень, систем контролю доступу та відеоспостереження потребує постійних інвестицій, однак є необхідною умовою запобігання втратам обладнання та даних.

2. Фінансові ризики природних та техногенних факторів. Наслідки надзвичайних ситуацій можуть призводити до значних збитків, тому підприємства змушені інвестувати у резервні центри обробки даних та системи аварійного відновлення.

Операційні вразливості безпосередньо впливають на здатність підприємства ефективно реагувати на інциденти та підтримувати безперервність бізнес-процесів:

1. Недостатній рівень інвестицій у моніторинг безпеки. Відсутність систем постійного контролю призводить до пізнього виявлення атак і, як наслідок, збільшення фінансових втрат через тривалий період їх впливу.

2. Витрати на резервне копіювання та відновлення даних. Хоча впровадження систем резервного копіювання потребує додаткових витрат, воно є критично важливим для забезпечення безперервності діяльності підприємства.

3. Фінансові наслідки недотримання стандартів безпеки. Порушення внутрішніх або міжнародних вимог може призводити до штрафів, судових витрат та компенсаційних виплат контрагентам [37].

Таким чином, у сукупності технічні, організаційні, фізичні та операційні вразливості формують багаторівневу систему ризиків, яка безпосередньо впливає на економічну безпеку підприємства та потребує комплексного, системного підходу до управління.

Кожен із типів вразливостей інформаційних систем по-різному впливає на фінансово-економічні показники діяльності підприємства. Порушення у сфері кібербезпеки, як правило, супроводжуються значними прямими та непрямими витратами, що включають відновлення працездатності інформаційних систем, відновлення або відтворення втрачених даних, оплату послуг зовнішніх спеціалістів з кібербезпеки, а також модернізацію захисної інфраструктури. Додатково, у разі витоку або компрометації критично важливої інформації, підприємство зазнає опосередкованих збитків, пов’язаних із втратою конкурентних позицій та зниженням рівня довіри з боку клієнтів і партнерів.

Своєчасне виявлення, оцінювання та класифікація вразливостей є важливим елементом управління кіберризиками, оскільки дозволяє не лише зменшити ймовірність реалізації загроз, але й оптимізувати витрати на

впровадження заходів захисту. Це також сприяє зниженню потенційних фінансових втрат, пов’язаних із штрафними санкціями та іншими видами юридичної відповідальності за недотримання вимог законодавства у сфері захисту інформації та персональних даних.

Додатковий економічний ефект від належного управління вразливостями проявляється у підвищенні стабільності фінансових потоків підприємства та раціоналізації витрат на інформаційні технології. Впровадження ефективної системи кіберзахисту дозволяє мінімізувати ризики виникнення непередбачуваних витрат, пов’язаних із зупинкою бізнес-процесів, відновленням діяльності після інцидентів або виплатою компенсацій контрагентам. Водночас належний рівень інформаційної безпеки сприяє зміцненню довіри з боку клієнтів і партнерів, що є важливим чинником забезпечення стабільних доходів та розширення ринкових позицій підприємства в довгостроковій перспективі.

Таблиця 2.2. Комплексна модель впливу інформаційних загроз на діяльність підприємства

Рівень впливу	Джерело загрози	Механізм впливу	Наслідки для підприємства	Економічний ефект
Технічний	кібератаки, збій ПЗ	порушення роботи систем	зупинка процесів	прямі фінансові втрати
Організаційний	помилки персоналу	неправильні дії користувачів	витік даних	штрафи, витрати на відновлення
Інформаційний	фішинг, витік даних	компрометація доступу	втрата конфіденційності	репутаційні втрати
Інфраструктурний	відмова серверів	фізичне/логічне пошкодження	недоступність сервісів	втрата доходу
Зовнішній	DDoS, ransomware	цілеспрямовані атаки	блокування бізнесу	зупинка операцій

Таким чином, інвестування у систему інформаційної безпеки слід розглядати не лише як витрати на захист інформаційних ресурсів, а й як стратегічно обґрунтований напрям забезпечення економічної безпеки підприємства, його стійкого розвитку, збереження ділової репутації та підвищення конкурентоспроможності.

2.3. Економічні наслідки загроз інформаційній безпеці в системі економічної безпеки підприємств

У сучасних умовах цифровізації економіки українські підприємства все активніше використовують інформаційні технології як базовий інструмент організації та управління господарською діяльністю. Використання сучасних інформаційних систем, зокрема ERP-систем (Enterprise Resource Planning), CRM-платформ (Customer Relationship Management) та інших спеціалізованих програмних рішень, забезпечує комплексну автоматизацію бізнес-процесів, підвищує оперативність прийняття управлінських рішень і сприяє більш ефективному використанню ресурсів. У результаті цього підвищується узгодженість роботи структурних підрозділів, зменшуються трансакційні витрати, покращується якість взаємодії з клієнтами, що загалом позитивно впливає на конкурентоспроможність підприємства.

Водночас посилення залежності бізнесу від інформаційних систем обумовлює зростання вразливості до різноманітних загроз інформаційної безпеки. Порушення функціонування інформаційної інфраструктури може призводити до втрати критично важливих даних, спотворення управлінської інформації або обмеження доступу до ключових ресурсів. Найпоширенішими є кібератаки, спрямовані на порушення базових властивостей інформації – конфіденційності, цілісності та доступності. При цьому сучасні методи атак включають як технічні інструменти (шкідливе програмне забезпечення, експлуатація вразливостей), так і соціально-інженерні підходи, що ускладнює їх виявлення та нейтралізацію.

Окрему групу ризиків становлять загрози несанкціонованого доступу до інформаційних ресурсів підприємства. У таких випадках можливе розголошення комерційної таємниці, викрадення баз даних клієнтів або порушення прав інтелектуальної власності. Це не лише створює прямі фінансові ризики, а й формує додаткові юридичні наслідки. Зокрема, відповідно до положень законодавства України у сфері захисту персональних даних, суб’єкти господарювання несуть відповідальність за неналежне

забезпечення захисту інформації, що може супроводжуватися застосуванням фінансових санкцій та штрафів.

Загрози інформаційній безпеці підприємств безпосередньо трансформуються в економічні втрати різного характеру. До них належать прямі витрати на ліквідацію наслідків інцидентів, відновлення інформаційних систем, залучення зовнішніх експертів з кібербезпеки, а також непрямі втрати, пов’язані зі зниженням продуктивності та перериванням бізнес-процесів. У випадку масштабних інцидентів, зокрема кібератак, можливе тимчасове призупинення операційної діяльності підприємства, що призводить до втрати доходів і послаблення ринкових позицій [38, С. 60].

Важливим аспектом економічних наслідків є також репутаційний ризик. У сучасному інформаційному середовищі негативна інформація про витоки даних або кібератаки поширюється надзвичайно швидко, що суттєво впливає на сприйняття компанії з боку клієнтів, партнерів та інвесторів. Втрата довіри, як правило, має довгостроковий характер і може призводити до скорочення клієнтської бази, зменшення обсягів продажів та ускладнення залучення нових партнерів.

Таким чином, загрози інформаційній безпеці підприємств формують багаторівневу систему економічних ризиків, які охоплюють як прямі фінансові втрати, так і опосередковані наслідки у вигляді втрати репутації та ринкових позицій. Це зумовлює необхідність розгляду інформаційної безпеки як невід’ємного елементу системи економічної безпеки підприємства та формування комплексних підходів до управління відповідними ризиками в умовах цифрової трансформації економіки.

Основні економічні наслідки інформаційних загроз:

1. *Прямі фінансові втрати.* Інформаційні загрози можуть спричиняти суттєві фінансові втрати для підприємств, які пов’язані з ліквідацією наслідків інцидентів, відновленням працездатності інформаційних систем, а також компенсацією недоотриманих доходів

унаслідок простоїв. Як приклад, можна навести ситуацію з ПриватБанком, який у 2022 році зазнав кібератак, що призвело до часткового порушення роботи інформаційних систем і ускладнення надання банківських послуг клієнтам. У результаті інциденту банк був змушений спрямувати значні ресурси на відновлення стабільності операційної діяльності, зокрема на залучення кіберфахівців, аналіз причин атаки та модернізацію систем захисту [39].

Додатково показовим є інцидент із вірусом NotPetya у 2017 році, який охопив значну кількість українських підприємств, зокрема НАК «Нафтогаз України». Внаслідок атаки було заблоковано доступ до ключових інформаційних систем, що спричинило значні витрати на ліквідацію наслідків інциденту та подальше посилення кіберзахисту. Це негативно вплинуло на фінансові результати компаній, оскільки витрати включали як прямі втрати, так і довгострокові інвестиції у безпеку [40].

2. *Втрати продуктивності.* Інформаційні загрози також істотно знижують рівень продуктивності підприємств. Особливо це проявляється у випадках, коли кібератаки або технічні збої блокують доступ до даних, порушують роботу окремих підрозділів або повністю зупиняють виробничі процеси. Прикладом є ситуація з компанією «Прикарпаттяобленерго», яка у 2015 році стала об’єктом кібератаки, що призвело до тимчасового припинення електропостачання на окремих ділянках мережі. Це спричинило як прямі економічні втрати, так і суттєві репутаційні наслідки [41].

Зниження продуктивності внаслідок інформаційних інцидентів потребує додаткових витрат на відновлення роботи систем, залучення фахівців, а також навчання персоналу з метою недопущення подібних випадків у майбутньому. У сукупності це підвищує загальний рівень витрат підприємства та потребує врахування у фінансовому плануванні.

3. *Репутаційні втрати.* Економічні наслідки інформаційних загроз також включають втрату ділової репутації, яка хоча і є непрямим фактором, однак має значний вплив на ринкові позиції підприємства. У випадку витоку

конфіденційної інформації або інших інцидентів інформаційної безпеки підприємство ризикує втратити довіру клієнтів і партнерів, що призводить до зменшення обсягів продажів і відтоку споживачів до конкурентів. Наприклад, у 2018 році один з українських ритейлерів зазнав репутаційних втрат унаслідок витоку даних клієнтських транзакцій, що негативно вплинуло на рівень довіри до бренду та його позиції на ринку [42].

Репутаційні втрати також зумовлюють додаткові економічні витрати, пов’язані з необхідністю відновлення іміджу компанії. Це включає витрати на маркетингові кампанії, посилення заходів кіберзахисту та реалізацію програм підвищення лояльності клієнтів. Відновлення репутації зазвичай є тривалим процесом.

4. *Витрати на забезпечення інформаційної безпеки.* З метою запобігання негативним економічним наслідкам інформаційних загроз підприємства змушені інвестувати значні кошти у розвиток систем кіберзахисту. Наприклад, НАК «Нафтогаз України» після масштабних кібератак суттєво збільшила фінансування заходів інформаційної безпеки. До таких витрат належать впровадження систем моніторингу загроз, резервного копіювання, навчання персоналу та модернізація захисної інфраструктури.

Подібну практику застосовують і інші українські підприємства, зокрема аграрні холдинги, такі як «Миронівський хлібопродукт» (МХП), діяльність яких пов’язана з великими обсягами даних та складними логістичними процесами. Інвестиції у кібербезпеку для таких компаній є критично важливими для забезпечення безперервності діяльності та зниження ризиків інформаційних інцидентів. Витрати включають закупівлю спеціалізованого програмного та апаратного забезпечення, аудит систем безпеки та підтримку резервної інфраструктури [43].

Таким чином, аналіз економічних наслідків інформаційних загроз на прикладі українських підприємств свідчить про їх багаторівневий вплив. Кібератаки, витоки даних і порушення роботи інформаційних систем спричиняють як прямі, так і опосередковані фінансові втрати. Прямі витрати

пов’язані з ліквідацією наслідків інцидентів, відновленням даних та забезпеченням безперервності діяльності, які в окремих випадках можуть досягати значних обсягів і суттєво впливати на фінансовий стан підприємств.

Опосередковані економічні наслідки інформаційних загроз, до яких належать зниження продуктивності, репутаційні втрати та витрати на забезпечення кібербезпеки, також мають суттєве значення у формуванні загального рівня витрат підприємства. Падіння продуктивності, що виникає внаслідок кібератак, зазвичай пов’язане з порушенням або уповільненням ключових бізнес-процесів, що, у свою чергу, призводить до скорочення обсягів виробництва та зменшення доходів. Найбільш відчутним цей вплив є для підприємств виробничого та сервісного секторів, де безперервність операцій і швидкість реагування визначають ефективність діяльності.

Репутаційні втрати, які формуються внаслідок інформаційних інцидентів, можуть мати довгостроковий економічний ефект. Зниження рівня довіри з боку клієнтів і ділових партнерів часто супроводжується відтоком споживачів та скороченням обсягів реалізації продукції або послуг, що негативно позначається на фінансових результатах підприємства. За оцінками експертів, процес відновлення ділової репутації після кібератаки потребує значних фінансових ресурсів і може становити приблизно 20–30% від загальних витрат, пов’язаних із ліквідацією наслідків інциденту.

В умовах посилення кіберзагроз українські підприємства змушені розробляти та впроваджувати комплексні стратегії захисту інформації, що виступають важливим елементом забезпечення економічної стійкості та конкурентоспроможності. Інвестиції у сферу кібербезпеки поступово набувають характеру не лише витрат, а й стратегічних вкладень у довгостроковий розвиток бізнесу. Сучасні системи кіберзахисту, що поєднують технічні та організаційні рішення, дають змогу зменшити ймовірність реалізації загроз і мінімізувати потенційні фінансові втрати.

Формування внутрішніх підрозділів інформаційної безпеки, а також залучення зовнішніх експертів у сфері кіберзахисту є ефективними

інструментами підвищення рівня захищеності підприємств. Це дозволяє забезпечити як захист критично важливих даних, так і стабільність функціонування бізнес-процесів у разі виникнення загроз. У практичному вимірі такі інвестиції можуть бути економічно виправданими, оскільки сприяють уникненню значно більших втрат унаслідок можливих кібератак.

Таблиця 2.3. Оцінка економічної значущості інформаційних загроз для підприємства

Група загроз	Ймовірність реалізації	Рівень фінансового впливу	Тривалість наслідків	Рівень критичності
Кібератаки (ransomware, DDoS)	висока	дуже високий	коротко-/середньостроковий	критичний
Витоки даних	середня	високий	довгостроковий	високий
Помилки персоналу	висока	середній	короткостроковий	середній
Збої систем	середня	середній	короткий	середній
Природні катастрофи	низька	дуже високий	довгостроковий	критичний

Таким чином, для українських підприємств інформаційна безпека має розглядатися як невід’ємна складова загальної стратегії розвитку бізнесу. Системне управління ризиками інформаційних загроз є ключовою умовою забезпечення економічної стійкості, адаптивності до змін зовнішнього середовища та підтримання конкурентних позицій на ринку.

РОЗДІЛ 3. СИСТЕМА СТРАТЕГІЧНОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК СКЛАДОВА ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

3.1. Формування стратегій управління інформаційними ризиками підприємства

У сучасних умовах глобалізації економічних процесів та активного розвитку цифрових технологій інформація набуває статусу ключового стратегічного ресурсу, який безпосередньо визначає рівень конкурентоспроможності та ефективності діяльності підприємств. Особливо це стосується українських суб'єктів господарювання, які функціонують в умовах динамічних змін ринкового середовища та потреби впровадження інноваційних підходів до управління. Зі зростанням обсягів інформаційних потоків і розширенням використання цифрових технологій питання ефективного управління інформаційними ризиками набуває особливої актуальності, оскільки їх недооцінка або ігнорування може спричинити значні фінансові втрати, погіршення репутації та зниження ринкових позицій підприємства.

Управління інформаційними ризиками являє собою комплекс взаємопов'язаних процесів і процедур, спрямованих на виявлення, аналіз, оцінювання та мінімізацію ризиків, що виникають у процесі використання інформаційних ресурсів підприємства. До складу інформаційних активів відносять усі види даних, електронні інформаційні масиви, бази даних, програмні продукти, а також інфраструктуру, що забезпечує їх обробку, зберігання та передачу. Виникнення ризиків у цій сфері може бути зумовлене як зовнішніми факторами (кібератаки, витоки інформації, несанкціонований доступ), так і внутрішніми причинами (низький рівень цифрової грамотності персоналу, недосконаліть внутрішніх регламентів та політик безпеки) [44].

Ефективні стратегії управління інформаційними ризиками передбачають не лише попередження можливих втрат, а й формування

здатності підприємства до адаптації в умовах реалізації загроз. Такий підхід забезпечує підвищення стійкості організації до впливу інформаційних інцидентів, до яких належать збої в роботі інформаційних систем, витоки конфіденційних даних та кібератаки різного рівня складності. Підприємства, які впроваджують системні підходи до управління інформаційними ризиками, як правило, демонструють вищу швидкість відновлення після інцидентів та збереження довіри з боку клієнтів і партнерів.

Крім того, впровадження системи управління інформаційними ризиками сприяє не лише зниженню ймовірності реалізації загроз, але й загальному підвищенню рівня інформаційної безпеки підприємства. Ключовими етапами цього процесу є ідентифікація потенційних загроз, оцінювання ймовірності їх виникнення та визначення можливих наслідків, а також розроблення та впровадження заходів реагування і нейтралізації [45]. У результаті стратегії управління інформаційними ризиками стають невід'ємним елементом забезпечення стабільного функціонування та розвитку підприємств в умовах високої невизначеності бізнес-середовища.

Початковим етапом формування ефективної системи управління інформаційними ризиками є їх ідентифікація, що передбачає систематичне виявлення потенційних загроз, здатних негативно вплинути на інформаційні активи підприємства. В умовах активної цифровізації бізнес-процесів та зростання залежності підприємств від інформаційних систем якісна ідентифікація ризиків виступає важливою передумовою забезпечення стабільності та конкурентоспроможності. Вона охоплює не лише фіксацію наявних загроз, але й прогнозування можливих наслідків їх реалізації [46].

Інформаційні ризики характеризуються різноманітністю проявів: від технічних збоїв, що виникають через апаратні несправності або програмні помилки, до цілеспрямованих кібератак, спрямованих на отримання несанкціонованого доступу до конфіденційної інформації. При цьому важливо враховувати, що ризики в інформаційній сфері умовно поділяються

на зовнішні та внутрішні, що зумовлює різні підходи до їх виявлення, оцінювання та управління.

Зовнішні ризики переважно формуються під впливом діяльності сторонніх суб'єктів та факторів зовнішнього середовища. До цієї групи належать:

1. *Кібератаки***.** Однією з найбільш небезпечних загроз у сучасному інформаційному середовищі залишаються кібератаки, які можуть реалізовуватися у різних формах. Зокрема, атаки типу «відмова в обслуговуванні» (DDoS) спрямовані на перевантаження серверної інфраструктури підприємства, що призводить до тимчасової недоступності інформаційних ресурсів і, як наслідок, до фінансових втрат. Фішингові атаки базуються на використанні підроблених повідомлень або вебресурсів з метою отримання конфіденційних даних користувачів, таких як логіни та паролі, при цьому рівень їхньої складності постійно зростає, що ускладнює виявлення. Окрему загрозу становить шкідливе програмне забезпечення (ransomware), яке обмежує доступ до інформації до моменту сплати викупу; за оцінками досліджень, витрати на ліквідацію наслідків таких атак можуть досягати мільйонних значень у валютному еквіваленті.

2. *Витоки даних.* Несанкціоноване розкриття інформації є наслідком як зовнішніх атак, спрямованих на використання вразливостей програмного забезпечення, так і внутрішніх порушень правил доступу. Сучасна практика демонструє, що масштабні інциденти витоку даних у великих організаціях призводять до компрометації персональної інформації значної кількості користувачів, що підкреслює критичність даної проблеми. Подібні інциденти супроводжуються значними фінансовими втратами, а також суттєвими репутаційними наслідками для підприємств.

3. *Природні катастрофи.* Стихійні явища, такі як повені, землетруси чи інші надзвичайні події природного характеру, можуть завдавати значної шкоди фізичній інфраструктурі підприємств, включаючи серверне обладнання та системи зберігання даних. Витрати на відновлення

після таких подій зазвичай є значними, тому організації змушені заздалегідь формувати плани безперервності бізнесу та реагування на надзвичайні ситуації з метою мінімізації потенційних втрат [47, С. 47-48].

Внутрішні ризики формуються безпосередньо в межах організації та пов'язані з особливостями її функціонування:

1. *Людський фактор.* Одним із ключових джерел внутрішніх загроз є людські помилки, що виникають через недостатній досвід, неуважність або недотримання встановлених процедур. До таких ситуацій належать випадкове надсилання конфіденційних матеріалів не тому адресату або порушення правил доступу до інформаційних ресурсів. Додатковим ризиком виступає недостатній рівень підготовки персоналу у сфері кібербезпеки, що знижує загальну обізнаність щодо важливості захисту інформаційних активів.

2. *Недостатність або відсутність політик інформаційної безпеки.* Організації, які не впровадили чітко регламентовані політики безпеки або не забезпечують контроль за їх виконанням, формують додаткові ризики для інформаційних систем. Відсутність стандартизованих процедур щодо обробки, зберігання та доступу до конфіденційних даних підвищує ймовірність виникнення інцидентів безпеки та несанкціонованого доступу.

3. *Технічні збої в інформаційних системах.* Порушення роботи апаратного або програмного забезпечення може спричиняти втрату даних або тимчасове припинення функціонування бізнес-процесів. Такі збої негативно впливають на операційну діяльність підприємства та можуть призводити до фінансових втрат, особливо у випадках тривалого простою критичних систем [48].

Таким чином, комплексне усвідомлення структури інформаційних ризиків та їх своєчасна ідентифікація є ключовими передумовами формування ефективної системи управління ризиками в межах підприємства. Процес ідентифікації повинен носити безперервний характер і передбачати участь усіх рівнів управління, а також регулярний моніторинг змін у

зовнішньому та внутрішньому середовищі. Враховуючи динамічний характер розвитку інформаційних технологій, підприємства мають постійно адаптувати підходи до управління ризиками, що дозволяє зменшувати рівень вразливості та підвищувати загальну ефективність системи інформаційної безпеки.

Після етапу ідентифікації інформаційних ризиків наступною ключовою складовою процесу управління є їх оцінювання. Оцінка ризиків виступає важливою аналітичною процедурою, що дозволяє підприємству визначити потенційний рівень загроз та їх можливий вплив на результати діяльності. У сучасних умовах цифровізації бізнес-процесів це має особливе значення, оскільки порушення в інформаційних системах можуть спричиняти суттєві фінансові втрати, операційні збої та репутаційні ризики [49, С. 63].

Застосування оцінки ризиків дає змогу підприємствам не лише виявити найбільш критичні загрози, але й сформувати обґрунтовані управлінські рішення щодо їх мінімізації. Зокрема, дана процедура забезпечує:

1. *Визначення пріоритетності загроз.* Оцінювання ризиків дозволяє встановити, які з них потребують першочергового реагування. Наприклад, у разі виявлення загрози, що потенційно може спричинити значні фінансові втрати або зупинку бізнес-процесів, підприємство зосереджує ресурси на її оперативному усуненні.

2. *Раціоналізацію використання ресурсів.* На основі визначених пріоритетів підприємство має можливість більш ефективно розподіляти фінансові, технічні та кадрові ресурси, концентруючи увагу на найбільш критичних ризиках і уникаючи надмірних витрат на другорядні загрози.

3. *Підвищення рівня обізнаності персоналу.* Оцінка ризиків сприяє формуванню усвідомлення потенційних загроз серед працівників, що є важливим елементом загальної системи інформаційної безпеки, оскільки значна частина інцидентів пов’язана з людським фактором [50].

У практиці управління інформаційними ризиками застосовуються різні методичні підходи до їх оцінювання, серед яких найбільш поширеними є кількісний та якісний.

Кількісний підхід базується на використанні числових показників і дозволяє формалізувати рівень ризику. Його реалізація включає такі етапи:

1. *Визначення ймовірності настання ризику.* На цьому етапі здійснюється оцінка частоти виникнення загрози на основі статистичних даних, історичних інцидентів або аналітичного моделювання. Наприклад, регулярність кіберінцидентів може слугувати базою для оцінки ймовірності їх повторення.

2. *Оцінювання можливих фінансових наслідків.* Визначаються потенційні втрати у разі реалізації ризику, включаючи витрати на відновлення систем, компенсації клієнтам, втрати доходів через простої та інші економічні наслідки.

3. *Розрахунок інтегрального рівня ризику.* Узагальнений показник визначається як добуток ймовірності настання події та величини можливих втрат: *Ризик = Ймовірність × Втрати.* Такий підхід забезпечує кількісне уявлення про ступінь впливу ризику на діяльність підприємства [51, С. 11–112].

Якісний підхід ґрунтується на експертному оцінюванні та класифікації ризиків за рівнями значущості (високий, середній, низький). Він застосовується у випадках, коли відсутні достатні статистичні дані для точного розрахунку.

1. *Експертне оцінювання.* До процесу залучаються фахівці з інформаційної безпеки, які на основі професійного досвіду визначають ймовірність та потенційний вплив ризиків.

2. *SWOT-аналіз.* Використання даного інструменту дозволяє комплексно оцінити сильні та слабкі сторони підприємства, а також зовнішні можливості і загрози, що сприяє більш системному розумінню ризикового середовища [52].

Результати оцінювання ризиків створюють основу для формування пріоритетів управління та розробки відповідних заходів реагування. У процесі аналізу можуть бути виявлені ризики, які раніше недооцінювалися, проте фактично мають високий рівень загрозливості та потенційно значний вплив на діяльність підприємства.

Таким чином, етап оцінки ризиків є необхідним елементом системи управління інформаційною безпекою, що забезпечує обґрунтованість управлінських рішень, оптимізацію використання ресурсів та підвищення загальної стійкості підприємства до інформаційних загроз. В умовах динамічного розвитку інформаційного середовища регулярне оцінювання ризиків набуває стратегічного значення для забезпечення стабільного функціонування та конкурентоспроможності підприємств.

Стратегії управління інформаційними ризиками є ключовим елементом системи забезпечення інформаційної безпеки підприємства. Їх основне призначення полягає не лише у виявленні та оцінюванні потенційних загроз, але й у формуванні комплексу управлінських заходів, спрямованих на їх мінімізацію або контроль. У теорії ризик-менеджменту виділяють декілька базових підходів до управління ризиками, зокрема: уникнення, зниження, прийняття та передача ризиків [53].

1. Уникнення ризиків. Уникнення ризиків розглядається як одна з найбільш превентивних стратегій, що передбачає зміну бізнес-процесів, технологічної інфраструктури або організаційних підходів з метою повного усунення потенційної загрози або суттєвого зменшення ймовірності її виникнення. Дана стратегія базується на принципі пріоритетності попередження ризиків над ліквідацією їх наслідків [54].

Наприклад, підприємства можуть відмовлятися від використання застарілих програмних рішень або інформаційних систем, які містять відомі вразливості, та переходити на сучасні платформи, що відповідають актуальним стандартам кібербезпеки.

2. Зниження ризиків. Стратегія зниження ризиків передбачає впровадження організаційних, технічних та процедурних заходів, спрямованих на зменшення ймовірності реалізації загроз або пом’якшення їх наслідків. Важливу роль у цьому процесі відіграє людський фактор, оскільки значна частина інцидентів у сфері інформаційної безпеки пов’язана з діями персоналу [55].

Зокрема, ефективним інструментом є регулярне навчання працівників з питань кібербезпеки, включаючи розпізнавання фішингових атак, правил роботи з конфіденційною інформацією та дотримання політик безпеки.

3. Прийняття ризиків. Прийняття ризику застосовується у випадках, коли витрати на його мінімізацію перевищують потенційні економічні втрати від можливого інциденту. Такий підхід є доцільним за умови обмеженості ресурсів або низького рівня критичності ризику для діяльності підприємства [56].

У таких випадках організація свідомо залишає ризик без активного впливу, однак формує резервні механізми реагування, включаючи плани відновлення діяльності та процедури реагування на інциденти.

4. Передача ризиків. Передача ризиків передбачає делегування частини відповідальності за наслідки ризикових подій третім сторонам. Найчастіше це реалізується через страхування кіберризиків або залучення зовнішніх провайдерів послуг інформаційної безпеки [57].

Наприклад, підприємство може передати функції моніторингу та реагування на кіберінциденти спеціалізованій компанії або застрахувати потенційні фінансові втрати, пов’язані з витоком даних чи кібератаками.

Отже, зазначені стратегії формують комплексну систему управління інформаційними ризиками, яка забезпечує гнучкість реагування підприємства на різні типи загроз. Їх практичне застосування дозволяє не лише підвищити рівень інформаційної безпеки, але й зменшити потенційні економічні втрати та забезпечити стабільність функціонування бізнесу в умовах динамічного цифрового середовища.

Водночас сучасні інформаційні технології виступають важливим інструментом реалізації стратегій управління ризиками, забезпечуючи багаторівневий захист інформаційних активів, автоматизацію процесів моніторингу та оперативне реагування на інциденти. Використання технологій шифрування, систем контролю доступу та спеціалізованого програмного забезпечення дозволяє підприємствам підвищувати ефективність системи кіберзахисту.

Таким чином, формування та впровадження стратегій управління інформаційними ризиками є невід'ємною складовою забезпечення економічної безпеки підприємства, оскільки вони безпосередньо впливають на рівень захищеності інформаційних активів, фінансову стабільність та конкурентоспроможність організації.

В умовах динамічного розвитку інформаційного середовища підприємства змушені функціонувати в умовах постійного виникнення нових кіберзагроз, які здатні безпосередньо впливати на їх фінансово-економічні результати. Зокрема, реалізація кібератак може спричиняти суттєві економічні втрати, пов'язані як із витратами на відновлення працездатності інформаційних систем, так і з непрямими втратами, зумовленими зниженням рівня довіри з боку клієнтів і ділових партнерів. У цьому контексті оцінка ризиків виступає інструментом раннього виявлення найбільш критичних загроз, що впливають на економічну стабільність підприємства, та створює підґрунтя для формування ефективних механізмів їх нейтралізації.

Систематичне проведення оцінки ризиків є невід'ємним елементом сучасної стратегії забезпечення економічної безпеки підприємства в частині інформаційного захисту. Такий підхід дозволяє не лише мінімізувати ймовірність реалізації кіберінцидентів, але й підвищити загальну стійкість бізнесу до зовнішніх і внутрішніх деструктивних впливів. Практика свідчить, що підприємства, які впроваджують комплексні системи управління інформаційними ризиками, демонструють вищий рівень захищеності активів та зниження потенційних фінансових втрат у довгостроковій перспективі.

Крім того, належна оцінка ризиків виконує функцію економічного інструменту зміцнення ринкових позицій підприємства. Вона формує передумови для підвищення рівня довіри з боку клієнтів, інвесторів та партнерів, оскільки свідчить про здатність організації ефективно управляти загрозами інформаційній безпеці. У результаті це сприяє підвищенню конкурентоспроможності підприємства та забезпеченню його стабільного розвитку в умовах сучасного висококонкурентного бізнес-середовища.

3.2. Організаційні інструменти зміцнення інформаційної безпеки підприємства

Організаційні інструменти відіграють визначальну роль у формуванні цілісної системи інформаційної безпеки підприємства, оскільки саме вони забезпечують упорядкування процесів захисту інформаційних ресурсів та координацію дій персоналу. В умовах цифрової трансформації економіки та постійного ускладнення кіберзагроз підприємства змушені адаптувати свої внутрішні управлінські механізми до нових викликів. З огляду на зростаючу цінність інформації як ключового нематеріального активу, неналежний рівень її захисту може призводити до суттєвих фінансових втрат, втрати ділової репутації та зниження довіри з боку контрагентів і клієнтів.

Організаційні інструменти забезпечення інформаційної безпеки спрямовані на формування системного підходу до управління інформаційними активами підприємства та гарантування їхньої конфіденційності, цілісності й доступності. У сучасних умовах їх значення посилюється необхідністю безперервного функціонування бізнес-процесів, мінімізації впливу внутрішніх і зовнішніх загроз, а також забезпечення стабільності економічної діяльності підприємства. Основною метою застосування організаційних інструментів є зниження рівня інформаційних ризиків, забезпечення стійкості бізнес-процесів та зміцнення економічної безпеки суб’єкта господарювання.

Таблиця 3.1 Класифікація організаційних інструментів забезпечення інформаційної безпеки

Група інструментів	Зміст	Основна мета
Інституційні	Створення підрозділів, визначення відповідальних осіб	Формування структури управління ІБ
Процедурні	Регламенти, політики, інструкції	Стандартизація процесів безпеки
Контрольні	Аудит, моніторинг, перевірки	Виявлення та запобігання порушенням
Мотиваційні	Система стимулювання персоналу	Зниження людських ризиків
Інформаційно-просвітницькі	Навчання, тренінги	Підвищення обізнаності персоналу

Ключові завдання організаційних інструментів можна деталізувати таким чином:

1. *Формування внутрішніх політик і регламентів інформаційної безпеки.* Передбачає розробку комплексу нормативних документів, які визначають правила обробки, зберігання та захисту інформації на підприємстві. Такі політики встановлюють стандарти поведінки користувачів, вимоги до використання інформаційних систем та механізми контролю їх дотримання.

2. *Створення системи управління інформаційною безпекою.* Йдеться про побудову організаційної структури, що забезпечує координацію заходів безпеки на всіх рівнях управління. Це включає визначення відповідальних осіб, розподіл функцій між підрозділами та формування механізмів внутрішнього контролю.

3. *Управління та оцінювання інформаційних ризиків.* Організаційні інструменти передбачають постійне виявлення потенційних загроз, аналіз їх ймовірності та можливих наслідків для діяльності підприємства. На основі отриманих результатів формуються управлінські рішення щодо мінімізації ризиків.

4. *Розвиток корпоративної культури інформаційної безпеки.* Важливим елементом є підвищення рівня обізнаності працівників щодо кіберзагроз і правил безпечної роботи з інформацією. Це досягається шляхом

проведення навчань, інструктажів і тренінгів, що зменшує вплив людського фактора.

5. *Організація моніторингу та внутрішнього контролю.* Передбачає регулярне спостереження за станом інформаційних систем, перевірку дотримання встановлених політик безпеки та проведення внутрішніх аудитів з метою виявлення потенційних слабких місць.

6. *Формування процедур реагування на інциденти***.** Необхідним елементом є розробка чітких алгоритмів дій у разі виникнення кіберінцидентів, включаючи порядок їх виявлення, локалізації та ліквідації наслідків, а також визначення відповідальності персоналу.

7. *Забезпечення нормативно-правової відповідності.* Організаційні інструменти мають враховувати вимоги чинного законодавства та міжнародних стандартів у сфері інформаційної безпеки, зокрема щодо захисту персональних даних та комерційної інформації.

У підсумку слід зазначити, що організаційні інструменти є невід’ємною складовою системи зміцнення інформаційної та економічної безпеки підприємства. Їх ефективне впровадження забезпечує зниження рівня ризиків, підвищення керованості інформаційних процесів і формування стійкої моделі функціонування підприємства в умовах сучасного цифрового середовища.

Мета та завдання організаційних інструментів забезпечення інформаційної безпеки підприємства полягають у формуванні багаторівневої системи управління захистом інформаційних активів, яка забезпечує їхню конфіденційність, цілісність та доступність у процесі господарської діяльності. У сучасних умовах цифрової трансформації економіки такі інструменти набувають стратегічного значення, оскільки безпосередньо впливають на рівень економічної безпеки підприємства, його фінансову стабільність та конкурентоспроможність.

Формування ефективної системи організаційного забезпечення інформаційної безпеки спрямоване на підтримання безперервності бізнес-

процесів, мінімізацію ймовірності реалізації кіберінцидентів, а також зниження потенційних фінансових втрат, що можуть виникати внаслідок порушення функціонування інформаційних систем. Досягнення зазначених цілей передбачає розробку внутрішніх регламентів і політик, закріплення відповідальності за інформаційну безпеку, впровадження системи навчання персоналу та постійний моніторинг рівня ризиків. У сукупності ці елементи формують цілісну організаційну модель управління інформаційною безпекою підприємства [73, С. 112–114].

Організаційні інструменти інформаційної безпеки виступають складовою системи економічної безпеки підприємства, оскільки дозволяють зменшити ризики втрати інформаційних активів, які мають пряму економічну цінність. Їх реалізація охоплює комплекс управлінських, контрольних та превентивних заходів, спрямованих на підвищення стійкості інформаційної інфраструктури до внутрішніх і зовнішніх загроз. Умовно такі інструменти поділяються на інституційні, процедурні, мотиваційні, інформаційно-освітні та контрольні, що взаємодіють між собою у межах єдиної системи управління безпекою [77].

Інституційні інструменти формують організаційно-управлінську основу системи інформаційної безпеки підприємства. Вони визначають структуру управління, розподіл функцій і рівень відповідальності, що є критично важливим для ефективного контролю інформаційних процесів.

Основні інституційні інструменти:

1. *Формування підрозділів з інформаційної безпеки.* На підприємстві доцільно створювати окремі структурні одиниці (служби або відділи інформаційної безпеки), які забезпечують постійний моніторинг стану захищеності інформаційних систем, аналіз інцидентів та впровадження заходів реагування. Це дозволяє централізувати управління кіберризиками та підвищити оперативність реагування на загрози.

2. *Призначення відповідальних осіб за напрямами безпеки.* Ефективна система управління передбачає розподіл відповідальності між

посадовими особами: керівник з інформаційної безпеки, фахівці з кіберзахисту, адміністратори систем та відповідальні за управління ризиками. Такий підхід забезпечує багаторівневий контроль та зменшує ймовірність системних помилок.

3. *Розробка політик та стандартів інформаційної безпеки.* Політики безпеки визначають правила доступу до інформаційних ресурсів, порядок обробки даних, вимоги до паролів, використання програмного забезпечення та регламент реагування на інциденти. Вони формують нормативну базу внутрішнього контролю та є основою для функціонування системи захисту [78].

Таблиця 3.2. Основні інституційні інструменти та їх функції

Інструмент	Зміст	Ефект для підприємства
Відділ інформаційної безпеки	Спеціалізований підрозділ	Централізоване управління ризиками
CISO / відповідальний за ІБ	Призначена посадова особа	Підвищення рівня контролю
Політики безпеки	Внутрішні нормативні документи	Стандартизація дій персоналу

Процедурні інструменти регламентують порядок реалізації заходів інформаційної безпеки та забезпечують їх практичне впровадження у діяльність підприємства.

Основні процедурні інструменти:

1. *Систематичне управління інформаційними ризиками.* Передбачає регулярне виявлення, аналіз і переоцінку ризиків, пов’язаних із функціонуванням інформаційних систем. Це дозволяє своєчасно ідентифікувати потенційні загрози та оцінити їхній вплив на економічну діяльність підприємства.

2. *Розробка планів реагування на інциденти.* Формування чітких алгоритмів дій у разі виникнення кіберінцидентів (витоки даних, атаки, збої систем). До таких планів включаються механізми локалізації загроз, відновлення роботи систем та мінімізації фінансових втрат.

3. *Організація резервного копіювання та відновлення даних.* Створення резервних копій інформації є критичним елементом захисту, що забезпечує відновлення працездатності підприємства після інцидентів. Процедури backup та disaster recovery дозволяють мінімізувати втрати даних і скоротити час простою [79].

Таблиця 3.3. Процедурні та контрольні інструменти інформаційної безпеки

Група	Інструмент	Призначення
Процедурні	План реагування на інциденти	Швидка ліквідація загроз
Процедурні	Резервне копіювання	Відновлення даних
Контрольні	Аудит ІБ	Оцінка відповідності стандартам
Контрольні	Моніторинг систем	Виявлення інцидентів у реальному часі

Мотиваційні інструменти спрямовані на формування відповідального ставлення персоналу до питань інформаційної безпеки та зменшення впливу людського фактора.

Основні мотиваційні інструменти:

1. *Система стимулювання персоналу***.** Впровадження матеріальних і нематеріальних заохочень за дотримання правил інформаційної безпеки та активну участь у виявленні загроз сприяє підвищенню рівня залученості працівників.

2. *Формування корпоративної культури безпеки***.** Розвиток внутрішніх цінностей, у яких інформаційна безпека розглядається як спільна відповідальність, дозволяє знизити кількість інцидентів, пов’язаних із людськими помилками [80].

Таблиця 3.4. Мотиваційні та навчальні інструменти

Інструмент	Зміст	Економічний ефект
Система заохочень	Премії за дотримання політик	Зниження людських помилок
Корпоративна культура безпеки	Формування цінностей	Зменшення інсайдерських ризиків
Навчальні тренінги	Регулярне навчання персоналу	Зниження витрат на інциденти
Інформаційні бюлетені	Роз’яснення загроз	Підвищення обізнаності

Інформаційно-освітні заходи забезпечують підвищення рівня компетентності персоналу щодо сучасних кіберзагроз і методів їх запобігання.

Основні інструменти:

1. *Навчання та підвищення кваліфікації персоналу***.** Регулярні тренінги, семінари та інструктажі дозволяють формувати практичні навички розпізнавання загроз, зокрема фішингових атак, соціальної інженерії та шкідливого програмного забезпечення.

2. *Інформаційна підтримка та внутрішні комунікації.* Використання внутрішніх бюлетенів, інструкцій та інформаційних повідомлень сприяє підтриманню актуального рівня обізнаності працівників щодо нових кіберризиків [81].

Контрольні та аудиторські процедури є важливими складовими системи забезпечення інформаційної безпеки на підприємстві, оскільки вони забезпечують можливість об’єктивної оцінки ефективності впроваджених захисних механізмів. Їх застосування дозволяє своєчасно виявляти невідповідності внутрішнім регламентам, ідентифікувати слабкі місця в організаційних процесах та формувати обґрунтовані управлінські рішення щодо їх усунення.

Основні контрольні заходи:

1. *Регулярний аудит інформаційної безпеки.* Проведення періодичних аудитів є ключовим інструментом оцінювання стану інформаційної безпеки підприємства. Аудиторські перевірки дають змогу визначити рівень відповідності внутрішніх політик і процедур встановленим стандартам, а також чинному законодавству. У межах аудиту здійснюється аналіз ефективності технічних і організаційних заходів захисту інформації, що дозволяє виявляти потенційні прогалини в системі безпеки та формувати рекомендації щодо їх усунення.

2. *Моніторинг інформаційних систем***.** Безперервний моніторинг є оперативним механізмом контролю стану інформаційної інфраструктури

підприємства. Він передбачає постійне відстеження подій, журналів активності та поведінки користувачів у системі. Завдяки цьому забезпечується можливість своєчасного виявлення аномальних процесів, несанкціонованих дій або ознак кіберінцидентів, що підвищує швидкість реагування та знижує потенційні збитки [82].

Загалом контрольні заходи формують основу системи зворотного зв’язку в управлінні інформаційною безпекою, забезпечуючи її адаптивність до змін зовнішнього та внутрішнього середовища. Вони охоплюють широкий спектр дій, які у взаємодії з іншими організаційними інструментами створюють цілісну модель управління захистом інформаційних ресурсів підприємства.

Організаційні заходи у сфері інформаційної безпеки мають не лише управлінське, але й виражене економічне значення. Їх впровадження сприяє зниженню ймовірності виникнення інцидентів, а також мінімізації фінансових втрат, пов’язаних із витоками даних, порушенням бізнес-процесів та репутаційними ризиками. У цьому контексті витрати на організаційні заходи доцільно розглядати як інвестиції у зниження потенційних збитків, що можуть виникнути внаслідок кіберзагроз.

Практика свідчить, що витрати на впровадження політик безпеки, організацію навчання персоналу та побудову системи моніторингу є значно нижчими порівняно з потенційними втратами від масштабних кіберінцидентів або зупинки операційної діяльності підприємства. Таким чином, організаційні інструменти забезпечення інформаційної безпеки виконують превентивну функцію, спрямовану на попередження економічних втрат.

Додатковий економічний ефект проявляється у підвищенні рівня координації між структурними підрозділами підприємства. Чітко визначена організаційна структура управління безпекою дозволяє оперативно реагувати на загрози, зменшуючи час простою систем і витрати на ліквідацію наслідків

інцидентів. Це, у свою чергу, позитивно впливає на стабільність бізнес-процесів і загальну економічну ефективність діяльності підприємства.

Важливим фактором також є підвищення рівня обізнаності персоналу щодо питань інформаційної безпеки. Формування корпоративної культури безпеки та систематичне навчання працівників зменшують імовірність помилок, що можуть призвести до порушення інформаційних систем. У результаті знижується рівень операційних ризиків та оптимізуються витрати на реагування на інциденти.

Таким чином, організаційні заходи забезпечення інформаційної безпеки формують важливий елемент економічної безпеки підприємства. Вони сприяють не лише підвищенню рівня захищеності інформаційних активів, але й забезпечують довгострокову економічну стійкість, зменшення витрат на усунення наслідків інцидентів та зміцнення конкурентних позицій підприємства в умовах цифрової трансформації та зростання кіберзагроз.

ВИСНОВКИ

У результаті проведеного комплексного дослідження встановлено, що інформаційна безпека є однією з ключових складових системи економічної безпеки суб'єктів господарювання в умовах цифровізації економіки та розвитку інформаційного суспільства. Захищеність інформаційних ресурсів, інформаційних систем і технологій безпосередньо впливає на стабільність функціонування підприємства, рівень його конкурентоспроможності, фінансову стійкість та здатність ефективно протидіяти внутрішнім і зовнішнім загрозам. Водночас стрімке поширення цифрових технологій супроводжується зростанням кількості інформаційних ризиків і кіберзагроз, що потребує формування комплексної системи захисту інформаційних активів підприємства.

Дослідження теоретичних засад економічної та інформаційної безпеки дозволило узагальнити сучасні наукові підходи до визначення їх сутності, змісту та взаємозв'язку. Встановлено, що інформаційна безпека є невід'ємним структурним елементом економічної безпеки підприємства та спрямована на забезпечення конфіденційності, цілісності, доступності й достовірності інформації. Визначено, що ефективне функціонування системи економічної безпеки неможливе без належного рівня захисту інформаційних ресурсів, які виступають важливим фактором прийняття управлінських рішень та забезпечення безперервності бізнес-процесів.

У процесі дослідження встановлено, що сучасний розвиток інформаційно-комунікаційних технологій суттєво трансформує підходи до забезпечення економічної безпеки суб'єктів господарювання. Активне використання цифрових платформ, автоматизованих систем управління, електронного документообігу, хмарних сервісів та технологій обробки даних створює нові можливості для підвищення ефективності діяльності підприємств, але водночас формує додаткові ризики, пов'язані з несанкціонованим доступом до інформації, витоком конфіденційних даних та кіберзлочинністю.

Особливу увагу в роботі приділено дослідженню місця інформаційної безпеки у структурі економічної безпеки підприємства. Встановлено, що інформаційна безпека виконує інтегруючу функцію, оскільки забезпечує захист інформаційних потоків, що супроводжують фінансову, кадрову, виробничу, техніко-технологічну та інші складові економічної безпеки. Доведено, що порушення інформаційної безпеки може спричиняти значні фінансові втрати, погіршення ділової репутації, зниження рівня конкурентоспроможності та виникнення кризових ситуацій у діяльності підприємства.

У другому розділі роботи здійснено аналіз сучасних загроз інформаційній безпеці підприємств та їх впливу на рівень економічної безпеки суб'єктів господарювання. Встановлено, що найбільш поширеними загрозами є кібератаки, шкідливе програмне забезпечення, фішингові атаки, соціальна інженерія, несанкціонований доступ до інформаційних ресурсів, витік конфіденційної інформації, а також внутрішні загрози, пов'язані з людським фактором та порушенням встановлених правил інформаційної безпеки.

Проведене дослідження дозволило визначити, що негативні наслідки реалізації інформаційних загроз виходять далеко за межі інформаційної сфери та безпосередньо впливають на економічні результати діяльності підприємства. Зокрема, порушення конфіденційності, цілісності або доступності інформації може призводити до фінансових втрат, зниження ринкової вартості підприємства, втрати ділової репутації, погіршення взаємовідносин із партнерами та клієнтами, а також до зниження ефективності управлінських рішень.

SWOT-аналіз системи інформаційної безпеки підприємства дозволив систематизувати сильні та слабкі сторони, а також визначити основні можливості й загрози сучасного цифрового середовища. До ключових можливостей віднесено використання сучасних технологій кіберзахисту, автоматизацію процесів моніторингу інформаційних ризиків, впровадження

систем контролю доступу та розвиток цифрових компетентностей персоналу. Серед основних загроз визначено зростання масштабів кіберзлочинності, постійне вдосконалення методів кібератак, дефіцит кваліфікованих фахівців у сфері інформаційної безпеки та недостатній рівень обізнаності працівників щодо інформаційних ризиків.

Особливу увагу приділено дослідженню механізмів забезпечення інформаційної безпеки підприємства. Встановлено, що ефективна система захисту інформаційних ресурсів повинна поєднувати організаційні, технічні, програмні, правові та кадрові заходи. Доведено, що лише комплексний підхід до управління інформаційною безпекою дозволяє забезпечити належний рівень захищеності інформаційних активів та мінімізувати негативний вплив інформаційних загроз на діяльність підприємства.

На основі отриманих результатів у третьому розділі роботи сформульовано практичні рекомендації щодо вдосконалення системи інформаційної безпеки у структурі економічної безпеки суб’єктів господарювання. Запропоновано впровадження сучасних засобів кіберзахисту, систем моніторингу та виявлення загроз, багатофакторної автентифікації користувачів, криптографічного захисту даних, резервного копіювання інформації та регулярного аудиту інформаційної інфраструктури підприємства.

Важливим напрямом підвищення ефективності системи інформаційної безпеки визначено вдосконалення організаційних механізмів управління інформаційними ризиками. Обґрунтовано необхідність розроблення внутрішніх політик інформаційної безпеки, регламентів роботи з конфіденційною інформацією, процедур контролю доступу до інформаційних ресурсів та механізмів реагування на інформаційні інциденти. Реалізація зазначених заходів сприятиме підвищенню рівня захищеності підприємства та зменшенню ймовірності реалізації інформаційних загроз.

Окремий акцент зроблено на кадровій складовій забезпечення інформаційної безпеки. Запропоновано систематичне проведення навчання

працівників, підвищення рівня цифрової грамотності персоналу, формування культури інформаційної безпеки та впровадження механізмів контролю за дотриманням вимог інформаційного захисту. Встановлено, що саме людський фактор залишається одним із найбільш уразливих елементів системи безпеки, а тому потребує постійної уваги з боку керівництва підприємства.

Узагальнюючи результати дослідження, можна зробити висновок, що інформаційна безпека є стратегічно важливою складовою економічної безпеки суб'єктів господарювання. Її ефективне забезпечення сприяє захисту економічних інтересів підприємства, підтриманню стабільності його функціонування, підвищенню конкурентоспроможності та створенню умов для сталого розвитку в сучасному цифровому середовищі.

Реалізація запропонованих у роботі рекомендацій дозволить підвищити рівень захищеності інформаційних ресурсів підприємства, мінімізувати інформаційні ризики та кіберзагрози, зміцнити систему економічної безпеки й забезпечити ефективне функціонування суб'єкта господарювання в умовах цифрової трансформації економіки та зростання глобальних викликів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Антонюк О. В. Інформаційна безпека підприємств: теоретичні основи та практичні підходи. Київ: Наукова думка, 2020. 320 с.

2. Шеремет В. В. Економічні аспекти інформаційної безпеки підприємства. *Економіка України*. 2019. № 3. С. 45-57.

3. ISO/IEC 27001:2017 Information technology – Security techniques – Information security management systems — Requirements. ISO, 2017. 25 с.

4. Грищенко Л. С. Корпоративна інформаційна безпека: проблеми та шляхи їх вирішення. *Безпека та оборона*. 2020. № 2. С. 33-42.

5. Гончаров А. В. Інформаційні загрози та методи їх нейтралізації в умовах цифровізації. *Вісник Київського національного університету*. 2021. № 5. С. 78-86.

6. Довгань І. В. Використання стандартів інформаційної безпеки для управління кіберризиками. Кібербезпека і технології захисту інформації, 2020, № 4, с. 12-25.

7. Ковальчук Є. М. Вплив інформаційної безпеки на економічну стабільність підприємства. *Вісник економічної безпеки*. 2020. № 6. С. 55-67.

8. Климчук С. О. Вплив технологій штучного інтелекту на інформаційну безпеку підприємств. *Інформаційні технології: науковий журнал.* 2022. № 4. С. 15-23.

9. Скакун О.Ф. Теорія держави і права: підручник. Харків: Консул. 2001. 656 с.

10. Е-майбутнє та інформаційне право / за ред. М. Швеця. 2-е вид., доп. Київ: НДЦПІ АПрН України, 2006. 234 с.

11. Правове забезпечення інформаційної діяльності в України / за заг. ред. Ю.С. Шемшученка, І.С. Чижа. Київ : Юридична думка. 2006. 384 с.

12. Субіна Т. Поняття і сутність інформації у просторі держави. *Науковий вісник Національної академії ДПС України.* 2004. № 4 (26). С. 210-211.

13. Бурячок В.Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби [Підручник] / В.Л. Бурячок, Г.М Гулак, В.Б. Толубко. – К. : ТОВ «СІК ГРУП УКРАЇНА», 2015. – 449 с.

14. Литвинов В.В. Моделювання та аналіз безпеки розподілених інформаційних систем: навч. пос. [для студ. спец. 121 «Інженерія програмного забезпечення»] / В.В. Литвинов, В.В. Казимир, І.В. Стеценко та ін. – Чернігів: Чернігів. нац. технол. ун-т, 2016. – 254 с.

15. Сащенко М. Проблемні аспекти запобігання кіберзлочинності в Україні. *Молодий вчений*. 2022. № 1 (101). С. 17-20.

16. Лисецький Ю. М., Калбазов Д. Й. Підходи до забезпечення інформаційної безпеки. *Математичні машини і системи*. 2023. №4. С. 26-32.

17. Лобода О. М. Захист інформації в корпоративних мережах. *Публічне управління та адміністрування у процесах економічних реформ*. 2020. С. 61-63.

18. Яіцький А. О., Сахаров М. Г. Ефективні методи та засоби захисту фішингових атак. *Problems of science and practice, tasks and ways to solve them.* 2022. Т. 11. С. 417.

19. Тацієнко В. В. Новітні способи і технології вчинення транснаціональних комп'ютерних злочинів у сфері економіки (згідно з дослідженнями зарубіжних вчених). *DICTUM FACTUM*. 2024. Вип. 1 (15). С. 170–175.

20. Сопільник Л. та ін. Розвиток цифрової економіки в контексті забезпечення інформаційної безпеки в Україні.*Traektoriâ Nauki= Path of Science*. 2020. Т. 6. №. 5. С. 2023-2032.

21. Хлистік М. А., Озеруга А. О. Проблемні питання боротьби із кіберзлочинністю в Україні // The 28th International scientific and practical conference "Science and development of methods for solving modern problems" (July 18–21, 2023), Melbourne, Australia. International Science Group, 2023. – 232 с.

22. Литвиненко О., Крисак І. СИСТЕМА ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА. XXXII International scientific and practical conference «Global Trends and Direction of Scientific Research Development»(July 31-August 2, 2024) Hamburg, Germany. International Scientific Unity, 2024. 285 p.

23. Сисоєва І. Аналіз потенційних загроз діяльності суб'єктів господарювання. *Економіка та суспільство*. 2020. № 22.

24. Сікора О., Кобильник Т. Технології захисту інформаційних ресурсів. *Перспективи та інновації науки.* 2024. № 8 (42).

25. Фостолович В. А. Штучний інтелект в сучасному бізнесі: потенціал, сучасні тренди та перспективи інтегрування у різні сфери господарської діяльності і життєдіяльності людини. Ефективна економіка. 2022. №. 7.

26. Румянцева О. В. Аналіз методів класифікаціїї вразливостей та загроз інформаційної системи. Моделювання та інформаційні технології в науці, техніці, кібербезпеці та освіті : матеріали Всеукр. наук.-практ. Internet-конф. , 15–16 листоп. 2022 р., м. Харків / Харків. нац. автомоб.-дор. ун-т. Харків : ХНАДУ, 2022. С. 52-56.

27. Магдаліна М. І. Методика аналізу загроз та вразливостей до кібератак сучасних інформаційних систем : пояснювальна записка до кваліфікаційної роботи здобувача вищої освіти на другому (магістерському) рівні, спеціальність 125 Кібербезпека. М-во освіти і науки України, Харків. нац. ун-т радіоелектроніки. Харків, 2023. 85 с.

28. Рубан І. В. Особливості розповсюдження ризико-орієнтованого підходу до оцінки вразливості об'єктів кіберзахисту. *Безпека інформації*. 2020. С. 145-155.

29. Новицький В. Я. Стратегічні засади забезпечення інформаційної безпеки в сучасних умовах. *Інформація і право*. 2022. №. 1 (40). С. 111-118.

30. Леськів Г., Гобела В., Лесик Н. Характеристика основних проблем забезпечення інформаційної безпеки в умовах впливу цифрових технологій. *Економіка та суспільство*. 2022. №. 43.

31. Калетнік В., Калетнік Н. Інформаційна безпека і кіберзахист як сучасна інтелектуальна зброя. *Молодий вчений*. 2021. №. 5 (93). С. 305-311.

32. Лисецький Ю. М., Калбазов Д. І. Інформаційна безпека корпоративних баз даних. *Математичні машини і системи*. 2023. №. 3. С. 31-37.

33. Стечишин Ю. Визначення ролі та місця інформаційно-аналітичного забезпечення в системі економічної безпеки. *Вчені записки Університету «КРОК».* 2023. №. 1 (69). С. 110-119.

34. Правдюк А. Захист персональних даних в контексті інформаційної безпеки. *Наукові інновації та передові технології*. 2024. № 5 (33).

35. Кравченко О. М. Організаційно-правові заходи забезпечення охорони конфіденційної інформації та комерційної таємниці бізнесу в Україні. *Вчені записки ТНУ імені ВІ Вернадського. Серія: Юридичні науки*. 2023. №. 3. С. 48-53.

36. Висоцька І., Нагірна О. Фінансове шахрайство банківського сектору в період дії воєнного стану. *Науковий вісник Львівського державного університету внутрішніх справ (серія економічна)*. 2024. №. 1. С. 12-18.

37. Дзяд О. В., Стародуб Д. С. Економічні втрати та механізми протидії кіберзлочинності. *Ефективна економіка*. 2022. №. 1.

38. Данченко О. Б., Ланських Є. В., Семко О. В. Інформаційні ризики цифрового формату. *Вісник Черкаського державного технологічного університету. Технічні науки*. 2020. №. 3. С. 58-66.

39. Тарасовський Ю., Шевчук С. ПриватБанк, Ощадбанк, monobank, Альфа-Банк, урядові сайти та портал «Дія» зазнали кібератаки. URL: https://forbes.ua/news/dzherela-v-nbu-privatbank-ta-oshchadbank-zaznali-

kiberataki-servisi-vzhe-vidnovlyuyut-robotu-15022022-3691 – Дата звернення: 05.11.2024.

40. Атака вірусу NotPetya була організована проти України - Британське МЗС. URL: https://www.epravda.com.ua/news/2018/02/15/634101/ – Дата звернення: 05.11.2024.

41. Підприємство «Прикарпаттяобленерго» зупинило роботу «Персонального кабінету» та кол-центру через загрозу кібератаки. URL: https://www.ukrinform.ua/rubric-economy/2255333-prikarpattaoblenergo-prizupinilo-robotu-servisiv-cerez-zagrozu-kiberataki.html – Дата звернення: 05.11.2024.

42. Деякі українські ритейлери зазнавали втрат репутації через витоки даних, що негативно вплинуло на лояльність клієнтів. Огляд національної ритейл-галузі. URL: https://retail-ukraine.ua. – Дата звернення: 05.11.2024.

43. Компанія «Миронівський хлібопродукт» (МХП) здійснює значні інвестиції у кібербезпеку. URL: https://mhp.com.ua. – Дата звернення: 05.11.2024.

44. Danchenko O. et al. Метод управління інформаційними ризиками в проєктах діджиталізації бізнес-процесів //Bulletin of the National Technical University" KhPI". Series: Strategic management, portfolio, program and project management. 2022. №. 2 (6). С. 25-29.

45. Чубаєвський В. Методи управління корпоративною інформаційною безпекою. *Економіка та суспільство.* 2022. №. 43.

46. Запорожець Т., Цимбаленко Я. Безпека інформаційних систем як чинник ефективності мережевого управління. *Аспекти публічного управління*. 2023. Т. 11. №. 3. С. 25-29.

47. Кісільов О. І., Качков С. О. Сутність інтегрованого управління проєктними та операційними ризиками в організації. *Управління розвитком складних систем*. 2023. №. 55. С. 46-54.

48. Галіцин В., Галіцина О. Управління інформаційними ризиками як чинник підвищення ефективності підприємства. *Економіка та суспільство*. 2024. №. 62.

49. Карпович І., Гладка О., Бухало Ю. Технології моделювання і оцінки ризиків інформаційної безпеки. *Технічні науки та технології*. 2021. №. 1 (23). С. 62-68.

50. Асєєва Л. А., Шушура О. М. Оцінка ризиків конфіденційності інформаційної безпеки проектів на основі нечіткої логіки. *Телекомунікаційні та інформаційні технології*. 2021. №. 1. С. 88-95.

51. Соколов В., Складанний П. Методика оцінки комплексних збитків від інциденту інформаційної безпеки. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка».* 2023. Т. 1. №. 21. С. 99-120.

52. Шурда К. Е. Методи якісного та кількісного аналізу ризиків. *Збалансоване природокористування*. 2020. №. 4. С. 64-72.

53. Балдинюк В. Управління ризиками господарської діяльності підприємства та шляхи їх зниження. *Економіка та суспільство*. 2023. №. 57.

54. Геврек Ю. С. Теоретичні основи механізму комплексного управління ризиками на підприємстві. *Бізнес-навігатор*. 2020. С. 81.

55. Захарова Н. Ю. Управління ризиками на підприємстві: сутність, підходи та методи. *Бізнес Інформ.* 2023. №. 1. С. 203-209.

56. Тебенко В. М., Болтянська Л. О., Лисак О. І. Управління ризиками як напрям забезпечення конкурентоспроможності підприємства. Збірник наукових праць Таврійського державного агротехнологічного університету імені Дмитра Моторного (економічні науки). 2023. Т. 3. №. 49.

57. Мирошниченко Г. Управління ризиками підприємницьких структур: аспекти ризик-менеджменту. *Економіка та суспільство*. 2022. №. 44.

58. Гонтаренко Ю. Д., Зачосова Н. В. Стратегії управління економічними ризиками об’єктів критичної інфраструктури для стабілізації

їх економічної безпеки умовах bani world та індустрії 4.0. Цифрова економіка та економічна безпека. 2023. №. 7 (07). С. 165-171.

59. Легомінова С. В. Теоретичні засади інформаційної безпеки підприємства. *Економіка. Менеджмент. Бізнес*. 2015. № 3. URL: https://journals.dut.edu.ua/index.php/emb/article/view/477/443

60. Голяш І. Д. Роль обліку та контролю в посиленні інформаційної безпеки підприємства: дис. … докт. екон. наук: 08.00.09 / І. Д. Голяш; Терноп. нац. екон. ун-т. Тернопіль, 2010. 480 с.

61. Тарангул Л. Л. Фінансова безпека України та інструменти її забезпечення. *Економічний вісник. Серія: фінанси, облік, оподаткування*. 2017. № 1. С. 201-208.

62. Квашук Д. М. Організаційні заходи з інформаційно-аналітичного забезпечення економічної безпеки підприємств з використанням технічних засобів обробки інформації. Університетські наукові записки. 2017. № 1. С. 232-243.

63. Запорожченко М. Проблема фішингу для інформаційної безпеки підприємств. Організаційні способи протидії. Інформаційна безпека та інформаційні технології: збірник тез доповідей V Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 26 листопада 2021 року. Львів, ЛДУ БЖД, 2021, 227 с.

64. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. Відомості Верховної Ради України. 2010. № 36-37. Ст. 482.

65. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, GDPR). *Official Journal of the European Union*. L 119, 4 May 2016, pages 1-88.

66. Орлов П. І. Правове забезпечення інформаційної безпеки. Вісник Харківського національного університету внутрішніх справ. 2001. Вип. 15. С. 96-99.

67. Якубівська Ю. Є. Колізії норм права та компетенції органів управління у сфері інтелектуальної власності як загроза інформаційній безпеці. *Зовнішня торгівля: економіка, фінанси, право*. 2015. № 4. С. 36-41.

68. Про основи кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 48. Ст. 439.

69. ISO/IEC 27001:2013. Інформаційні технології. Методи та засоби забезпечення інформаційної безпеки. Системи управління інформаційною безпекою. Вимоги. Міжнародна організація зі стандартизації (ISO), Міжнародна електротехнічна комісія (IEC). 2013.

70. Носов В. В. Міжнародна стандартизація з інформаційної безпеки у фінансових інформаційних системах. *Право і Безпека*. 2009. № 2. С. 259–267.

71. Нашинець-Наумова А. Ю. Питання забезпечення інформаційної безпеки підприємства. *Юридичний вісник. Повітряне і космічне право*. 2012. № 3. С. 58-62.

72. Азарова А. О., Дьогтєва І. О., Шиян А. А. Система підтримки прийняття рішень щодо підвищення рівня інформаційної безпеки підприємства. Інформаційні технології та комп'ютерна інженерія. 2022. № 1. С. 12-18.

73. Танцюра М. Ю. Забезпечення ефективності системи інформаційної безпеки підприємства: монографія. Сімферополь: ВД «АРІАЛ», 2013. 320 с.

74. Сирцева С. В. Інформаційне забезпечення економічної безпеки підприємства. Сучасні аспекти модернізації науки: стан, проблеми, тенденції розвитку: матеріали XLV-ої Міжнародної науково-практичної конференції / за ред. І.В. Жукової, Є.О. Романенка. м. Олександруполіс (Греція): ВАДНД, 07 червня 2024 р. С. 455-456.

75. Чубаєвський В., Жук Т. Економічна ефективність інформаційної безпеки підприємств торгівлі. *Scientia fructuosa*. 2022. Т. 141, № 1. С. 106–117.

76. Гордієнко, С. Б., Микитенко, О. С., Данильчук, В. Г. Методи та рекомендації забезпечення інформаційної безпеки консалтингової компанії. *Вісник Державного університету інформаційно-комунікаційних технологій*. 2013. № 1. С. 104-107.

77. Бурцева К. А., Тимофєєв Д. С. Підвищення рівня інформаційної безпеки за допомогою організаційних заходів на комерційних підприємствах. 2012. *URL: http://ir.nmu.org.ua/bitstream/handle/123456789/1673/6.pdf*

78. Северина С. В. Інформаційна безпека та методи захисту інформації. *Вісник Запорізького національного університету. Економічні науки*. 2016. №1. С. 155-161.

79. Радуш В. В., Лебедєва О. Ю., Кушніренко Н. І., Зорило В. В. Моделювання організаційних заходів для створення політики безпеки організації з використанням бізнес-процесів. *Інформатика та математичні методи в моделюванні*. 2021. Т. 11, № 3. С. 239–246.

80. Скиба А. В., Архипов О. Є. Метод управління загальним станом захищеності інформаційної безпеки компанії за допомогою аналізу причинно-наслідкових взаємозв'язків за методом Ісікави. *Економіка та держава*. 2016. № 1. С. 86-89.

81. Новицький В. Я. Стратегічні засади забезпечення інформаційної безпеки в сучасних умовах. *Інформація і право*. 2022. № 1 (40). С. 111–118.

82. Мазник Л. В., Драган О. І. Інформаційна безпека організації як фактор посилення бренду роботодавця. *Київський економічний науковий журнал*. 2023. № 1. С. 39-44.

ДОДАТКИ