Міністерство освіти і науки України
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

ННІ економіки, управління і бізнесу ім. Г. Е. Вейнштейна
Кафедра – економічної теорії та фінансово – економічної безпеки
Ступінь вищої освіти – другий (магістр)
Спеціальність – 051 Економіка
Освітня програма – Фінансово-економічна безпека

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

на тему: «Інформаційна безпека як складова економічної безпеки підприємств»

ШИФР КРМ. ЕТтаФЕБ.1.626.03-2.2

Здобувач _____ Іванова Анастасія Володимирівна
(ПІБ)
Керівник:_____ к.ю.н., доц. Шишлюк В. Р.
(науковий ступінь, вчене звання, ПІБ)

Кваліфікаційна робота допускається до захисту

Рішення кафедри від 09.12. 2024, протокол № 6

В. о. завідувача кафедри

ЕТ та ФЕБ _____ Олена ЗАБОЛОТНА
Назва кафедри (підпис)

Одеса – 2024 р.

ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

ННІ економіки, управління і бізнесу ім. Г. Е. Вейнштейна
Кафедра – економічної теорії та фінансово – економічної безпеки
Ступінь вищої освіти – другий (магістр)
Спеціальність – 051 Економіка
Освітня програма – Фінансово-економічна безпека

ЗАТВЕРДЖУЮ
Зав. кафедри економічної теорії та
фінансово-економічної безпеки
_____ Згадова Н. С.
«07» листопада 2023 р.

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ МАГІСТРА

здобувача
Анастасії ІВАНОВОЇ
(ім'я, ПРІЗВИЩЕ **)**

1. Тема роботи: «Інформаційна безпека як складова економічної безпеки підприємств» затверджена наказом ОНТУ від 07.11.2023. р. № 668-03, зі змінами та доповненнями від 10.10.2024. р. № 626-03.

2. Термін здачі здобувачем закінченої роботи 06.12.2024 р.

3. Вихідні дані роботи: нормативна база, наукова та методична література.

4. Зміст кваліфікаційної роботи магістра. Вступ. Теоретичні основи інформаційної безпеки підприємства. Оцінка сучасних загроз інформаційній безпеці підприємства. Стратегії та методи забезпечення інформаційної безпеки. Висновки та пропозиції. Список використаних джерел.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень) таблиць –, рисунків –.

6. Консультанти по роботі, із зазначенням розділів проекту, що стосуються їх:

Розділ	Консультант	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання 07.11.2023

Керівник _____ к.ю.н., доц. Шишлюк В. Р.
(підпис)

Завдання прийняв до виконання _____ Іванова А. В.
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів кваліфікаційної магістерської роботи	Термін виконання етапів роботи	Примітка
1	*Підготовка першого розділу теоретичні основи інформаційної безпеки підприємства.*	07.11.2023 - 31.03.2024	Виконано
2	*Оцінка сучасних загроз інформаційній безпеці підприємств*	05.04 - 31.05.2024	Виконано
3	*Стратегії та методи забезпечення інформаційної безпеки*	15.06-31.08.2024	Виконано
4	*Висновки. Список використаних джерел*	01.09-21.10.2024	Виконано
5	*Оформлення кваліфікаційної роботи*	29.11-06.12.2024	Виконано

Керівник _____ Шишлюк В. Р.
(підпис)
Здобувач-магістр _____ Іванова А. В.
(підпис)

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-магістр _____ /Іванова А. В./
підпис

АНОТАЦІЯ

кваліфікаційної роботи магістра **Іванової Анастасії Володимирівни**

Інформаційна безпека як складова економічної безпеки підприємств

Мета дослідження – розробка та обґрунтування методів і заходів для забезпечення інформаційної безпеки підприємств як ключового компонента їх економічної безпеки. Дослідження спрямоване на аналіз актуальних загроз, ризиків та викликів, пов'язаних з інформаційною безпекою, а також визначення шляхів мінімізації їх негативного впливу на економічну діяльність підприємств.

Дана робота складається з трьох розділів.

Перший розділ розглядає теоретичні основи інформаційної безпеки підприємств, визначає сутність поняття та його роль у загальній системі економічної безпеки.

Другий розділ присвячений аналізу основних загроз та ризиків для інформаційної безпеки, а також правових і організаційних аспектів її забезпечення на підприємствах України.

У третьому розділі розроблено рекомендації щодо вдосконалення системи інформаційної безпеки підприємств для підвищення рівня їхньої економічної стійкості та захищеності від інформаційних загроз.

У **висновках** сформульовано пропозиції з підвищення рівня інформаційної безпеки підприємств через інтеграцію її в загальну систему економічної безпеки.

Ключові слова: інформаційна безпека, економічна безпека підприємств, інформаційні загрози, ризики, захист інформації, економічна стійкість, правові аспекти, організаційні заходи, мінімізація негативного впливу, системи безпеки, інформаційні виклики.

ABSTRACT

Master's Qualification Work by **Ivanova Anastasiia**

Information Security as a Component of Economic Security of Enterprises

The ***aim of the research*** is to develop and substantiate methods and measures for ensuring information security of enterprises as a key component of their economic security. The research focuses on analyzing current threats, risks, and challenges related to information security and identifying ways to minimize their negative impact on the economic activities of enterprises.

The thesis consists of three chapters.

The ***first chapter*** examines the theoretical foundations of information security for enterprises, defining the concept and its role in the overall system of economic security.

The ***second chapter*** analyzes the main threats and risks to information security, as well as the legal and organizational aspects of ensuring it at Ukrainian enterprises.

The ***third chapter*** presents recommendations for improving the information security systems of enterprises to enhance their economic resilience and protection against information threats.

The **conclusions** propose measures to improve the level of information security for enterprises by integrating it into the overall system of economic security.

Keywords: information security, economic security of enterprises, information threats, risks, information protection, economic resilience, legal aspects, organizational measures, minimizing negative impact, security systems, information challenges.

ЗМІСТ

ВСТУП

Актуальність теми дослідження обумовлена швидким розвитком інформаційних технологій та зростанням кіберзагроз, які постійно еволюціонують і стають дедалі складнішими. У сучасному світі інформація є не лише стратегічним ресурсом, а й основним інструментом створення конкурентних переваг. Порушення інформаційної безпеки здатне призвести до суттєвих фінансових втрат, зниження продуктивності, втрати ділової репутації та підриву довіри до підприємства з боку партнерів та клієнтів.

Значна кількість підприємств в Україні та за кордоном стикається з проблемами витоку інформації, викраденням даних, шахрайством і несанкціонованим доступом до інформаційних систем. Ці загрози вимагають впровадження надійних заходів інформаційної безпеки, що сприятимуть забезпеченню сталого розвитку підприємств. Недостатня увага до інформаційної безпеки може призвести до значних втрат для економічної стабільності підприємства і навіть до його банкрутства, особливо в умовах економічної нестабільності.

Актуальність теми дослідження підсилюється тим, що нормативна база та практичні рекомендації щодо інформаційної безпеки підприємств в Україні ще знаходяться на етапі розвитку і потребують адаптації до сучасних вимог. Це дослідження спрямоване на те, щоб глибше розглянути інформаційну безпеку як важливий елемент загальної економічної безпеки підприємств, виявити основні інструменти та механізми забезпечення захисту інформаційних активів, а також розробити ефективні рекомендації для зниження ризиків і мінімізації втрат.

Таким чином, дана тема дослідження є актуальною з огляду на необхідність підприємств розвивати комплексні системи інформаційної безпеки, що стануть важливою складовою їхньої економічної стійкості й ефективного функціонування в умовах зростаючої конкуренції та кіберзагроз.

Мета та завдання дослідження. Мета дослідження полягає у розробці та обґрунтуванні ефективних підходів і заходів для забезпечення

інформаційної безпеки як ключового елементу економічної безпеки підприємств. Дослідження спрямоване на аналіз та оцінку сучасних викликів, ризиків і загроз інформаційній безпеці, а також на визначення шляхів мінімізації негативного впливу інформаційних ризиків на економічну діяльність підприємства.

Завдання дослідження:

1. дослідити теоретичні основи та сучасні підходи до інформаційної безпеки в контексті економічної безпеки підприємства;
2. проаналізувати нормативно-правову базу, що регулює питання інформаційної безпеки підприємств в Україні, а також вивчити міжнародний досвід у цій сфері;
3. визначити основні загрози і ризики для інформаційної безпеки підприємства та їхній вплив на економічну безпеку;
4. провести аналіз інструментів і методів забезпечення інформаційної безпеки, які використовуються на підприємствах, і оцінити їх ефективність;
5. розробити рекомендації щодо вдосконалення системи інформаційної безпеки підприємств з метою підвищення рівня їхньої економічної стійкості і захищеності від інформаційних загроз;
6. розробити практичні заходи для інтеграції інформаційної безпеки в загальну систему економічної безпеки підприємства, враховуючи специфіку українських підприємств і сучасні технологічні виклики.

Об'єктом дослідження є система інформаційної безпеки підприємств як складова частина загальної системи економічної безпеки, що включає в себе інформаційні ресурси, технології, процеси та методи, спрямовані на захист від інформаційних загроз і ризиків, що можуть впливати на економічну стабільність і ефективність діяльності підприємства.

Предметом дослідження є механізми, інструменти та методи забезпечення інформаційної безпеки підприємств, а також їх взаємодія з іншими компонентами економічної безпеки підприємства. Це включає

вивчення заходів захисту інформаційних активів, оцінку ризиків, методи моніторингу та управління інформаційною безпекою, а також вплив інформаційних загроз на фінансову та операційну діяльність підприємства.

Методи дослідження. Методологічною основою даного дослідження є загальнонаукові та спеціально наукові методи дослідження. Зокрема, за допомогою діалектичного методу досліджено поняття та сутність інформаційної безпеки (підрозділ 1.1). Герменевтичний метод було використано при з'ясуванні окремих понять, що застосовуються при характеристиці процесів забезпечення інформаційної безпеки, а також місця інформаційної безпеки в загальній системі економічної безпеки підприємства (підрозділи 1.3, 2.1, 2.2, 2.3, розділ 3).

Методи порівняльного аналізу, фінансово-економічного та статистичного аналізу – для оцінки різних підходів до забезпечення інформаційної безпеки на підприємствах, а також для порівняння міжнародних стандартів і практик з українським досвідом (підрозділи 2.2, 2.3).

В роботі використовувались також інші методи наукового пізнання, зокрема, догматичний (підрозділи 1.1, 1.3, розділ 3.1), а також методи аналізу та синтезу для розгляду теоретичних аспектів інформаційної безпеки та економічної безпеки підприємств, а також для узагальнення наукових підходів і практичних рекомендацій щодо їх взаємодії (підрозділи 2.1, 2.2, 2.3).

Теоретична основа дослідження. Слід зазначити, що поняття «інформаційної безпеки підприємства» розглядали 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 у розробці інтегрованого підходу до забезпечення інформаційної безпеки як складової економічної

безпеки підприємств, що враховує економічні наслідки інформаційних загроз та пропонує критерії оцінки її ефективності. Запропоновані рекомендації базуються на кращих міжнародних практиках та адаптовані до українських умов, спрямовані на посилення стійкості підприємств та підвищення їх конкурентоспроможності.

Структура кваліфікаційної роботи. Кваліфікаційна робота складається із вступу, трьох розділів, які включають дев’ять підрозділів, висновків та списку використаних джерел.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

1.1. Поняття та сутність інформаційної безпеки

В умовах сучасної української реальності, яка характеризується високою нестабільністю як у зовнішньому, так і у внутрішньому середовищі, підприємства змушені формувати стратегії виживання, ґрунтуючись на активному використанні інформаційних технологій. Ці технології є однією з ключових переваг економічно розвинених країн. Інформаційні технології розширили можливості підприємств, сприяли прискоренню обміну інформацією та співпраці, а також відкрили доступ до більш ефективних управлінських рішень. Однак, одночасно з цим, вони створили загрози для економічної безпеки підприємств, що може призвести до зниження стабільності їхньої фінансово-економічної діяльності.

Інформація, яка раніше виступала інструментом для підвищення ефективності виробництва, тепер стала важливим засобом конкурентної боротьби. Володіння інформацією дає підприємству не лише можливість отримати прибуток, а й забезпечити стійкий розвиток. Це підтверджує правдивість вислову: «Хто володіє інформацією, той володіє світом». У такій ситуації захист інформаційної складової економічної безпеки підприємства набуває особливого значення.

У зв'язку з цим багато підприємств вирішують питання забезпечення своєї економічної безпеки через впровадження сучасної корпоративної системи інформаційної безпеки. Така система має на меті захист конфіденційної інформації від несанкціонованого доступу та усунення загроз, що можуть вплинути на економічну стабільність компанії.

Ця система повинна забезпечувати максимально можливе зниження ризиків, пов'язаних з використанням інформаційних технологій, при мінімальних витратах на її впровадження, а також бути достатньо гнучкою, щоб самостійно адаптуватися до змін у зовнішньому середовищі.

Інформаційна безпека – це багатогранне поняття, яке охоплює сукупність засобів, методів і процесів, спрямованих на захист інформації, що використовується, зберігається чи передається підприємством, від внутрішніх і зовнішніх загроз. Інформація, як стратегічний ресурс, потребує захисту, оскільки її компрометація може призвести до значних економічних, репутаційних і правових втрат для підприємства.

Різні науковці і практики пропонують різноманітні підходи до трактування цього поняття. Згідно з дослідженнями українського науковця О. В. Антонюка, інформаційна безпека підприємства визначається як стан захищеності інформаційних ресурсів, що забезпечує їх цілісність, конфіденційність і доступність під час зберігання, обробки і передачі [1]. Це визначення вказує на необхідність збереження трьох основних характеристик інформації: конфіденційності, цілісності та доступності, які є критичними для захисту інформаційних ресурсів.

Інший підхід до визначення інформаційної безпеки надає В. В. Шеремет, який підкреслює не лише технічні аспекти захисту, але й організаційні. За його словами, інформаційна безпека – це сукупність політик, процедур та технічних рішень, спрямованих на мінімізацію ризиків, пов'язаних із несанкціонованим доступом, витоком або модифікацією інформації, що використовується підприємством [2]. Такий підхід акцентує увагу на важливості комплексного управління інформаційними ризиками.

Міжнародні стандарти, такі як **ISO/IEC 27001**, також надають широке визначення інформаційної безпеки. Згідно з цим стандартом, інформаційна безпека охоплює управління ризиками, пов'язаними з конфіденційністю, цілісністю та доступністю інформації, забезпечуючи ефективний захист даних від загроз [3]. Такий підхід ґрунтується на формалізованих процедурах та стандартах, які впроваджують підприємства для забезпечення стійкості своїх інформаційних систем.

Як зазначалося вище, інформаційна безпека складається з трьох основних компонентів:

1. *Конфіденційність:* означає, що доступ до інформації мають лише ті особи, яким надано відповідні права. Це забезпечується через використання таких засобів, як шифрування даних, управління доступом та автентифікація користувачів.

Наприклад, у дослідженні Л. С. Грищенко наголошується, що конфіденційність інформації є основою економічної безпеки підприємства. Компанії, які не забезпечують належного рівня конфіденційності своїх даних, піддаються значному ризику витоку інформації, що може призвести до втрати конкурентних переваг [4].

2. *Цілісність:* ця характеристика стосується збереження точності та повноти інформації. Цілісність інформації забезпечується через використання контрольних механізмів, які гарантують, що дані не будуть змінені або пошкоджені без належної авторизації.

А. В. Гончаров зазначає, що цілісність є критичним аспектом для забезпечення стабільної роботи підприємства. Недостовірні дані можуть призвести до прийняття неправильних управлінських рішень, що у свою чергу вплине на фінансові результати компанії [5].

3. *Доступність:* передбачає, що уповноважені користувачі мають змогу отримати доступ до інформації, коли це необхідно. Важливою складовою доступності є наявність механізмів резервного копіювання та відновлення даних, які дозволяють швидко відновити роботу інформаційних систем після збоїв або атак.

Відповідно до досліджень І. В. Довгань, підприємства часто стикаються з проблемами, пов'язаними з доступністю інформації під час кіберінцидентів, таких як DDoS-атаки. Відсутність доступу до критичних даних може спричинити серйозні фінансові втрати і навіть зупинку бізнес-процесів [6].

З огляду на ключові характеристики інформаційної безпеки, існують різні підходи до її забезпечення. Ось декілька основних методів:

1. *Технічні заходи:* це широкий спектр інструментів і технологій, що використовуються для захисту інформаційних систем. Вони включають

брандмауери, системи виявлення загроз, шифрування даних, резервне копіювання та захист мереж.

2. *Організаційні заходи:* сюди входять політики, правила і процедури, що регулюють доступ до інформаційних ресурсів та їхнє використання. Наприклад, розробка чітких політик доступу до даних та управління правами користувачів є важливою складовою захисту конфіденційності і цілісності інформації.

3. *Правові заходи:* ці заходи включають дотримання законодавчих норм і стандартів, таких як GDPR або українське законодавство у сфері захисту персональних даних, які визначають відповідальність за порушення законодавства у сфері інформації.

Забезпечення інформаційної безпеки стикається з низкою проблем, серед яких можна виділити:

Зростання кіберзагроз: у сучасних умовах зловмисники використовують все більш складні методи атак на інформаційні системи. Згідно з дослідженням Є. М. Ковальчука, загрози у вигляді вірусів, фішингових атак та експлойтів стають дедалі частішими і небезпечнішими [7].

Нестача кваліфікованих кадрів: підприємства стикаються з труднощами у пошуку фахівців у галузі кібербезпеки, що ускладнює створення ефективних систем захисту.

Проблеми з фінансуванням: не всі підприємства можуть дозволити собі впровадження комплексних рішень для забезпечення інформаційної безпеки через високу вартість необхідних технологій та Визначення інформаційної безпеки охоплює не лише технічні заходи, але й організаційні та правові аспекти, що забезпечують захист інформації від загроз.

Головною метою інформаційної безпеки є збереження конфіденційності, цілісності та доступності даних, які є критично важливими для стабільної роботи підприємства. Зростаючі кіберзагрози та нові виклики, з якими стикаються підприємства, роблять інформаційну безпеку одним із ключових елементів їхньої стратегії економічної безпеки.

Для забезпечення високого рівня інформаційної безпеки підприємствам необхідно дотримуватись міжнародних стандартів. Одним з найбільш відомих є **ISO/IEC 27001**, який встановлює вимоги до систем управління інформаційною безпекою. Він допомагає підприємствам створювати, впроваджувати та підтримувати ефективні системи захисту інформації [6].

Також значущим є стандарт **NIST Cybersecurity Framework**, який пропонує комплексний підхід до управління кіберризиками. Згідно з дослідженням І. В. Довгань, впровадження цих стандартів дозволяє значно знизити ризики кіберзагроз і підвищити стійкість підприємств до атак [7].

Одним з ключових викликів для сучасних підприємств є постійне оновлення технологій і загроз, з якими вони стикаються. Це вимагає від бізнесу постійної адаптації та модернізації систем інформаційної безпеки. На думку С. О. Климчука, у майбутньому зростатиме значення технологій штучного інтелекту для підвищення рівня інформаційного захисту [8].

Інформаційна безпека є невід'ємною складовою загальної економічної безпеки підприємства. Вона охоплює комплекс технічних, організаційних та правових заходів, спрямованих на захист інформаційних ресурсів від зовнішніх і внутрішніх загроз. У сучасних умовах, коли інформація стала ключовим активом підприємств, її захист набуває стратегічного значення для підтримки конкурентоспроможності та стабільного розвитку бізнесу.

1.2. Механізми забезпечення інформаційної безпеки підприємства

Інформаційна безпека являє собою важливий аспект забезпечення стабільності та стійкості держави, а також суспільства в цілому. Вона визначається як міра захищеності ключових сфер життєдіяльності, таких як економіка, наука, техносфера, управлінська діяльність і військова справа, від дестабілізуючих та деструктивних інформаційних впливів. Ці впливи можуть загрожувати державним інтересам і базовим цінностям, ставлячи під ризик не лише безпеку окремих інститутів, а й цілісність національної системи.

Під інформаційною безпекою держави розуміється здатність системи реагувати на потенційні загрози та нейтралізувати їх. Це передбачає активні заходи, спрямовані на захист інформаційних ресурсів, а також на забезпечення конфіденційності, цілісності та доступності інформації. Інформаційна безпека включає в себе не лише технологічні, але й організаційні, правові, соціальні та психологічні аспекти.

Джерелами дестабілізуючих факторів можуть виступати як окремі особи, так і різного роду організації, їхні об'єднання та колективи. У цьому контексті важливо зазначити, що дестабілізуючі фактори можуть мати різноманітні форми, включаючи економічні, політичні, соціальні та культурні загрози. Сукупність цих джерел та видів впливу формує широкий спектр інформаційних загроз, які безпосередньо впливають на рівень інформованості особистості, суспільства і держави в цілому.

Важливо враховувати, що інформаційна безпека не є статичною характеристикою, а постійно змінюється у відповідь на нові виклики і загрози. Сучасні технології, зокрема, впровадження нових інформаційних і комунікаційних технологій, у свою чергу, можуть як зміцнити, так і послабити інформаційну безпеку. З одного боку, вони надають нові можливості для захисту даних і інформаційних систем. З іншого – відкривають нові канали для здійснення кіберзлочинів та інформаційних атак.

Тому для забезпечення інформаційної безпеки держави необхідно розробляти та реалізовувати комплексні стратегії, що включають не лише технологічні рішення, а й підходи, орієнтовані на формування відповідної культури безпеки в суспільстві. У цьому контексті важливу роль відіграють навчання, підвищення обізнаності населення, а також правова регуляція в сфері інформаційної безпеки.

Загалом, інформаційна безпека виступає ключовим елементом у забезпеченні стабільності та розвитку суспільства, оскільки вона охоплює всі аспекти життєдіяльності держави та впливає на її стратегічні інтереси, безпеку громадян і національну цілісність.

Одним із складників забезпечення інформаційної безпеки в державі виступає забезпечення інформаційної безпеки підприємницької діяльності. На цей час своєчасна та об'єктивна інформація є важливим фактором виробництва, який розглядають як один з основних ресурсів розвитку суспільства. Паралельно з розвитком і ускладненням засобів, методів, форм автоматизації процесів обробки інформації підвищується залежність суб'єктів підприємництва від ступеню безпеки використовуваних ними інформаційних технологій [9, С. 205].

У найзагальнішому розумінні інформаційна безпека може бути визначена як стан захищеності інформаційного середовища суспільства, що гарантує його формування, використання та розвиток відповідно до інтересів громадян, організацій і держави. Інформаційне середовище включає в себе сукупність взаємопов'язаних елементів і процесів, які забезпечують створення, обробку та споживання інформації.

Детальніше, інформаційне середовище може бути умовно розділене на кілька ключових компонентів:

1. *Створення та розповсюдження вихідної та похідної інформації.* Цей компонент охоплює процеси генерації інформаційних даних, які можуть виникати в результаті досліджень, аналізу або спостережень. Вихідна інформація може бути первинною, тобто отриманою безпосередньо з джерела, а похідна – це інформація, що виникає на основі обробки вихідних даних. Важливість цього аспекту полягає в тому, що якість і достовірність вихідної інформації є критично важливими для подальшої її обробки та споживання.

2. *Формування інформаційних ресурсів та підготовка інформаційних продуктів.* Цей етап включає в себе організацію та систематизацію інформації для створення інформаційних ресурсів, які можуть використовуватися в різних сферах діяльності. Інформаційні продукти можуть включати звіти, аналітичні огляди, програмне забезпечення тощо. Надання інформаційних послуг, таких як консультації, підтримка в обробці даних, є важливим елементом цього процесу.

3. *Споживання інформації*. Цей компонент охоплює дії осіб або організацій, які використовують наявну інформацію для прийняття рішень, виконання завдань або задоволення інших потреб. Споживання інформації може здійснюватися через різні канали, такі як публікації, електронні медіа, навчальні програми тощо. Важливим є також забезпечення доступності інформації для всіх категорій населення.

4. *Створення та застосування інформаційних систем і технологій*. Інформаційні системи – це складні комплекси, що складаються з апаратного та програмного забезпечення, які забезпечують обробку, зберігання та передачу інформації. Використання інформаційних технологій на всіх етапах – від створення до споживання інформації – є необхідним для підвищення ефективності діяльності підприємств та організацій.

5. *Створення і застосування засобів і механізмів інформаційної безпеки*. У сучасному світі, де загрози інформаційній безпеці стають дедалі більш складними і різноманітними, цей компонент набуває особливого значення. Він включає в себе розробку та впровадження технологій і процедур, які покликані захистити інформацію від несанкціонованого доступу, втрати або пошкодження. Це може бути досягнуто шляхом використання програмних засобів, систем шифрування, політик доступу, а також шляхом навчання користувачів основам безпеки інформації.

Отже, інформаційна безпека є складним і багатогранним процесом, що охоплює всі етапи інформаційного циклу. Вона не лише забезпечує захист інформаційних ресурсів, але і сприяє розвитку інформаційного середовища, яке, у свою чергу, є основою для ефективного функціонування суспільства в цілому. Таким чином, успішна реалізація заходів інформаційної безпеки є критично важливою для збереження стабільності та розвитку як окремих організацій, так і держави в цілому.

Важливо підкреслити, що задоволення потреб в інформації, у будь-якій формі, призводить до накопичення знань про навколишній світ та події, які в

ньому відбуваються. Це сприяє підвищенню рівня інформованості як окремої особи, так і суспільства та держави в цілому [10, С. 46-48].

Концепція інформаційної безпеки держави – це систематизована сукупність відомостей про інформаційну безпеку держави та шляхи її забезпечення. У цій концепції проводиться системна класифікація дестабілізуючих факторів і інформаційних загроз безпеці особистості, суспільства і держави; обґрунтовуються основні положення з організації забезпечення інформаційної безпеки держави; розробляються пропозиції щодо способів і форм забезпечення інформаційної безпеки [10, С. 24-25].

Важливе місце у забезпеченні інформаційної безпеки держави посідає інформаційна безпека підприємницької діяльності. Загрозами інформаційній безпеці сучасного підприємства є: протизаконна діяльність деяких економічних структур у сфері формування, поширення і використання інформації; порушення встановлених регламентів збору, обробки та передачі інформації; навмисні дії та ненавмисні помилки персоналу інформаційних систем; помилки в проектуванні інформаційних систем; відмова технічних засобів і проблеми програмного забезпечення в інформаційних і телекомунікаційних системах тощо [10, С. 28].

Джерела негативних впливів на інформаційну безпеку підприємства можуть бути різноманітними та складатися з кількох категорій.

По-перше, це можуть бути дії окремих посадових осіб і суб’єктів господарювання, які як свідомо, так і несвідомо впливають на безпеку інформації. Сюди належать представники органів державної влади, міжнародних організацій, а також конкуренти, що можуть вдаватися до дій, які загрожують інформаційній безпеці підприємства. Ці дії можуть включати як прямі атаки на інформаційні системи, так і непрямі, наприклад, через регуляторні зміни або інформаційні кампанії, спрямовані на дискредитацію.

По-друге, негативні впливи можуть виникати внаслідок збігу об'єктивних обставин. Це може бути пов'язано зі станом фінансової кон'юнктури на ринках, науковими відкриттями, технологічними розробками

або навіть форс-мажорними обставинами, такими як природні катастрофи або соціально-політичні кризи. Ці фактори можуть істотно вплинути на роботу підприємства і його здатність захищати свої інформаційні ресурси.

Залежно від природи виникнення негативних впливів, їх можна поділити на об’єктивні та суб’єктивні. Об’єктивними вважаються ті впливи, які виникають незалежно від волі конкретного підприємства або його працівників. Наприклад, зміни в економічній ситуації, які підприємство не може контролювати, можуть призвести до зниження його інформаційної безпеки.

Натомість суб’єктивні впливи пов’язані з неефективною діяльністю самого підприємства або окремих його співробітників, зокрема керівників та функціональних менеджерів. Сюди можна віднести недоліки в управлінні, недостатнє навчання персоналу, а також нерегулярне оновлення систем захисту інформації. Саме ці фактори можуть стати причинами уразливостей, які загрожують інформаційній безпеці підприємства.

Отже, негативні впливи на інформаційну безпеку підприємства мають складний характер і вимагають системного підходу для їх усунення, що включає як аналіз об'єктивних обставин, так і вдосконалення внутрішніх процесів управління безпекою.

Основною метою інформаційної безпеки підприємства є забезпечення його стабільного, безперебійного та максимально ефективного функціонування в даний момент, а також створення високого потенціалу для майбутнього розвитку. У сучасних умовах, коли бізнес-середовище стає дедалі складнішим, захист інформаційних активів і систем підприємства набуває особливого значення.

Одним із основних джерел загроз для інтересів суспільства в інформаційній сфері є постійне ускладнення інформаційних систем, а також мереж зв’язку, що становлять критично важливу інфраструктуру для забезпечення нормального функціонування суспільства. Ці системи не лише

підтримують повсякденну діяльність, а й є невід'ємною частиною національної безпеки.

Загрози, що виникають у цій сфері, можуть проявлятися у різних формах. Наприклад, вони можуть бути результатом навмисних дій, таких як кібератаки, або ненавмисних помилок, які виникають через неуважність чи відсутність належної кваліфікації персоналу. Окрім того, можуть відбуватися технічні збої та відмови, пов’язані з апаратним або програмним забезпеченням, які призводять до негативних наслідків для роботи інформаційних систем.

Шкідливі впливи також можуть виходити від злочинних структур і кримінальних елементів, які намагаються скористатися вразливостями в інформаційній інфраструктурі для своїх власних цілей. Об’єктами таких атак можуть бути системи, що забезпечують енергетичні, транспортні, трубопровідні та інші важливі елементи інфраструктури.

Ці системи є критично важливими для безпеки і добробуту суспільства, і їх уразливість може призвести до серйозних наслідків. Наприклад, збої в енергетичних системах можуть спричинити перебої в постачанні електроенергії, що в свою чергу негативно вплине на діяльність підприємств і якість життя громадян. Аналогічно, збої в транспортних мережах можуть призвести до затримок, збільшення витрат та втрати довіри з боку споживачів.

Таким чином, інформаційна безпека підприємства є не лише внутрішньою справою організації, а й важливим аспектом, що впливає на загальну безпеку суспільства. Забезпечення високого рівня інформаційної безпеки потребує комплексного підходу, що включає постійний моніторинг, аналіз ризиків, підвищення кваліфікації персоналу та впровадження сучасних технологій захисту інформації. Це, в свою чергу, дозволить підприємству не лише захистити свої інформаційні активи, а й забезпечити стабільність та розвиток в умовах постійних викликів сучасного світу.

Небезпечним джерелом загроз виступає можливість концентрації засобів масової інформації в руках невеликої групи власників. Ці загрози

можуть проявлятися у вигляді маніпуляції суспільною думкою по відношенню до тих чи інших суспільно значимих подій, а також руйнування моральних устоїв суспільства шляхом нав'язування чужорідних цінностей.

Нарешті, небезпечним джерелом загроз є розширення масштабів вітчизняної і міжнародної комп'ютерної злочинності. Ці загрози можуть проявлятися у вигляді спроб здійснення шахрайських операцій з використанням глобальних або вітчизняних інформаційно-телекомунікаційних систем, відмивання фінансових коштів, одержаних протиправним шляхом, одержання неправомірного доступу до фінансової, банківської та іншої інформації, яка може бути використаною з корисливою метою [11, С. 19-20].

Окрім зазначеного, існує три основних зовнішніх джерела загроз, які можуть негативно вплинути на функціонування підприємства.

По-перше, це може бути несприятлива економічна політика держави. Зміни в валютному курсі, митних ставках, податковій політиці та інших регуляторних аспектах можуть суперечити бізнес-моделям і комерційній стратегії підприємства. Також реальні загрози можуть виникати з адміністративних дій органів влади, які можуть обмежувати товарно-грошові відносини, порушувати законодавство, що регулює підприємницьку діяльність, перевищувати свою компетенцію у стосунках з підприємством, безпідставно втручатися в його фінансову, комерційну та виробничу діяльність, а також зазіхати на власність підприємства. Виходячи на міжнародні ринки, підприємство може також стати жертвою негативного впливу через несприятливу економічну політику інших країн.

По-друге, ще одним джерелом зовнішніх загроз для комерційної діяльності підприємства є дії окремих суб'єктів господарювання. Зокрема, мова йде про недобросовісну конкуренцію, яка визначається по-різному в різних джерелах. Згідно з міжнародно-правовими нормами, можна виокремити три основні види недобросовісної конкуренції: по-перше, це дії, спрямовані на те, щоб подати комерційну діяльність однієї компанії за

діяльність іншої; по-друге, це дискредитація конкурентів шляхом поширення неправдивої інформації про їхню діяльність; по-третє, це неправомірне використання знаків та позначень у процесі комерційної діяльності, що може ввести споживачів в оману.

Форми та методи забезпечення інформаційної безпеки створюють специфічний інструментарій, за допомогою якого органи інформаційної безпеки виконують комплекс завдань, спрямованих на захист життєво важливих інтересів особистості, суспільства та держави. У зв'язку з цим важливо забезпечити належне юридичне оформлення при розробці нормативних актів, які регулюють діяльність органів інформаційної безпеки.

Інформаційний патронат – форма забезпечення інформаційної безпеки фізичних і юридичних осіб з боку держави. Він припускає забезпечення органів управління системи інформаційної безпеки держави відомостями про дестабілізуючі фактори і загрози стану інформованості фізичних і юридичних осіб (інформаційне забезпечення інформаційної безпеки) і, власне, захист життєво важливих інтересів цих осіб від інформаційних загроз або, як ще кажуть, – інформаційний захист [12].

Оскільки всі елементи та підсистеми в будь-якій системі мають взаємозв'язок, більшість завдань у сфері інформаційної безпеки реалізуються у співпраці з основними та допоміжними підсистемами економічної безпеки підприємства. Технічний аспект відповідає за захист інформації та активів підприємства, а також за виявлення фактів витоку інформації та неправомірних дій як з боку персоналу, так і сторонніх осіб, за допомогою технічних засобів.

Організаційний компонент, на нашу думку, має забезпечувати правильне поводження співробітників із конфіденційною інформацією та іншими об'єктами, які потребують захисту в межах господарюючого суб'єкта.

Дозвільний компонент системи інформаційної безпеки відповідає за класифікацію інформації підприємства за рівнями секретності та визначення ступеня доступу до неї. Щоб уникнути дезінформації, яка може призвести до

прийняття помилкових управлінських рішень, а також для зниження ймовірності витоку секретної інформації, система інформаційної безпеки повинна включати *попереджувальний компонент*. Правовий аспект забезпечує захист юридичних інтересів підприємства у сфері інформації та закріплює права на комерційну таємницю в установчих документах, договорах та інших нормативних актах.

Пропоновані науковцями та практиками системи захисту інформації не повною мірою враховують всі завдання та функції, які стоять перед захистом інформації в системі інформаційної безпеки та інформаційного забезпечення в цілому в сучасних умовах. Основними завданнями системи захисту інформації можна вважати:

- організацію спеціального діловодства та контролю за секретними документами;

- виявлення, попередження та припинення каналів витоку інформації;

- створення посадових інструкцій, положень, пам’яток та методичних рекомендацій для роботи з інформацією, що є комерційною таємницею;

- захист інформації під час використання комп’ютерних технологій та інших технічних засобів обробки та передачі даних;

- виявлення потреби, обґрунтування та організацію впровадження необхідних технічних засобів для збереження інформації;

- захист інтересів підприємства у судових та інших державних органах у справах, що стосуються комерційної таємниці;

- розроблення нормативної документації з питань комерційної таємниці на підприємстві;

- навчання співробітників правилам інформаційної безпеки.

Оскільки система захисту інформації є найважливішою частиною інформаційної безпеки, більшість складових елементів у цій системі належать саме до захисту інформації. Таким чином, технічний, організаційний та правовий компоненти відносяться до системи захисту інформації. Крім того, до системи захисту інформації включається попереджувальний компонент,

який охоплює передбачення, виявлення та блокування каналів витоку інформації.

Безпека сучасного комерційного підприємства забезпечується через реалізацію кількох ключових режимів:

1. *Режим конфіденційності,* що включає в себе захист об'єктів інтелектуальної власності, який є невід'ємною складовою інформаційної безпеки.

2. *Фізична охорона*, що передбачає забезпечення фізичної безпеки майна підприємства та його персоналу.

В умовах, що панують на українському ринку, підприємці можуть розраховувати на ефективний захист своїх життєво важливих інтересів лише в тому випадку, якщо вони здатні організувати процес, орієнтований на процедури, що спрямований на запобігання доступу потенційних супротивників до інформації про виробничі та торговельні можливості і наміри підприємства. Це досягається, зокрема, шляхом виявлення та усунення індикаторів (демаскуючих ознак і каналів витоку інформації), що пов'язані з плануванням і здійсненням підприємницької діяльності. Важливо, щоб у цьому процесі брали участь усі працівники підприємства, а не лише служба безпеки.

Концепція системного підходу до забезпечення інформаційної безпеки полягає у припиненні, зменшенні або, в крайньому випадку, обмеженні витоку цінної інформації, яка може надати конкурентам можливість передбачити плани та дії керівництва фірми.

На жаль, в Україні майже відсутні важливі складові, необхідні для реалізації системного підходу, такі як:

- достатньо розвинена законодавча база, що регулює основні відносини у бізнес-сфері, адже приватне право та юридичне забезпечення економічної діяльності в нашій країні все ще потребують удосконалення;

- налагоджений механізм економічних реформ на загальнодержавному та регіональному рівнях;

- високий рівень залучення суспільства до процесів економічних змін;
- державна програма боротьби з корупцією в національній економіці;
- ефективна національна статистика та контроль.

Ігнорування принципів ринкової економіки та вимог економічної безпеки часто призводить до негативних наслідків, таких як втрата вигідних угод, укладання контрактів з недобросовісними партнерами або прийняття на роботу осіб з низькими моральними стандартами, які можуть бути пов'язані з недобросовісною конкуренцією або організованою злочинністю. Тому збереження необхідного рівня економічної безпеки є легшим, дешевшим і вигіднішим, ніж ведення тривалих і часто невдалих судових процесів, що вимагають значних фінансових витрат для захисту своїх прав.

Серед ключових механізмів забезпечення інформаційної безпеки підприємницької діяльності в Україні, яка є важливим елементом загальної інформаційної безпеки держави, доцільно виділити кілька основних складових. По-перше, це інформаційний патронат, який передбачає захист інформаційних ресурсів підприємств на рівні держави та спеціалізованих організацій. По-друге, інформаційний захист, що охоплює судовий, адміністративний і автономний захист, має на меті забезпечення правового захисту інформації від різного роду загроз. Третім важливим механізмом є інформаційна кооперація, що передбачає спільні дії підприємств та держави в сфері обміну інформацією і ресурсами для підвищення рівня безпеки. Четвертим є формування ефективних систем захисту інформації, які повинні включати технічні, організаційні та кадрові заходи для запобігання витокам і несанкціонованому доступу.

У сучасних умовах ефективне забезпечення безпеки підприємницької діяльності, як і всієї національної економіки, повинно базуватися на системному підході, що включає ряд взаємопов’язаних заходів. Серед цих заходів необхідно відзначити захист від злочинного світу, який передбачає вжиття заходів протидії кримінальним елементам. Далі, важливим є захист від порушень законодавства, щоб уникнути можливих санкцій. Не менш

актуальним є захист від недобросовісної конкуренції, що може завдати шкоди підприємству, а також захист від протиправних дій з боку власних співробітників.

Забезпечення інформаційної безпеки підприємницької діяльності в Україні має ґрунтуватися на специфічних принципах, серед яких визначальними є превентивний характер проведених заходів та адекватна інформованість об'єктів безпеки, включаючи міжнародні аспекти. Це створює потребу в розробці конкретних механізмів реалізації зазначених принципів, що, в свою чергу, визначає перспективи подальших досліджень у цій важливій галузі. Таким чином, ефективна інформаційна безпека стає ключовим чинником стабільності та розвитку підприємств, а також економіки країни в цілому.

1.3. Місце інформаційної безпеки в загальній системі економічної безпеки підприємства

У сучасних умовах економічної діяльності особливо актуальним є питання обґрунтування механізмів захисту економічних інтересів українських підприємств, а також прийнятих стратегічних рішень. Процеси євроінтеграції ставлять перед підприємствами України ряд вимог, що змушує їх адаптуватися до зростаючого рівня конкуренції, а також шукати адекватні рішення для вирішення найскладніших проблем і зменшення загроз, які виникають у результаті конфліктності, невизначеності та ризиків.

На жаль, сучасні наукові дослідження, що стосуються діяльності національних підприємств, не забезпечують цілісного розуміння питання економічної безпеки бізнесу. Зокрема, практично відсутнє чітке уявлення про характер функціонування системи в умовах агресивного середовища, а також про механізми забезпечення економічної безпеки підприємств у контексті глобалізації бізнесу в цілому. У нинішніх умовах ведення бізнесу постає серйозна проблема забезпечення економічної безпеки підприємств, оскільки

ефективне вирішення цього питання безпосередньо впливає на економічне зростання національної економіки.

Основною метою забезпечення економічної безпеки підприємства є створення системи, яка протидіє як потенційним, так і реальним загрозам. Це передбачає розробку превентивних заходів, спрямованих на усунення або мінімізацію ризиків, що забезпечить суб’єкту господарювання успішну діяльність у нестабільних умовах як зовнішнього, так і внутрішнього середовища. Безпека підприємства повинна бути забезпечена за кількома ключовими напрямами, зокрема економічною, науково-технічною, інформаційною, кадровою, соціальною, екологічною та фізичною безпекою.

Прорив інформаційних технологій наприкінці XX – на початку XXI сторіччя викликав у світі значні системні перетворення, що дали можливість сформуватись і розвинутись принципово новим і невід’ємним глобальним субстанціям – інформаційному простору та інформаційному суспільству. Неконтрольоване поширення та необмежене застосування провідними країнами світу інформаційного простору як арени дій у процесі сучасного інформаційного протиборства поступово привело до уразливості інформаційної сфери цих країн до впливу внутрішніх і зовнішніх кібернетичних втручань та загроз навмисного, випадкового, природного або штучного характеру [13].

Питання інформаційної безпеки стало невід'ємною частиною стратегії управління для багатьох великих національних і міжнародних компаній, що зумовлено необхідністю захисту від ризиків, пов'язаних із використанням інсайдерської інформації. Упродовж останніх років спостерігається тенденція, коли керівники середнього та малого бізнесу в Україні також починають усвідомлювати серйозність загроз, що можуть виникнути внаслідок зовнішніх і внутрішніх втручань в інформаційні системи їхніх підприємств.

Зовнішнє та внутрішнє втручання може суттєво вплинути на конфіденційність, цілісність, доступність і достовірність інформації, що, у

свою чергу, може призвести до серйозних негативних наслідків для функціонування підприємства. Серед цих наслідків варто виділити:

1. *Збої у функціонуванні систем управління технологічними та управлінськими процесами*. Порушення інформаційних потоків може призвести до неефективного управління ресурсами та затримок у виробництві.

2. *Розголошення комерційних та інших таємниць*. Втрата конфіденційності може загрожувати конкурентоспроможності підприємства.

3. *Порушення достовірності фінансової звітності*. Викривлення фінансової інформації може знизити довіру інвесторів та партнерів.

4. *Несанкціонований доступ до бази даних підприємства*. Це може призвести до крадіжки інформації, яка є критично важливою для бізнесу.

5. *Викривлення публічної інформації*. Неправильні або маніпулятивні дані можуть знизити репутацію компанії в очах громадськості.

Наслідки викривлення інформації можуть мати катастрофічні наслідки для підприємства, включаючи:

зменшення вартості капіталу – неправдива інформація може призвести до зниження інтересу з боку інвесторів;

складнощі у залученні інвестицій – інвестори можуть відмовитися фінансувати компанію через сумніви у її надійності;

розрив або погіршення ділових відносин із партнерами – партнери можуть втратити довіру до підприємства, що веде до зниження співпраці;

зрив переговорів і втрата вигідних контрактів – неправдиві дані можуть знищити можливості укладення вигідних угод;

відмова від рішень, які стали неефективними через розголос інформації – неправильні рішення можуть призвести до фінансових втрат;

втрата можливості запатентувати результати науково-технічної діяльності – це може загрожувати інноваційній діяльності компанії;

зниження цін або обсягів реалізації – невірна інформація може призвести до зниження попиту на продукцію;

втрата репутації та авторитету компанії – це може мати тривалий негативний вплив на бізнес;

більш жорсткі умови отримання кредитів – фінансові установи можуть підвищити ризики для підприємства через інформаційні втрати;

труднощі в постачанні та придбанні обладнання - втрата довіри постачальників може ускладнити ведення бізнесу.

У критичних випадках недотримання принципів інформаційної безпеки може призвести до повної втрати бізнесу, що робить питання захисту інформації вкрай важливим.

Концепцію інформаційної безпеки слід розглядати з кількох аспектів. По-перше, це стан захищеності інформаційного середовища, що забезпечує його формування, використання і розвиток в інтересах громадян, організацій і держави. По-друге, це стан захищеності інформаційних потреб індивідуумів, суспільства та держави, за якого гарантовано їх існування і прогресивний розвиток незалежно від наявності внутрішніх та зовнішніх загроз.

Спектр інтересів у сфері інформаційної безпеки, що стосується інформації, інформаційних систем і інформаційних технологій як об'єктів безпеки, можна класифікувати на три основні категорії: доступність, цілісність та конфіденційність.

1. *Доступність* визначає можливість отримання конкретної інформаційної послуги у визначений проміжок часу. Це означає, що користувачі повинні мати змогу отримати доступ до інформації та систем у будь-який момент, коли це необхідно, без затримок або перешкод. Забезпечення доступності є критично важливим для підтримки ефективності бізнес-процесів та реагування на запити клієнтів.

2. *Цілісність* інформації характеризується її релевантністю та несуперечливістю. Це означає, що інформація повинна бути точною, повною і незмінною протягом часу, зокрема, вона повинна бути захищена від руйнування та несанкціонованих змін. Відсутність цілісності може призвести

до серйозних помилок у прийнятті рішень, оскільки дані можуть бути спотворені або некоректно відображати реальність.

3. *Конфіденційність* вказує на захищеність інформації від несанкціонованого доступу. Це аспект безпеки, який гарантує, що тільки авторизовані особи мають доступ до чутливої інформації, що є критично важливим для захисту комерційної таємниці та персональних даних.

З точки зору інформаційних технологій, інформаційна безпека є системою заходів, що дозволяє виявляти вразливі місця інформаційно-комунікаційних систем підприємства, а також ідентифікувати загрози, що можуть вплинути на їх функціонування, і методи їх нейтралізації.

Загроза визначається як подія, здатна спричинити порушення функціонування інформаційної системи, що включає спотворення, знищення або несанкціоноване використання бази даних. Суть загрози полягає в тому, що вона може знизити ефективність операцій або навіть призвести до серйозних фінансових втрат.

Можливість реалізації загроз безпосередньо залежить від наявності вразливих місць у інформаційній системі. Склад і специфіка таких вразливостей визначаються типом вирішуваних завдань, характером оброблюваної інформації, а також апаратно-програмними особливостями, які використовуються в підприємстві. Додатково, важливу роль відіграє також наявність та ефективність засобів захисту, оскільки їх характеристики можуть суттєво вплинути на загальний рівень інформаційної безпеки.

У зв'язку з цим, забезпечення інформаційної безпеки має бути інтегрованим підходом, що враховує всі ці аспекти та активно впроваджує відповідні заходи для їхнього захисту. Це може включати як технічні рішення (системи шифрування, брандмауери, антивірусні програми), так і організаційні заходи (регламенти, політики доступу, навчання персоналу), що в сукупності забезпечить надійний захист інформації та зменшить ризики, пов’язані з інформаційними загрозами.

Аналіз теорії та практики свідчить про наявність двох основних категорій загроз для інформаційної безпеки підприємства. Ці категорії включають ненавмисні або випадкові дії, а також навмисні загрози.

Ненавмисні або випадкові дії являють собою загрози, що виникають внаслідок неадекватної підтримки механізмів захисту, а також через помилки в управлінні. Такі дії можуть бути викликані недбалим ставленням до процесів безпеки, недосвідченістю персоналу або відсутністю належних процедур. Наприклад, випадкове видалення важливих даних, неправильна конфігурація системи або неуважність співробітників можуть призвести до серйозних наслідків, які вплинуть на функціонування підприємства.

Навмисні загрози є результатом свідомих дій, спрямованих на завдання шкоди інформаційним системам. Це може включати несанкціонований доступ до інформації, крадіжку даних, а також маніпуляції з ресурсами та самими інформаційними системами. Такі дії можуть вчинятися як з боку зовнішніх осіб, таких як хакери, так і з боку внутрішніх користувачів, які мають доступ до системи. Наприклад, недобросовісні співробітники можуть використовувати свої привілеї для отримання конфіденційної інформації з метою її подальшого розголошення або продажу конкурентам.

Класифікація загроз для інформаційної безпеки може також базуватися на поділі загроз на ті, що пов’язані з внутрішніми і зовнішніми факторами.

Внутрішні загрози виникають внаслідок дій або бездіяльності співробітників підприємства. Вони можуть бути як ненавмисними, так і навмисними. Внутрішні загрози є особливо небезпечними, оскільки часто мають місце в умовах наявності доступу до чутливої інформації та ресурсів підприємства. Внутрішні користувачі можуть, наприклад, випадково порушити політики безпеки або, навпаки, свідомо скористатися своїми правами для нанесення шкоди.

Зовнішні загрози походять ззовні організації і можуть бути представлені різними формами атак, такими як кібератаки, фішинг, шкідливе програмне забезпечення або соціальна інженерія. Ці загрози часто є більш очевидними,

однак їх складність і різноманіття постійно зростають, ускладнюючи завдання захисту інформації.

Загалом, усвідомлення різноманітних типів загроз інформаційній безпеці підприємства, а також розуміння їх походження та механізмів дії, є ключовим для формування ефективних стратегій управління безпекою. Підприємствам необхідно не лише виявляти та аналізувати загрози, а й розробляти та впроваджувати відповідні заходи для їх нейтралізації. Це може включати як технічні засоби захисту, так і організаційні заходи, спрямовані на підвищення обізнаності співробітників щодо проблем безпеки та забезпечення належної підтримки процесів захисту інформації.

Окремо варто виділити загрози, пов’язані з навмисними помилками, що виникають за межами бізнесу. До таких загроз відносять [13, 14]:

– несанкціонований доступ до інформації, що зберігається в системі;

– заперечення дій, пов’язаних із маніпулюванням інформацією (наприклад, несанкціонована модифікація, яка веде до порушення цілісності даних);

– введення в програмні продукти і проекти «логічних бомб», які спрацьовують за виконання певних умов або після закінчення певного періоду часу і частково або повністю виводять з ладу комп’ютерну систему;

– розроблення і поширення комп’ютерних вірусів; – недбалість у розробленні, підтримці та експлуатації програмного забезпечення, що приводить до краху комп’ютерної системи;

– зміна комп’ютерної інформації і підробка електронних підписів;

– розкрадання інформації з подальшим маскуванням;

– перехоплення інформаційних потоків;

– заперечення дій або послуги;

– відмова в наданні послуги.

На жаль, слід зазначити, що єдиний, уніфікований підхід до класифікації загроз інформаційній безпеці на сьогоднішній день відсутній. Це відсутність системи зрозуміла, адже існує велике різноманіття інформаційних систем, які

призначені для автоматизації численних технологічних процесів, що охоплюють різні сфери людської діяльності. У таких умовах жорстка систематизація та класифікація загроз є неприйнятними, оскільки кожна система має свої унікальні характеристики, структуру та контекст використання.

Врахування особливостей різних інформаційних систем, їхньої специфіки, а також унікальних факторів середовища, в якому вони функціонують, вимагає гнучкого підходу до класифікації загроз. Системи можуть мати різні рівні доступу, типи даних, які вони обробляють, та рівень вразливості до загроз, що ускладнює створення універсальних категорій загроз.

Таким чином, для ефективного управління інформаційною безпекою важливо розробити адаптивні підходи до класифікації загроз, які враховували б особливості конкретної інформаційної системи, а також зміни в технологічному середовищі та зовнішньому контексті. Це дозволить більш точно ідентифікувати потенційні загрози та розробити відповідні заходи для їх нейтралізації.

Дослідивши джерела [13, 14], можна запропонувати таку класифікацію загроз:

За проявом та наслідками: злочин; шахрайство; хуліганство;

За типом – програмне; апаратне, інше;

За метою – оперативні, тактичні, стратегічні;

За характером виникнення – навмисні, ненавмисні;

За інформаційними технологіями – об’єкт загроз, методи підготовки загроз, інструментарій загроз, середовище загроз;

За місцем виникнення – інсайдерські, зовнішні;

За об’єктом впливу – системні, локальні;

За причиною виникнення – збої в обладнанні, збої в роботі програмного забезпечення, недосконала архівація даних, несанкціонований доступ.

Розвиток інформаційних технологій та комунікаційних засобів створює дедалі більше можливостей для доступу до інформаційних ресурсів та переміщення великих обсягів даних на значні відстані. Відкритий доступ широкого кола користувачів, які можуть перебувати у будь-якому місці, до ресурсів, розташованих в рамках глобальної інформаційної мережі, суттєво підвищує ризики для інформаційних ресурсів підприємства, а також для інформаційних систем загалом.

У цьому контексті інформація, яка є важливим товаром, потребує належного збереження та надійного захисту. Одним із ключових напрямів діяльності, що забезпечує інформаційну безпеку підприємства, є виявлення, оцінка та запобігання загрозам для інформаційно-комунікаційних систем і ресурсів.

Сучасні корпоративні системи інформаційної безпеки покликані захищати конфіденційну інформацію від несанкціонованого доступу, запобігати зловмисним або випадковим змінам, що дозволяє контролювати цілісність даних, а також забезпечувати необхідний рівень доступу до інформації.

Забезпечення інформаційної безпеки включає три основні напрямки: технічні, адміністративні та організаційні заходи, які діють у комбінації.

Отже, у сучасних умовах господарювання, коли інформаційні технології набувають глобального масштабу, інформаційна безпека виступає невід’ємним елементом системи економічної безпеки як окремого господарюючого суб’єкта, так і держави в цілому. Це підкреслює важливість інтеграції інформаційної безпеки у всі аспекти економічної діяльності, що дозволяє забезпечити стійкість та конкурентоспроможність у динамічному та ризикованому інформаційному середовищі.

РОЗДІЛ 2. ОЦІНКА СУЧАСНИХ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ПІДПРИЄМСТВ

2.1. Основні загрози інформаційній безпеці

На сучасному етапі розвитку інформаційних технологій загрози інформаційній безпеці підприємств стають складнішими, а їхня кількість та масштаби впливу на бізнес постійно зростають. Інформаційні активи підприємств, що включають комерційну, технічну та іншу важливу інформацію, є основними чинниками їхньої конкурентоспроможності. Захист інформації стає стратегічним пріоритетом, адже витік, модифікація чи пошкодження даних можуть завдати суттєвих фінансових втрат, призвести до втрати репутації та конкурентних переваг. Розглянемо основні загрози інформаційній безпеці, що становлять ризики для підприємств у різних секторах економіки.

Однією з найбільших загроз інформаційній безпеці є кіберзлочинність, що охоплює широкий спектр незаконних дій, які здійснюються через інформаційні системи або з використанням технологій. Кіберзлочинці часто націлені на крадіжку конфіденційної інформації, злам внутрішніх мереж підприємства, атаки на бази даних або інші ресурси, зокрема для збору особистої інформації, комерційної таємниці або фінансових даних. За останні роки частота кіберзлочинів суттєво зросла, що пов'язано з активним розвитком технологій та зростанням частки комерційної діяльності в Інтернеті.

Методи кіберзлочинців постійно вдосконалюються: від звичайних фішингових атак до використання передових методів соціальної інженерії та розповсюдження шкідливих програм. Злочинці маніпулюють користувачами, змушуючи їх виконувати дії, які відкривають доступ до захищених систем. За даними міжнародного дослідження, понад 60% компаній щорічно стикаються з кіберзагрозами, що вказує на високий рівень ризику та необхідність посиленої уваги до кібербезпеки [15, С. 18].

Інформаційна безпека підприємств на сучасному етапі стикається з новими методами кібератак. Важливо відзначити, що злочинці не лише вдосконалюють свої техніки, але й активно розробляють нові інструменти для обхідного шляху захисних систем. Наприклад, сучасні кіберзлочинці часто використовують бот-мережі, які складаються з безлічі комп'ютерів або пристроїв з інтернет-з’єднанням, що були заражені шкідливим програмним забезпеченням. Власники таких пристроїв часто не знають про їхнє використання в кібератаках. Відзначимо, що бот-мережі застосовуються для здійснення DDoS-атак та розповсюдження спаму.

Для боротьби з кіберзлочинністю важливо впроваджувати оновлення систем безпеки, встановлювати інструменти для виявлення аномалій, фільтрувати підозрілий трафік та застосовувати сучасні антивірусні програми. Зокрема, варто впроваджувати систему контролю доступу на основі ролей (RBAC), що обмежує доступ до критичних даних лише тим співробітникам, які дійсно цього потребують [16, С. 27-28].

Атаки типу DoS (Denial of Service) і DDoS (Distributed Denial of Service) є поширеним способом виведення з ладу інформаційних систем підприємства. Ці атаки зазвичай націлені на перевантаження серверів або мережевих ресурсів підприємства, що тимчасово блокує їх роботу. Такі дії можуть спричиняти значні фінансові збитки та втрати клієнтів, особливо для підприємств, що надають онлайн-послуги або працюють з великою кількістю користувачів.

За останніми статистичними даними, кількість DDoS-атак щорічно зростає на 10-15%, що свідчить про тенденцію до збільшення ризиків. Відомо, що злочинці нерідко використовують DoS-атаки для відволікання уваги служби безпеки, здійснюючи паралельно інші кіберзлочини, наприклад, крадіжку конфіденційної інформації або встановлення шкідливого ПЗ на сервери підприємства [17].

Фішинг та соціальна інженерія є одними з найбільш розповсюджених методів, які використовують зловмисники для отримання конфіденційної

інформації. Фішингові атаки спрямовані на те, щоб обманом змусити жертву розкрити свої облікові дані, наприклад, шляхом надсилання електронного листа, який виглядає як офіційне повідомлення від банку чи іншої установи. Поширеною формою є spear-фішинг, коли злочинці збирають інформацію про конкретну особу чи організацію, щоб виглядати правдоподібніше [18].

Для боротьби з фішингом важливо впроваджувати навчальні програми для працівників, які включають навчання розпізнаванню підозрілих електронних листів та посилань. Окрім цього, корисно використовувати багатофакторну автентифікацію, що значно ускладнює доступ до системи навіть у випадку крадіжки облікових даних.

Однією з основних загроз є шкідливе програмне забезпечення (або "малваре", від англ. malware) – спеціальні програми, що використовуються зловмисниками для отримання несанкціонованого доступу до інформаційних ресурсів або пошкодження даних. Основні види шкідливого програмного забезпечення включають віруси, троянські програми, шпигунське програмне забезпечення та програми-вимагачі.

Програми-вимагачі, зокрема, стають все більш популярними серед кіберзлочинців через свою здатність приносити високий прибуток. Наприклад, у 2021 році кількість атак із використанням програм-вимагачів зросла на 40%, і зловмисники вимагали викуп за розблокування доступу до даних або відновлення контролю над системою. Цей тип загроз є особливо небезпечним для малих та середніх підприємств, які можуть не мати достатніх фінансових і технічних ресурсів для швидкого відновлення після атаки [19, С. 172].

Програми-вимагачі, або ransomware, стали однією з найсерйозніших загроз для бізнесу. Ці програми блокують доступ до даних на комп'ютері або системі до тих пір, поки власник не виплатить викуп. Найчастіше атаки реалізуються через відкриття заражених вкладень електронних листів або через інфіковані сайти. Підприємства, які не мають резервних копій даних, часто стають жертвами цих атак, адже втрата інформації може спричинити значні фінансові втрати та збитки для репутації.

Для захисту від атак із використанням програм-вимагачів необхідно регулярно створювати резервні копії важливих даних та зберігати їх у захищеному місці, наприклад, на зовнішніх носіях чи у хмарних сервісах з багаторівневим захистом. Також варто забезпечити регулярне оновлення системи та програмного забезпечення для уникнення експлуатації вразливостей, через які здійснюється проникнення в систему.

Витік даних є однією з найпоширеніших загроз інформаційній безпеці, адже втрата чи розголошення конфіденційної інформації може призвести до серйозних фінансових втрат, втрати репутації та клієнтів. Витоки даних можуть відбуватися як внаслідок дій зловмисників, так і через помилки або недбалість співробітників підприємства. За статистикою, до 30% витоків даних спричинені людськими помилками або недостатнім контролем доступу.

Важливу роль у запобіганні витокам відіграє підвищення обізнаності співробітників у питаннях інформаційної безпеки, зокрема регулярні тренінги та навчальні програми. Також компанії часто використовують багаторівневі системи контролю доступу, щоб мінімізувати ймовірність несанкціонованого доступу до важливих даних [20].

Недосконалості в програмному забезпеченні або інформаційних системах, які експлуатують компанії, можуть стати "вхідними дверима" для зловмисників. Такі вразливості можуть бути пов’язані з недостатнім тестуванням або поспішним впровадженням нових функцій. Згідно з дослідженнями, кожен четвертий кіберзлочин стається через використання вразливостей у програмному забезпеченні [21, С. 94].

Для підприємств, що працюють із комплексними інформаційними системами, ці вразливості становлять особливий ризик. Оновлення програмного забезпечення та впровадження політик кібербезпеки є необхідними заходами для мінімізації таких ризиків. Тим не менш, на усунення вразливостей потрібні значні фінансові та людські ресурси, що може бути викликом для багатьох організацій.

Ще одним значущим ризиком для підприємств є вразливості в програмному забезпеченні, які зловмисники можуть використовувати для отримання несанкціонованого доступу до інформаційних систем. Зокрема, вразливості в поширених програмних продуктах, таких як операційні системи та офісні пакети, регулярно стають причинами атак, оскільки на підприємствах не завжди своєчасно впроваджуються оновлення безпеки [22, С. 105].

Для захисту необхідно впроваджувати політику регулярного оновлення та моніторингу програмного забезпечення, а також використовувати системи виявлення вторгнень (IDS), що дозволяють ідентифікувати підозрілу активність в мережі. Особливу увагу варто приділяти тестуванню безпеки нових програмних продуктів перед їх впровадженням.

Внутрішні загрози можуть виникати як через випадкові дії співробітників, так і через навмисні дії осіб, які мають доступ до конфіденційної інформації. Внутрішні ризики охоплюють випадки, коли працівники ненавмисно сприяють витоку даних або надають доступ до інформаційних систем стороннім особам, а також випадки, коли особи здійснюють цілеспрямовані дії для завдання шкоди підприємству через особисті інтереси або конфліктні ситуації.

Щоб знизити ризик внутрішніх загроз, підприємства використовують моніторинг дій співробітників і впроваджують системи для аналізу аномальної поведінки користувачів, що дозволяє виявляти потенційні інциденти безпеки на ранніх стадіях [23].

Внутрішні загрози можуть мати значний вплив на інформаційну безпеку підприємств, адже співробітники мають доступ до внутрішніх ресурсів та конфіденційної інформації. Внутрішні загрози часто виникають внаслідок недбалості або умисних дій працівників, які можуть спричинити витік даних чи інші порушення безпеки.

Для мінімізації внутрішніх загроз варто впроваджувати моніторинг дій співробітників та системи аналізу поведінки користувачів, які здатні

ідентифікувати аномалії. Також необхідно розробити чіткі політики безпеки та забезпечити регулярне навчання персоналу щодо важливості дотримання стандартів інформаційної безпеки. Крім цього, корисно встановлювати політики обмеження доступу до конфіденційної інформації, що дозволяє зменшити ризик витоку даних з боку персоналу.

Використання хмарних технологій і мобільних пристроїв для зберігання та обробки корпоративних даних створює нові виклики для забезпечення інформаційної безпеки. Підприємства, що користуються хмарними сервісами, можуть зіткнутися з проблемою контролю над збереженням і обробкою інформації, якщо провайдер не забезпечує належного рівня захисту.

Мобільні пристрої також становлять ризик, адже працівники можуть користуватися незахищеними мережами або ненадійними додатками, які відкривають доступ до конфіденційної інформації. Для захисту хмарних даних та інформації на мобільних пристроях рекомендується використовувати методи шифрування, контроль доступу та антивірусні програми, що дозволяє зменшити ймовірність компрометації даних [24].

Поширення мобільних пристроїв для роботи з корпоративними даними підвищує ризик витоку конфіденційної інформації. Часто співробітники підключаються до публічних мереж або використовують додатки, які можуть не відповідати стандартам корпоративної безпеки, що створює можливості для перехоплення даних зловмисниками.

Для захисту важливо використовувати VPN (віртуальні приватні мережі) під час підключення до публічних мереж, а також впроваджувати політику BYOD (bring your own device), яка передбачає певні вимоги до використання особистих пристроїв для роботи. Окрім того, варто застосовувати системи контролю доступу до корпоративних даних на основі розташування, що знижує ризик доступу до інформації з незахищених мереж.

Інтеграція технологій штучного інтелекту та машинного навчання у системи інформаційної безпеки підприємств дозволяє значно підвищити рівень захисту. Зокрема, штучний інтелект здатний аналізувати великі обсяги

даних та ідентифікувати аномалії у поведінці користувачів або у мережевій активності, що вказує на можливу кібератаку. Системи на базі штучного інтелекту автоматично визначають підозрілі дії та можуть миттєво реагувати на загрози [25].

Важливим прикладом є використання штучного інтелекту для прогнозування нових типів кібератак на основі аналізу попередніх випадків. Це дозволяє підприємствам бути готовими до атак, що розвиваються, та вчасно впроваджувати захисні заходи. Також варто відзначити системи глибокого навчання, що використовуються для виявлення фішингових атак та захисту від шкідливого програмного забезпечення.

Основні загрози інформаційній безпеці підприємств охоплюють широкий спектр дій, що здійснюються зловмисниками як ззовні, так і зсередини, а також спричиняються випадковими діями співробітників. Ефективний захист інформаційних ресурсів вимагає всебічного підходу, що включає технічні, організаційні та освітні заходи. Впровадження систем моніторингу, шифрування даних, контроль доступу, регулярне навчання персоналу та адаптація нових технологій дозволяють зменшити ризик витоку та втрати інформації, забезпечуючи надійний рівень інформаційної безпеки.

Захист інформаційної безпеки підприємств на сучасному етапі розвитку технологій вимагає багатокомпонентного підходу та активного впровадження новітніх технологій. Досягнення високого рівня безпеки можливе лише за умови реалізації як технічних, так і організаційних заходів, що враховують особливості сучасних загроз. Розвиток технологій штучного інтелекту, автоматизація процесів моніторингу та системи контролю доступу на основі поведінки користувачів є ключовими інструментами для забезпечення надійного захисту інформації. Таким чином, інформаційна безпека повинна бути постійним пріоритетом для підприємств, що прагнуть уникнути ризиків, пов'язаних із компрометацією конфіденційної інформації та порушенням їхньої діяльності.

2.2. Аналіз вразливостей інформаційних систем підприємств

На сучасному етапі розвитку економіки та технологій інформаційні системи є основою ефективного функціонування будь-якого підприємства. Інформація, яка циркулює в системах, є цінним активом, що забезпечує не лише безперервність бізнес-процесів, але й формує конкурентні переваги на ринку. Інформаційні системи підтримують виконання таких критично важливих завдань, як управління даними клієнтів, фінансовими операціями, інвентаризацією, логістикою, маркетинговою аналітикою тощо. Проте, зі зростанням обсягів оброблюваних даних, а також зі збільшенням кількості користувачів та точок доступу, підвищується і рівень ризиків, пов'язаних із вразливостями інформаційних систем.

Захист інформаційних систем стає пріоритетом для підприємств різних галузей, оскільки будь-яка вразливість може бути використана кіберзлочинцями для отримання несанкціонованого доступу до критично важливої інформації або навіть для зупинки операцій компанії. За даними останніх звітів з кібербезпеки, кількість інцидентів, пов’язаних з кіберзагрозами, щороку збільшується, а компанії витрачають значні кошти на усунення наслідків атак та на вдосконалення систем захисту. Така тенденція вимагає системного підходу до виявлення та оцінки вразливостей, що дає змогу мінімізувати можливі ризики, пов'язані з функціонуванням інформаційних систем, і уникнути значних збитків.

Актуальність аналізу вразливостей інформаційних систем обумовлена як збільшенням числа та складності загроз, так і необхідністю дотримання нормативних вимог щодо захисту даних. Для підприємств, що оперують конфіденційною інформацією, захист від зовнішніх та внутрішніх загроз є важливим елементом стратегії економічної безпеки, а також має значний вплив на підтримання репутації серед клієнтів і партнерів. Крім того, існує потреба у впровадженні кращих практик кібербезпеки, таких як регулярне тестування систем на проникнення, аудит безпеки, впровадження політик

управління доступом, що забезпечують цілісність, конфіденційність і доступність даних.

Інформаційні системи підприємств є багаторівневими структурами, що складаються з апаратного забезпечення, програмного забезпечення, комунікаційних мереж і даних. Усі ці компоненти можуть мати вразливості, тобто недоліки, які зловмисники можуть використовувати для несанкціонованого доступу, маніпуляцій або порушення цілісності інформаційних процесів. Відповідно до стандартів кібербезпеки, вразливості інформаційних систем зазвичай класифікуються за кількома основними типами: технічні, організаційні, фізичні та операційні [26, С. 53]. Така класифікація дозволяє структурувати процес управління кіберризиками та обрати відповідні методи для захисту інформаційної системи.

Технічні вразливості пов'язані з недосконалостями в програмному або апаратному забезпеченні, які можуть виникати як на етапі розробки, так і при експлуатації системи. Цей тип вразливостей є найбільш поширеним, оскільки сучасні інформаційні системи містять величезну кількість компонентів з різноманітними функціями [27]. Технічні вразливості включають:

1. Недоліки в програмному забезпеченні – баги, помилки коду або недостатній рівень захисту. Наприклад, вразливості типу SQL-ін'єкції або відсутність належного захисту паролів є популярними точками входу для зловмисників. SQL-ін'єкції можуть дозволяти зловмисникам виконувати несанкціоновані запити до баз даних, що може призвести до крадіжки або модифікації даних.

2. Вразливості у протоколах передачі даних – недоліки в протоколах передачі, наприклад, в SSL/TLS, можуть призводити до перехоплення інформації в процесі передачі між користувачем і сервером.

3. Незахищені API – багато інформаційних систем інтегруються з іншими програмами за допомогою API, але недостатній захист API може відкрити доступ до внутрішніх ресурсів компанії для сторонніх осіб. Наприклад, атаки типу «атака на відкритий API» дозволяють зловмисникам

отримати доступ до критично важливих функцій системи, обійшовши процеси автентифікації.

4. Слабкі паролі та аутентифікаційні механізми – недостатній рівень складності паролів, використання повторних паролів чи відсутність багатофакторної автентифікації може значно полегшити несанкціонований доступ до системи [28].

Технічні вразливості вимагають регулярного моніторингу та оновлення, а також використання інструментів для автоматичного виявлення та усунення недоліків у системі.

Організаційні вразливості пов'язані з людським фактором, політиками безпеки та управлінням персоналом. Цей тип вразливостей обумовлений недостатньою увагою до управління інформаційною безпекою на рівні компанії, а також відсутністю культури кібербезпеки серед співробітників. До організаційних вразливостей відносяться:

1. *Недосконалі політики безпеки* – коли компанія не має чітких інструкцій щодо управління інформаційною безпекою, це може призводити до нерегламентованого доступу до інформації та використання вразливих методів обробки даних.

2. Низька обізнаність співробітників – один із найпоширеніших видів вразливостей, коли персонал компанії не обізнаний щодо основних правил інформаційної безпеки. Фішинг-атаки або соціальна інженерія можуть сприяти розголошенню конфіденційної інформації, коли співробітники не вміють розпізнавати шахрайські дії.

3. *Недостатня підготовка до інцидентів* – відсутність чітких інструкцій на випадок надзвичайних ситуацій може призвести до хаосу і неефективної реакції на кібератаки, що значно посилює можливі наслідки для компанії [29].

Організаційні вразливості можна мінімізувати за допомогою регулярного навчання персоналу, впровадження чітких політик безпеки та проведення тренувань на випадок надзвичайних ситуацій.

Фізичні вразливості пов'язані з фізичним доступом до об’єктів, де зберігається та обробляється інформація, та із захистом обладнання. Фізичні ризики можуть включати:

1. Несанкціонований доступ до приміщень – відсутність належного контролю за доступом до офісів, серверних кімнат або інших приміщень може дозволити зловмисникам фізично проникнути в зону зберігання критичної інформації.

2. Вразливість до природних катастроф – фізичні загрози, як-от пожежі, землетруси чи затоплення, також можуть спричинити втрату або пошкодження обладнання, що зберігає інформацію.

3. Викрадення обладнання – у разі відсутності належного захисту мобільних пристроїв та ноутбуків, що використовуються співробітниками, можливе викрадення обладнання разом із збереженими конфіденційними даними [30].

Для мінімізації фізичних вразливостей необхідно забезпечити захищеність об'єктів, контроль за доступом та резервне копіювання даних у віддалених локаціях.

Операційні вразливості з'являються через недоліки в управлінні та організації процесів, пов'язаних з інформаційною безпекою. Вони включають:

1. Неналежне управління доступом – відсутність контролю за тим, хто має доступ до конкретних даних чи систем, може призводити до несанкціонованого використання ресурсів компанії.

2. Недоліки у процесах моніторингу – відсутність систематичного моніторингу подій безпеки призводить до того, що аномалії залишаються непоміченими, і зловмисники можуть діяти тривалий час без виявлення.

3. Відсутність або недостатність резервного копіювання – якщо компанія не використовує належні методи резервного копіювання, відновлення даних після атак, таких як віруси-вимагачі, стає майже неможливим [31, С. 306].

Операційні вразливості мінімізуються завдяки регулярному аналізу ризиків, постійному моніторингу та оновленню процесів управління безпекою.

Класифікація вразливостей інформаційних систем на технічні, організаційні, фізичні та операційні допомагає виявити слабкі місця, які можуть бути використані зловмисниками, та розробити відповідні захисні заходи. Кожен з типів вразливостей вимагає різних підходів до управління, а чітка класифікація полегшує процес формування цілісної стратегії кібербезпеки на підприємстві.

Розвиток інформаційних технологій створює як нові можливості, так і нові загрози для підприємств. Уразливості інформаційних систем безпосередньо впливають на фінансові результати підприємств, адже будь-який інцидент може спричинити значні економічні втрати. Витрати на відновлення інформаційних систем, втрата даних і репутації, судові витрати та штрафи – усе це супроводжує більшість кібератак і, зазвичай, веде до великих фінансових збитків для компаній.

В економічному контексті класифікація вразливостей дозволяє підприємствам краще оцінювати ризики і планувати заходи з управління та мінімізації втрат. Технічні, організаційні, фізичні та операційні вразливості відрізняються не лише своїми характеристиками, а й економічними наслідками для бізнесу.

Технічні вразливості, зокрема, недоліки в програмному забезпеченні, мають значні економічні наслідки, оскільки вони є найпоширенішою причиною кібератак, що призводять до втрат інформації та прямого фінансового збитку. Економічні аспекти технічних вразливостей включають:

1. *Витрати на відновлення*. Усунення технічних вразливостей, зокрема після інцидентів, потребує залучення спеціалізованих фахівців і додаткових ресурсів. Вартість одного витоку даних, за даними аналітичних звітів, може сягати мільйонів доларів, враховуючи витрати на відновлення, впровадження патчів і оновлень системи [32].

2. *Втрати через зниження продуктивності*. Якщо інформаційна система виходить з ладу внаслідок атаки, підприємство може втратити можливість обслуговувати клієнтів і виконувати свої основні операції, що безпосередньо впливає на прибуток. Наприклад, у банківському секторі тимчасове блокування доступу до системи може призвести до втрати клієнтів та значних витрат на репутаційні кампанії [33].

3. *Підвищення страхових витрат*. Через зростання технічних загроз багато підприємств страхують свої ризики від кібератак. Проте у разі наявності технічних вразливостей страхові премії зростають, що підвищує загальні витрати компанії на забезпечення інформаційної безпеки.

4. *Штрафи за недотримання регулятивних вимог*. У разі порушення норм безпеки, що призводить до витоку конфіденційних даних, компанія може стикатися з великими штрафами відповідно до законодавства. Наприклад, відповідно до положень GDPR, витік персональних даних може обійтися компанії в штраф до 4% від її річного обороту [34].

Організаційні вразливості, пов’язані з управлінням персоналом та політиками інформаційної безпеки, мають значний вплив на довгострокові економічні показники компанії. Основні економічні аспекти таких вразливостей:

1. *Втрати через недосконале управління доступом*. Відсутність чітких правил щодо доступу до інформації призводить до підвищених ризиків інсайдерських атак, які завдають значної шкоди фінансовим показникам підприємства. Інсайдерські атаки є більш витратними для компанії, оскільки для їх виявлення потрібен час і додаткові ресурси [35].

2. *Витрати на навчання персоналу*. Для зменшення організаційних вразливостей необхідно інвестувати в регулярне навчання співробітників. Витрати на підвищення кваліфікації працівників можуть здатися високими, проте вони є важливими для мінімізації загроз з боку соціальної інженерії та шахрайства.

3. *Економічні втрати від шахрайства через фішинг та соціальну інженерію*. Соціальна інженерія, зокрема фішинг, завдає значної шкоди організаціям через витрати на відновлення доступу до систем, відновлення репутації та підвищення безпеки [36]. Багато компаній повідомляють про втрату конфіденційної інформації через фішингові атаки, і кожен такий випадок може коштувати тисячі доларів.

Фізичні вразливості, що пов'язані з фізичним доступом до приміщень і обладнання, також мають свої економічні наслідки:

1. *Витрати на фізичну охорону та доступ*. Інвестиції у фізичну охорону приміщень, системи відеоспостереження та захист доступу до критично важливих об'єктів є необхідними для запобігання несанкціонованому проникненню. Фізичні загрози мають прямий економічний вплив, адже будь-яке порушення може призвести до втрати обладнання чи важливих даних, що вплине на діяльність компанії.

2. *Ризики через природні катастрофи*. Втрати через відсутність захисту від природних катастроф можуть стати критичними для підприємств. Багато компаній інвестують у створення віддалених центрів обробки даних і резервне копіювання, щоб запобігти фінансовим втратам у разі знищення інформації.

Операційні вразливості впливають на ефективність функціонування інформаційної системи підприємства та на можливість швидко реагувати на інциденти:

1. *Відсутність інвестицій у моніторинг.* Відсутність ефективних процесів моніторингу інформаційної безпеки призводить до того, що кібератаки можуть тривати значний час, завдаючи серйозної шкоди бізнесу. Інвестиції у системи моніторингу допомагають підприємствам своєчасно виявляти та усувати загрози, що сприяє зниженню витрат на відновлення.

2. *Витрати на резервне копіювання*. Для мінімізації ризиків компанії витрачають значні кошти на резервне копіювання даних, що дозволяє швидко відновити інформаційні ресурси у разі втрати даних. Хоча ці витрати можуть

здаватися високими, вони є необхідними для збереження безперервності бізнесу та зниження ризиків фінансових втрат.

3. *Штрафи та компенсації через недотримання стандартів*. Підприємства, які не дотримуються стандартів безпеки, можуть стикатися з додатковими витратами через штрафи, судові витрати та компенсації. Це стосується як державних вимог, так і договорів з партнерами чи клієнтами, які передбачають дотримання певного рівня безпеки [37].

Кожен тип вразливості інформаційних систем має унікальний вплив на фінансово-економічні показники підприємства. Порушення у сфері кібербезпеки можуть призвести до значних витрат на усунення наслідків інцидентів, включаючи витрати на відновлення інформації, технічну підтримку, а також оплату послуг зовнішніх експертів. Крім того, у випадку витоку або втрати важливої інформації, підприємство може зіштовхнутися зі значними збитками через втрату конкурентних переваг або навіть недовіру клієнтів.

Вчасна оцінка ризиків і правильна класифікація вразливостей не лише мінімізують ймовірність кіберінцидентів, а й зменшують потенційні витрати на відповідні заходи захисту. Це включає скорочення витрат, пов'язаних із фінансовими штрафами та санкціями за недотримання законодавчих вимог щодо захисту даних і конфіденційності.

Окремий економічний ефект від управління вразливостями також проявляється через підвищення стабільності грошових потоків та оптимізацію витрат на інформаційні технології. Ефективна стратегія кібербезпеки допомагає підприємству знизити ризики непередбачених витрат, які можуть призвести до перебоїв у роботі та необхідності виплат компенсацій клієнтам або партнерам. Надійний кіберзахист сприяє зростанню довіри клієнтів і партнерів, що є важливим фактором для підтримки стабільного рівня доходів і збільшення частки ринку в довгостроковій перспективі.

Таким чином, інвестиції в кібербезпеку є важливою складовою не лише захисту інформації, але й забезпечення стійкого економічного розвитку

підприємства, збереження його репутації та підвищення конкурентоспроможності.

2.3. Економічні наслідки інформаційних загроз

У сучасних умовах господарювання українські підприємства активно інтегрують інформаційні технології у свою діяльність, що дозволяє їм не лише оптимізувати бізнес-процеси, але й значно підвищувати ефективність управлінських рішень. Впровадження сучасних інформаційних систем, таких як ERP (Enterprise Resource Planning), CRM (Customer Relationship Management) та інших програмних рішень, забезпечує автоматизацію рутинних завдань, що дає змогу зосередитися на стратегічних аспектах розвитку бізнесу. Це дозволяє підприємствам покращувати комунікацію між підрозділами, скорочувати витрати на обробку інформації, підвищувати якість обслуговування клієнтів і, в результаті, підвищувати свою конкурентоспроможність на ринку.

Проте така залежність від інформаційних технологій і систем породжує численні загрози, які можуть негативно впливати на функціонування підприємств. Зокрема, підприємства стикаються з ризиками кібератак, які можуть бути спрямовані на порушення цілісності, доступності або конфіденційності даних. Кібератаки можуть мати різну природу: від простих вірусних атак до складних злочинних схем, що використовують методи соціальної інженерії. Такі загрози вимагають від підприємств постійної уваги до питання інформаційної безпеки та значних інвестицій у засоби захисту інформації.

Крім того, існує ризик несанкціонованого доступу до конфіденційних даних, що може призвести до витоку інформації, порушення прав на інтелектуальну власність або викрадення особистих даних клієнтів. Це не лише підриває довіру споживачів до компанії, але й може спричинити серйозні юридичні наслідки. Наприклад, відповідно до Закону України «Про захист персональних даних», підприємства зобов’язані забезпечувати належний

рівень захисту особистої інформації своїх клієнтів, і порушення цих вимог може призвести до значних штрафів.

Загрози інформаційній безпеці, що виникають внаслідок залежності від інформаційних систем, не лише порушують стабільне функціонування підприємств, але й можуть призвести до суттєвих економічних втрат. Такі втрати можуть включати безпосередні фінансові збитки, пов’язані з ліквідацією наслідків атак, витратами на відновлення систем, а також втрату доходів через зниження продуктивності праці. Наприклад, внаслідок кібератаки підприємство може зазнати зупинки виробничих процесів, що призведе до втрати обсягів продажів та зниження ринкових позицій [38, С. 60].

Важливо також зазначити, що інформаційні загрози можуть негативно вплинути на репутацію компанії. У світі, де інформація швидко поширюється через соціальні мережі та новинні платформи, новини про кібератаки або витоки даних можуть швидко завдати шкоди іміджу підприємства. Це, в свою чергу, може призвести до зниження довіри споживачів та відтоку клієнтів, що вкрай негативно позначиться на фінансових результатах.

Отже, сучасні підприємства мають усвідомлювати, що з розвитком інформаційних технологій виникає новий рівень ризиків, і для їхньої ефективної роботи необхідно розробляти та впроваджувати стратегії управління інформаційною безпекою. Це не лише дозволить захистити цінні дані та інформаційні ресурси, а й забезпечить стабільне та успішне функціонування підприємств в умовах постійно зростаючих загроз.

Основні економічні наслідки інформаційних загроз:

1. Прямі фінансові втрати. Інформаційні загрози здатні призвести до значних фінансових втрат підприємств, які виникають у зв'язку з необхідністю ліквідації наслідків інцидентів, відновлення роботи інформаційних систем і компенсації втрат доходів, пов’язаних із простоєм. Як приклад, можна розглянути ситуацію з ПриватБанком, що став об’єктом кібератаки у 2022 році, коли його інформаційні системи були частково заблоковані, що викликало ускладнення з наданням послуг клієнтам. В результаті інциденту

ПриватБанк змушений був інвестувати значні ресурси для відновлення стабільності операційної діяльності, включаючи оплату послуг кіберфахівців, детальний аналіз причин інциденту та оновлення системи безпеки [39].

Інший масштабний приклад – атака вірусу NotPetya у 2017 році, яка вразила численні підприємства України, включаючи Національну акціонерну компанію «Нафтогаз України». Під час цієї атаки було заблоковано доступ до ключових систем, через що компанія зазнала значних витрат, спрямованих як на подолання наслідків, так і на забезпечення безпеки для запобігання подібним ситуаціям у майбутньому. Це відобразилось на фінансових показниках, оскільки сукупні витрати на реагування включали не лише компенсацію безпосередніх втрат, але й витрати на довготривалі заходи кібербезпеки [40].

2. Втрати продуктивності. Інформаційні загрози також можуть мати значний негативний вплив на продуктивність праці підприємства. Це особливо характерно для випадків, коли кібератака або збій в інформаційній системі перешкоджають ефективній роботі окремих підрозділів, блокують доступ до важливих даних або навіть зупиняють виробничі процеси. Показовим прикладом у цьому контексті є випадок з компанією «Прикарпаттяобленерго», яка зазнала кібератаки у 2015 році. Внаслідок цього інциденту тимчасово було зупинено електропостачання на окремих ділянках мережі, що завдало не лише економічних втрат, але й спричинило значні репутаційні збитки для компанії [41].

Зниження продуктивності в результаті інформаційних інцидентів потребує додаткових витрат на відновлення нормальної діяльності, залучення кваліфікованих фахівців, а також проведення навчальних програм для співробітників з метою попередження аналогічних ситуацій у майбутньому. Подібні заходи підвищують загальні витрати підприємства, що вимагає детального врахування економічних наслідків і відповідного фінансування для попередження таких інцидентів.

3. Репутаційні втрати. Економічні наслідки інформаційних загроз включають також і репутаційні втрати, які, хоча і є непрямими, однак здатні суттєво знизити ринкові позиції підприємства. Підприємства, які зазнали витоку конфіденційних даних або іншого інформаційного інциденту, можуть втратити довіру клієнтів та партнерів, що спричинить зниження обсягу продажів та відтік клієнтів до конкурентів. Наприклад, у 2018 році один з відомих українських ритейлерів зазнав значних репутаційних збитків через витік даних про клієнтські транзакції. Це призвело до зниження рівня лояльності клієнтів та зростання негативної репутації у медіапросторі [42].

Репутаційні втрати викликають значні економічні наслідки, адже для повернення довіри споживачів підприємства змушені виділяти додаткові кошти на відновлення бренду. Це може включати витрати на маркетингові кампанії, посилення заходів кібербезпеки та введення спеціальних акцій для лояльних клієнтів. Такий вплив може бути тривалим, оскільки навіть після вжиття заходів з кібербезпеки і маркетингу відновлення довіри потребує часу.

4. Витрати на забезпечення інформаційної безпеки. Для запобігання можливим економічним наслідкам, пов'язаним з інформаційними загрозами, українські підприємства інвестують значні кошти в удосконалення систем інформаційної безпеки. Наприклад, НАК «Нафтогаз України» значно збільшила обсяги фінансування кібербезпеки після атак, спрямованих на українські компанії. Інвестиції в сучасні системи захисту включають оновлення технологій для моніторингу загроз, резервне копіювання даних, навчання персоналу та впровадження інноваційних рішень для мінімізації ризиків кібератак.

Інші українські підприємства, зокрема аграрні компанії на кшталт «Миронівський хлібопродукт» (МХП), також активно інвестують у системи кіберзахисту, оскільки їх діяльність пов’язана з обробкою та збереженням великих обсягів даних, а також залежить від надійності ланцюгів поставок. Таким чином, для підприємств МХП інвестиції в безпеку є критичними для підтримання стабільної діяльності та забезпечення належного рівня захисту

інформаційних активів. Витрати на заходи кібербезпеки включають закупівлю спеціалізованого обладнання, підтримку резервних систем, регулярний аудит безпеки, що допомагає запобігати потенційним економічним втратам [43].

Таким чином, аналіз економічних наслідків інформаційних загроз на прикладі українських підприємств демонструє, що кібератаки, витоки даних і збої в інформаційних системах здатні мати як прямий, так і опосередкований економічний вплив на бізнес. Прямі втрати, пов’язані з інформаційними інцидентами, зазвичай виявляються у вигляді значних витрат на ліквідацію наслідків атак. До цих витрат належать витрати на відновлення пошкоджених систем, відновлення даних, а також фінансові компенсації за простої, які можуть тривати від кількох днів до кількох тижнів. Наприклад, випадки кібератак на українські банки в останні роки підтверджують, що витрати на відновлення нормального функціонування можуть сягати мільйонів гривень, що суттєво впливає на фінансові результати підприємств.

Опосередковані економічні наслідки інформаційних загроз, які охоплюють зниження продуктивності, репутаційні витрати та інвестиції в кібербезпеку, також відіграють важливу роль у формуванні загальних витрат для підприємства. Зниження продуктивності, яке може виникнути внаслідок кібератак, часто пов’язане із затримками у виконанні ключових бізнес-процесів, що призводить до зменшення обсягів виробництва та зниження доходів. Вплив на продуктивність може бути особливо відчутним для підприємств, які працюють у сфері виробництва або послуг, де швидкість реагування і безперервність процесів є критично важливими.

Репутаційні втрати, що виникають у результаті кібератак, можуть мати тривалі економічні наслідки. Втрата довіри клієнтів і партнерів може призвести до зниження обсягів продажів, що негативно вплине на фінансові показники компанії. За оцінками експертів, відновлення іміджу компанії після інформаційного інциденту може вимагати значних фінансових і ресурсних вкладень, що в результаті може скласти 20-30% від загальних витрат на ліквідацію наслідків.

В умовах постійного зростання загроз інформаційних інцидентів, українські підприємства змушені формувати та впроваджувати ефективні стратегії захисту інформації, які є важливим елементом для забезпечення економічної стійкості та конкурентоспроможності. Інвестиції в кібербезпеку стають не просто необхідними витратами, а стратегічним вкладенням у майбутнє бізнесу. Системи кіберзахисту, що включають як технологічні, так і організаційні рішення, допомагають підприємствам зменшити ризики і вартість потенційних збитків від інформаційних загроз.

Створення внутрішніх підрозділів з інформаційної безпеки і залучення зовнішніх консультантів з кібербезпеки є ефективними заходами для підвищення рівня захисту підприємств. Це дозволяє не лише захистити цінні дані, але й зберегти стабільність бізнес-процесів у разі загрози. Такі інвестиції, як показує практика, можуть окупитися у разі уникнення серйозних кібератак або їх наслідків.

Отже, для українських підприємств інформаційна безпека повинна стати невід’ємною частиною бізнес-стратегії. Системний підхід до управління ризиками, пов’язаними з інформаційними загрозами, є ключовим для забезпечення економічної стійкості, здатності реагувати на виклики ринку і підтримки конкурентоспроможності в умовах швидко змінюваного бізнес-середовища.

РОЗДІЛ 3. СТРАТЕГІЇ ТА МЕТОДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1. Стратегії управління інформаційними ризиками

У сучасних умовах глобалізації та інформатизації економіки інформація стає одним із найважливіших ресурсів, що визначає конкурентоспроможність та ефективність підприємств. Особливо це актуально для українських підприємств, які прагнуть впроваджувати інноваційні рішення та адаптуватися до змінюваного ринкового середовища. В умовах безперервного розвитку інформаційних технологій і збільшення обсягів оброблюваної інформації, ефективне управління інформаційними ризиками перетворюється на критично важливе завдання, оскільки невірно оцінені або ігноровані ризики можуть призвести до суттєвих фінансових втрат, репутаційних збитків і навіть до втрати конкурентоспроможності на ринку.

Управління інформаційними ризиками охоплює комплекс процесів і методів, які націлені на виявлення, оцінку та мінімізацію ризиків, що виникають у зв'язку з використанням інформаційних активів. До інформаційних активів відносять усі види інформації, включаючи дані, які зберігаються в електронному вигляді, бази даних, програмне забезпечення, а також інші ресурси, пов'язані з обробкою і зберіганням інформації. Ризики, пов'язані з цими активами, можуть виникати як у результаті зовнішніх загроз (наприклад, кібератак, витоків даних), так і внутрішніх факторів (недостатня кваліфікація співробітників, відсутність належних політик безпеки) [44].

Ефективні стратегії управління ризиками передбачають не лише запобігання втратам, але й створення умов для адаптації підприємства до можливих загроз. Вони дозволяють забезпечити стійкість організації в умовах непередбачених обставин, таких як інформаційні інциденти, які можуть включати в себе збої в роботі інформаційних систем, витоки конфіденційних даних або кібератаки. Підприємства, які впроваджують системи управління

інформаційними ризиками, здатні швидше відновлюватися після інцидентів та зберігати довіру клієнтів і партнерів.

Окрім того, управління інформаційними ризиками дозволяє не лише знизити ймовірність реалізації загроз, але й підвищити загальний рівень безпеки інформаційних систем. Важливими аспектами цього процесу є ідентифікація потенційних загроз, оцінка ймовірності їх виникнення, а також впровадження заходів щодо їх нейтралізації [45]. Таким чином, стратегії управління інформаційними ризиками стають необхідним інструментом для забезпечення стабільності та розвитку українських підприємств в умовах динамічного та часто непередбачуваного бізнес-середовища.

Першим етапом у формуванні ефективної стратегії управління інформаційними ризиками є їх *ідентифікація*, яка являє собою систематичний процес, спрямований на виявлення потенційних загроз, що можуть негативно вплинути на інформаційні активи підприємства. В умовах стрімкого розвитку інформаційних технологій та зростання залежності бізнесу від інформаційних систем, правильна ідентифікація ризиків стає вирішальним фактором для збереження стабільності та конкурентоспроможності підприємства. Ідентифікація ризиків передбачає не лише визначення їх наявності, а й оцінку можливих наслідків, що можуть виникнути внаслідок реалізації цих ризиків [46].

Інформаційні ризики можуть мати різноманітний характер, починаючи від технічних збоїв, які є наслідком системних помилок або апаратних дефектів, і закінчуючи навмисними кібератаками, що здійснюються з метою отримання несанкціонованого доступу до конфіденційної інформації. Важливо відзначити, що ризики в інформаційній сфері поділяються на зовнішні та внутрішні, що суттєво впливає на методи їх ідентифікації та управління.

Зовнішні ризики є переважно ризиками, що виникають внаслідок дій третіх осіб. До них належать:

1. *Кібератаки*. Це одна з найсерйозніших загроз у сучасному бізнес-середовищі. Кібератаки можуть мати різні форми, включаючи:

Атаки типу "відмова в обслуговуванні" (DDoS) спрямовані на перевантаження серверів підприємства, що призводить до тимчасового зупинення роботи системи і, відповідно, до фінансових втрат.

Фішинг передбачає використання обманних електронних листів або веб-сайтів для збору конфіденційної інформації, такої як логіни і паролі. Фішинг стає дедалі витонченішим, що ускладнює його виявлення.

Шкідливе програмне забезпечення (ransomware) блокує доступ до даних підприємства до моменту сплати викупу. За даними досліджень, витрати на відновлення після атаки програм-вимагачів можуть сягати мільйонів доларів.

2. *Витоки даних*. Несанкціонований доступ до інформаційних систем може статися внаслідок атак, які експлуатують вразливості програмного забезпечення або через внутрішні помилки в управлінні доступом. Наприклад, нещодавні випадки витоків даних у великих компаніях, які призвели до публікації особистих даних мільйонів користувачів, підкреслюють серйозність цієї загрози. Витоки даних можуть призвести до значних фінансових втрат, а також до серйозних репутаційних збитків.

3. *Природні катастрофи*. Такі події, як повені, землетруси або інші стихійні лиха, можуть знищити фізичні ресурси підприємства, включаючи сервери та системи зберігання даних. Витрати на відновлення після природних катастроф можуть бути колосальними, і підприємства повинні розробляти плани на випадок надзвичайних ситуацій, щоб мінімізувати наслідки таких інцидентів [47, С. 47-48].

Внутрішні ризики виникають всередині організації і можуть бути пов'язані з:

1. *Людським фактором*. Це один з найбільш вразливих аспектів інформаційної безпеки. Людські помилки, допущені співробітниками внаслідок недосвідченості або недбальства, можуть суттєво підвищити рівень ризику. Наприклад, ненавмисне надсилання конфіденційних документів на

неправильну електронну адресу або порушення правил доступу можуть стати причинами серйозних витоків інформації. Крім того, відсутність належного навчання з питань кібербезпеки може призвести до того, що співробітники не усвідомлюють важливість захисту інформаційних активів.

2. *Відсутністю або неналежною політикою безпеки*. Організації, які не мають чітко визначених політик безпеки або не дотримуються їх, створюють ризики для своїх інформаційних систем. Відсутність документованих процедур щодо обробки та зберігання конфіденційних даних, а також належного контролю доступу до інформації, може призвести до небажаних наслідків.

3. *Технічними збоями в інформаційних системах*. Технічні неполадки в апаратному чи програмному забезпеченні можуть призвести до втрати даних або зупинки операційних процесів, що негативно вплине на загальну продуктивність підприємства. Наприклад, несправність сервера або збій у програмному забезпеченні може призвести до тривалого простою, що, у свою чергу, матиме фінансові наслідки [48].

Таким чином, усвідомлення різноманітності інформаційних ризиків та їх ідентифікація є критично важливими для формування ефективної стратегії управління ризиками. Процес ідентифікації ризиків передбачає активну участь всіх структурних підрозділів підприємства та постійний моніторинг змін у зовнішньому та внутрішньому середовищі. Оскільки інформаційні технології та загрози, пов’язані з ними, постійно еволюціонують, підприємствам необхідно регулярно оновлювати свої підходи до управління ризиками. Адекватна ідентифікація ризиків дозволяє підприємствам розробити профілактичні заходи та стратегії реагування, що сприяють зниженню вразливості перед загрозами та підвищують загальний рівень інформаційної безпеки організації.

Після ідентифікації ризиків наступним важливим етапом у процесі управління інформаційними ризиками є їх *оцінка*. Оцінка ризиків є критично важливою процедурою, оскільки вона дозволяє підприємству зрозуміти, які

загрози можуть мати найбільший негативний вплив на його діяльність, а також оцінити можливі наслідки, які можуть виникнути у разі реалізації цих загроз [49, С. 63]. Це особливо актуально в сучасному світі, де інформаційні технології стали основою для більшості бізнес-процесів, а отже, ризики, пов'язані з ними, можуть призвести до значних фінансових та репутаційних втрат.

Оцінка ризиків допомагає підприємствам не лише виявити найбільш критичні загрози, але й розробити ефективні стратегії управління. Вона дозволяє підприємству:

1. *Визначити пріоритети*. Оцінка ризиків допомагає ідентифікувати ті загрози, які потребують термінового вирішення. Наприклад, якщо підприємство виявило ризик, пов'язаний із збоєм у системі, що може призвести до значних фінансових втрат, йому потрібно першочергово вжити заходів для усунення цього ризику.

2. *Управляти ресурсами*. Визначивши пріоритети ризиків, підприємства можуть ефективно розподілити свої ресурси. Це дозволяє уникнути витрат на управління менш значними ризиками та зосередитися на тих, які мають найбільший вплив на бізнес.

3. *Підвищити обізнаність*. Процес оцінки ризиків підвищує обізнаність співробітників про загрози, що існують у сфері інформаційної безпеки. Це важливо, оскільки людський фактор часто є одним із найбільших ризиків у кібербезпеці [50].

Для оцінки ризиків використовуються різні методи, кожен з яких має свої переваги і недоліки. Два основні підходи до оцінки ризиків – це квантитативний і якісний.

Квантитативний метод оцінки ризиків ґрунтується на використанні числових показників, що дозволяє кількісно визначити рівень ризику. Цей метод може бути реалізований через кілька основних етапів:

1. *Визначення ймовірності ризику*. На цьому етапі необхідно оцінити ймовірність реалізації ризику. Це може бути виконано через статистичні дані,

історичні аналізи або за допомогою моделей, що прогнозують можливі наслідки. Наприклад, якщо підприємство проводить регулярний моніторинг своїх систем і виявляє, що кібератаки відбуваються в середньому один раз на рік, це може бути використано для визначення ймовірності реалізації ризику.

2. *Оцінка фінансових втрат*. Наступним кроком є оцінка можливих фінансових втрат у разі реалізації ризику. Це може включати витрати на відновлення даних, відшкодування шкоди клієнтам або втрати від простою. Наприклад, якщо атака призведе до зупинки виробництва, підприємство може втратити значну частину доходу за цей час.

3. *Розрахунок рівня ризику*. На основі визначеної ймовірності та оцінки фінансових втрат підприємство може розрахувати загальний рівень ризику, використовуючи формулу: Ризик = Ймовірність × Втрата. Цей розрахунок дозволяє отримати чітке уявлення про потенційний вплив ризику на бізнес [51, С. 11-112].

Якісний метод оцінки ризиків базується на експертних оцінках і розподілі ризиків за категоріями, такими як високий, середній або низький. Це дозволяє підприємству отримати більш детальну картину ризиків, особливо в тих випадках, коли недостатньо даних для проведення кількісного аналізу.

1. *Експертні оцінки*. У цьому процесі залучаються фахівці, які добре знають специфіку підприємства та галузі. Вони можуть оцінити ризики на основі свого досвіду та знань. Наприклад, команда з кібербезпеки може надати думку про ймовірність реалізації конкретного ризику на основі аналізу попередніх інцидентів.

2. *SWOT-аналіз*. Використання SWOT-аналізу (сильні та слабкі сторони, можливості та загрози) дозволяє оцінити не лише ризики, а й потенційні можливості, які можуть з’явитися внаслідок змін у зовнішньому середовищі. Це допомагає підприємству зрозуміти, як найкраще використовувати свої ресурси для протидії загрозам [52].

Оцінка ризиків дозволяє підприємствам визначити пріоритети для подальшого управління ризиками. Наприклад, після проведення оцінки

підприємство може виявити, що певні ризики, які раніше не були визнані серйозними, насправді мають високу ймовірність реалізації та значні наслідки. У такому випадку, підприємство повинно зосередити свої зусилля на розробці заходів для зниження цих ризиків.

Таким чином, етап оцінки ризиків є критично важливим для прийняття зважених рішень щодо розподілу ресурсів, розробки планів реагування на інциденти та забезпечення загальної безпеки інформаційних активів підприємства. Це дозволяє не лише захистити бізнес від можливих загроз, але й підвищити його стійкість і конкурентоспроможність на ринку. В умовах постійно змінюваного інформаційного середовища, регулярна оцінка ризиків стає не лише необхідною, а й обов'язковою складовою успішної стратегії управління інформаційною безпекою підприємства.

Стратегії управління інформаційними ризиками відіграють вирішальну роль у забезпеченні інформаційної безпеки підприємств. Ці стратегії мають на меті не лише виявлення та оцінку ризиків, але й формулювання конкретних дій для їх мінімізації або управління ними. Ключові елементи цих стратегій можуть бути класифіковані на декілька категорій, зокрема: уникнення ризиків, зниження ризиків, прийняття ризиків та передачу ризиків [53].

1. Уникнення ризиків. Уникнення ризиків є однією з найбільш проактивних стратегій управління, що полягає у внесенні змін у бізнес-процеси або технологічні рішення для усунення або значного зменшення ймовірності виникнення ризику. В основі цієї стратегії лежить принцип, що запобігання ризикам є більш ефективним та економічним, ніж їх подальше усунення [54].

Приклад: Підприємство може ухвалити рішення про відмову від використання застарілих або небезпечних технологій, які мають високий ризик збою або кібератаки. Наприклад, компанія, яка займається фінансовими послугами, може відмовитися від застосування застарілих систем управління даними, які мають відомі вразливості, замінивши їх на сучасні, безпечніші рішення, що забезпечують відповідність сучасним стандартам безпеки.

2. Зниження ризиків. Зниження ризиків включає в себе впровадження додаткових заходів безпеки, які спрямовані на зменшення ймовірності реалізації ризику або пом'якшення наслідків, що можуть виникнути внаслідок його реалізації. Ця стратегія передбачає активну участь усіх працівників підприємства, оскільки людський фактор є одним із основних джерел ризиків у сфері інформаційної безпеки [55].

Приклад: Запровадження регулярних навчань для співробітників щодо основ кібербезпеки може суттєво знизити ризики, пов'язані з недбалістю або необізнаністю персоналу. Наприклад, навчання на теми фішингу та інших видів атак може допомогти співробітникам розпізнавати загрози, що в свою чергу зменшує ймовірність випадкового відкриття шкідливих посилань або вкладень.

3. Прийняття ризиків. Прийняття ризиків є стратегією, що базується на принципі, що в деяких випадках витрати на управління ризиками можуть перевищувати можливі втрати у разі їх реалізації. Ця стратегія може бути доречною, якщо підприємство має обмежені ресурси або якщо ризики вважаються прийнятними в контексті бізнес-моделі [56].

Приклад: Якщо підприємство оцінює, що ризик кібератаки з ймовірністю 5% призведе до збитків у розмірі 50 000 гривень, а витрати на впровадження заходів безпеки для зменшення цього ризику становитимуть 70 000 гривень, компанія може ухвалити рішення про прийняття цього ризику. Проте навіть у такому випадку підприємство повинно мати чітко розроблені плани дій на випадок реалізації ризику, які можуть включати процедури реагування на інциденти та заходи з відновлення після атаки.

4. Передача ризиків. Передача ризиків передбачає перекладання частини відповідальності за ризики на третіх осіб. Ця стратегія може бути реалізована через страхування або аутсорсинг послуг, що дозволяє підприємствам зменшити вплив ризиків на свою діяльність [57].

Приклад: Підприємство може укласти контракт з постачальником послуг кібербезпеки, який візьме на себе відповідальність за захист

інформаційних активів. Таке рішення може включати в себе впровадження зовнішнього моніторингу безпеки, реагування на інциденти та управління ризиками. Крім того, підприємство може оформити страхування кіберризиків, що дозволить зменшити фінансові наслідки у випадку кібератаки або витоку даних.

Отже, управління інформаційними ризиками є складним і багатогранним процесом, який вимагає комплексного підходу. Стратегії, такі як уникнення, зниження, прийняття та передача ризиків, забезпечують підприємствам гнучкість у реагуванні на загрози, що виникають у динамічному інформаційному середовищі. Впровадження цих стратегій не лише підвищує рівень інформаційної безпеки, а й сприяє загальному успіху підприємства на ринку.

Сучасні інформаційні технології відіграють критично важливу роль у формуванні стратегій управління інформаційними ризиками, оскільки забезпечують підприємствам засоби для ефективного захисту своїх інформаційних активів. У контексті зростаючих загроз, пов’язаних із кіберінцидентами, інформаційні технології стають не лише інструментами, а й невід’ємною частиною комплексного підходу до управління ризиками.

Сучасні інформаційні технології є невід’ємною частиною стратегії управління інформаційними ризиками для підприємств. Використання спеціалізованого програмного забезпечення, технологій шифрування даних та управління доступом забезпечує багатошаровий захист інформаційних активів і дозволяє підприємствам протистояти зростаючим загрозам. Зважаючи на динамічність інформаційних ризиків, підприємства повинні постійно вдосконалювати свої технології та підходи, щоб зберігати конкурентоспроможність і забезпечити стійкість перед кіберзагрозами.

Таким чином, етап оцінки ризиків має критичне значення в управлінні інформаційною безпекою підприємств, оскільки він створює основу для прийняття зважених рішень щодо розподілу ресурсів, формування планів реагування на інциденти та забезпечення загальної економічної безпеки

інформаційних активів. Ефективна оцінка ризиків дозволяє підприємствам не тільки захистити свої фінансові інтереси від потенційних загроз, але й підвищити їх стійкість та конкурентоспроможність на ринку.

В умовах швидко змінюваного інформаційного середовища, підприємства стикаються з безліччю нових загроз, які можуть суттєво вплинути на їх економічні результати. Наприклад, кібератаки можуть призвести до значних фінансових втрат через витрати на ліквідацію наслідків, а також через втрату репутації, що може знизити довіру з боку клієнтів і партнерів. Оцінка ризиків дозволяє ідентифікувати найбільш небезпечні загрози, що впливають на фінансові показники підприємства, і розробити стратегії для їх нейтралізації.

Регулярна оцінка ризиків стає необхідною складовою успішної економічної стратегії управління інформаційною безпекою. Це не лише забезпечує захист бізнесу від потенційних загроз, але й підвищує його стійкість на ринку, що в свою чергу, може призвести до зростання економічної ефективності. Наприклад, підприємства, які активно інвестують у системи інформаційної безпеки, мають змогу зберігати та примножувати свої активи, зменшуючи ймовірність фінансових втрат.

Належна оцінка ризиків може служити економічним інструментом для зміцнення позицій підприємства на ринку, адже вона забезпечує впевненість у здатності компанії протистояти кібератакам та іншим інформаційним інцидентам. Це, в свою чергу, веде до підвищення довіри з боку клієнтів і партнерів, що є важливим фактором для досягнення стабільного економічного зростання та успішного розвитку підприємства в умовах сучасної конкуренції.

3.2. Інструменти забезпечення інформаційної безпеки

Інформаційна безпека в умовах сучасного економічного середовища виступає важливим фактором, що гарантує стабільність і стійкість функціонування підприємства в умовах швидко змінюваного технологічного ландшафту. У зв'язку з різким збільшенням обсягів даних, що обробляються,

зберігаються та передаються підприємствами, зростає також кількість і різноманіття загроз, які можуть негативно впливати на ефективність і безперервність діяльності компанії. У цьому контексті інформаційна безпека не обмежується лише захистом конфіденційних даних, а охоплює комплексний підхід до збереження цілісності та стабільності інформаційних систем, які забезпечують безперебійну роботу бізнес-процесів.

Інформаційна безпека, як складова частина загальної стратегії управління підприємством, спрямована на збереження основних принципів управління інформацією, зокрема забезпечення її конфіденційності, цілісності та доступності. Одним з найважливіших аспектів є те, що інформаційна безпека не лише фокусується на захисті окремих елементів інформаційної інфраструктури, а й на створенні інтегрованої системи безпеки, яка дозволяє підприємству не лише убезпечити свої дані, але й оперативно реагувати на виникаючі загрози.

Для досягнення належного рівня інформаційної безпеки на підприємстві необхідно впроваджувати комплекс різноманітних інструментів і методів, що включають технічні, правові та організаційні засоби. Ці інструменти допомагають забезпечити високий рівень захисту інформаційних активів підприємства, знижуючи ризики, пов'язані з їх можливим витоком або пошкодженням [59]. Одночасно, важливою складовою є впровадження механізмів, які дозволяють своєчасно виявляти та нейтралізувати потенційні загрози, зменшуючи можливі економічні та репутаційні втрати.

Основними цілями інформаційної безпеки в умовах підприємства є:

забезпечення конфіденційності даних – запобігання несанкціонованому доступу до інформації, що є конфіденційною або важливою для бізнесу. Це включає як технологічні засоби захисту даних, так і організаційні методи контролю доступу.

підтримка цілісності та доступності інформаційних ресурсів – забезпечення того, щоб інформація залишалася точною, повною та актуальною протягом усього процесу її обробки, а також гарантування її

доступності в необхідний час для уповноважених осіб. Це означає захист від змін, які можуть бути здійснені зловмисно або випадково.

захист від внутрішніх та зовнішніх загроз – усунення ризиків, які можуть виникнути як ззовні (наприклад, через кібернапади або хакерські атаки), так і зсередини підприємства (наприклад, через недобросовісних співробітників або технічні помилки) [60, С. 136-138].

Таким чином, ефективна система забезпечення інформаційної безпеки підприємства повинна бути побудована на основі комплексного підходу, що включає інтеграцію різноманітних інструментів і стратегій для досягнення основних цілей безпеки інформаційних ресурсів. Це дозволяє не лише знижувати рівень ризиків, але й забезпечувати безперервність та стабільність діяльності підприємства на довгострокову перспективу.

Розглянемо інструменти інформаційної безпеки, які поділяються на кілька ключових категорій, кожна з яких відіграє важливу роль у загальній безпековій стратегії підприємства.

Інструменти забезпечення інформаційної безпеки можна умовно поділити на чотири основні категорії:

1. *Технічні інструменти* – це спеціальні засоби, які використовуються для захисту інформаційних систем від несанкціонованого доступу, кіберзагроз та технічних збоїв. До них належать брандмауери, системи захисту від шкідливого програмного забезпечення, засоби моніторингу мережевого трафіку, а також резервне копіювання даних.

2. *Організаційні інструменти* – це комплекс заходів, спрямованих на підвищення рівня інформаційної безпеки через створення певних політик, протоколів і процедур, що регулюють порядок використання інформаційних ресурсів підприємства. Вони включають розробку політик безпеки, навчання персоналу, а також регулярні аудити інформаційної безпеки.

3. *Програмні інструменти* – різноманітне програмне забезпечення для забезпечення цілісності та конфіденційності даних, захисту від несанкціонованого доступу, а також аутентифікації та ідентифікації

користувачів. До них відносяться системи шифрування, програми контролю доступу та системи двофакторної аутентифікації.

4. *Правові інструменти* – регуляторні заходи, що охоплюють дотримання законодавчих вимог у сфері інформаційної безпеки. Вони спрямовані на забезпечення відповідності політик підприємства національним та міжнародним стандартам захисту інформації [61].

Кожна з цих категорій охоплює важливі інструменти для забезпечення захисту даних, і для досягнення максимальної ефективності їх потрібно інтегрувати в загальну систему управління інформаційною безпекою на підприємстві.

Технічні інструменти є однією з основних складових системи забезпечення інформаційної безпеки, що прямо впливає на економічну стабільність підприємства. Їх використання зменшує ризики фінансових втрат, пов'язаних із витоками даних, кібератаками, порушенням бізнес-процесів і втратами клієнтів. Далі розглянемо основні інструменти та їхній економічний ефект для підприємства.

1. *Брандмауери*. Використання брандмауерів допомагає уникнути значних витрат, пов'язаних з витоками інформації та зломом корпоративних мереж. Захист від несанкціонованого доступу дозволяє знизити ймовірність кібератак, які можуть зупинити бізнес-процеси або призвести до втрати даних клієнтів. Таким чином, інвестиції в брандмауери допомагають запобігти фінансовим втратам і зберегти довіру клієнтів, що особливо важливо для підприємств, які працюють у фінансовому або банківському секторі.

2. *Системи захисту від шкідливого програмного забезпечення (антивірусні програми)*. Антивірусні програми забезпечують безпеку систем підприємства, що знижує ймовірність простоїв і, відповідно, втрат доходів через порушення роботи. Фінансові втрати внаслідок атак шкідливого програмного забезпечення можуть бути суттєвими, зокрема через втрату продуктивності, відшкодування шкоди та репутаційні втрати. Таким чином,

інвестиції в антивірусний захист швидко окупаються за рахунок зменшення потенційних збитків.

3. *Інструменти шифрування*. Вартість розробки і впровадження технологій шифрування значно менша, ніж можливі витрати, пов’язані з витоком конфіденційних даних. У випадку несанкціонованого доступу зашифровані дані залишаються недоступними для зловмисників, що мінімізує економічні ризики та втрати від компрометації критичної інформації. Особливо важливим цей аспект є для підприємств, що працюють з банківською інформацією або персональними даними клієнтів, де порушення конфіденційності може призвести до значних штрафів і репутаційних втрат.

4. *Системи управління доступом*. Контроль доступу на основі ролей знижує ризики, пов'язані з витоком даних через внутрішні загрози або випадкові помилки співробітників. Чіткий розподіл повноважень знижує вразливість системи та дозволяє мінімізувати внутрішні загрози. З економічної точки зору, це дозволяє зменшити витрати на усунення наслідків інцидентів і підвищити ефективність роботи команди, оскільки всі співробітники отримують доступ лише до тієї інформації, яка їм потрібна для виконання конкретних обов'язків.

5. *Системи резервного копіювання даних***.** Втрати даних через технічні збої можуть коштувати компанії мільйони доларів, особливо якщо йдеться про важливу інформацію, пов’язану з виробничими процесами або клієнтськими контрактами. Резервне копіювання допомагає уникнути витрат на відновлення інформації або на оплату штрафів за невиконання зобов'язань перед клієнтами. Регулярне створення копій даних забезпечує безперервність бізнес-процесів і підтримує надійність компанії в очах партнерів та інвесторів, що має стратегічне значення для стабільного розвитку бізнесу.

6. *Системи моніторингу та аналізу мережевого трафіку*. Моніторинг трафіку дозволяє оперативно виявляти та попереджати загрози, що мінімізує витрати на реагування в разі інциденту. Це забезпечує можливість економічно ефективного управління ризиками, оскільки раннє

виявлення потенційних атак допомагає уникнути масштабних збитків. Виявлення аномалій на ранніх стадіях дозволяє вчасно блокувати загрози, захищаючи як матеріальні, так і нематеріальні активи підприємства [62, С. 233-234].

Загалом, технічні інструменти інформаційної безпеки мають значний економічний вплив на діяльність підприємства. Інвестиції в інформаційну безпеку дозволяють уникнути потенційних витрат, пов'язаних з інцидентами безпеки, і забезпечують довгострокову стабільність бізнесу. Надійний захист даних, як і репутаційна вигода від дотримання високих стандартів інформаційної безпеки, стають вагомою конкурентною перевагою.

Витрати на впровадження технічних інструментів інформаційної безпеки є виправданими, оскільки вони створюють передумови для економічної безпеки компанії. Зокрема, зниження витрат, пов'язаних з реагуванням на інциденти, підтримка довіри клієнтів та партнерів, а також мінімізація штрафів і компенсаційних виплат сприяють підвищенню економічної ефективності підприємства.

Організаційні інструменти є важливим компонентом системи інформаційної безпеки, оскільки саме від них залежить чітка координація та управління заходами захисту на підприємстві. Вони відіграють значну роль у запобіганні економічним збиткам, пов’язаним з можливими витоками даних і порушенням бізнес-процесів. Застосування організаційних інструментів не тільки сприяє мінімізації ризиків витоку інформації, але й зміцнює загальну економічну стабільність та конкурентоспроможність підприємства.

1. *Розробка політики інформаційної безпеки***.** Політика інформаційної безпеки є основою для формування системи управління захистом даних на підприємстві. Вона визначає правила та регламент дій працівників і підрядників при роботі з інформаційними ресурсами. Чітко сформульована політика знижує ризики випадкових порушень або зловживань, які можуть призвести до економічних втрат. З економічної точки зору, наявність комплексної політики захисту зменшує ймовірність витрат на

ліквідацію наслідків інцидентів і підвищує ефективність ресурсів, що виділяються на безпеку.

2. *Навчання персоналу*. Високий рівень обізнаності працівників щодо загроз інформаційній безпеці є ключовим елементом зниження економічних ризиків. Навчання з основ кібербезпеки дозволяє зменшити ризики, пов'язані з людськими факторами, такими як випадкове розголошення конфіденційної інформації або відкриття фішингових листів. Інвестиції в навчання персоналу сприяють економічній безпеці підприємства, оскільки допомагають уникнути прямих і непрямих витрат, пов'язаних з потенційними інцидентами безпеки.

3. *Регулярні аудити інформаційної безпеки***.** Аудити дозволяють виявити слабкі місця в системі захисту даних і забезпечити відповідність внутрішніх процедур актуальним вимогам законодавства та стандартів. Підприємства, що регулярно проводять аудити, можуть оперативно усувати вразливості, зменшуючи ймовірність економічних втрат через зловживання або витоки даних. Таким чином, аудити не лише забезпечують інформаційну безпеку, а й мінімізують фінансові ризики, що можуть загрожувати стабільності підприємства.

4. *Розподіл прав доступу на основі ролей (RBAC)*. Системи розподілу прав доступу на основі ролей допомагають уникнути економічних втрат, пов'язаних з несанкціонованим доступом до критичних даних, що може вплинути на фінансові операції або стратегічні рішення. За допомогою RBAC компанія чітко контролює, хто має доступ до конфіденційної інформації, що мінімізує ризик внутрішніх витоків і підвищує економічну безпеку шляхом захисту важливих бізнес-даних.

5. *План реагування на інциденти*. План реагування на інциденти дозволяє оперативно вирішувати ситуації з порушенням інформаційної безпеки, що є особливо важливим для запобігання значним фінансовим збиткам. Швидке та ефективне реагування на інциденти може суттєво зменшити негативні економічні наслідки, а також уникнути простоїв у бізнес-процесах. Інвестиції в розробку та тестування таких планів сприяють

економічній безпеці, оскільки знижують можливі витрати на відновлення даних і компенсаційні виплати клієнтам [63, С. 40-42].

Організаційні інструменти дозволяють підприємствам більш ефективно контролювати інформаційні потоки та уникати витрат, пов'язаних з інцидентами безпеки. Запровадження стандартів і процедур, спрямованих на захист даних, підвищує загальну економічну стійкість підприємства, дозволяючи зосередити ресурси на розвитку бізнесу, а не на ліквідації наслідків інцидентів.

Організаційні заходи також покращують репутацію компанії на ринку, що сприяє залученню нових партнерів і клієнтів, а також підвищенню довіри інвесторів. Це є важливою конкурентною перевагою, особливо в галузях, де економічна безпека залежить від репутаційних ризиків та рівня захисту даних.

Правові інструменти є важливим елементом системи забезпечення інформаційної безпеки, оскільки вони встановлюють юридичні вимоги, обов'язки та санкції, які сприяють захисту інформації та даних підприємства. Вони допомагають знизити ризики порушення законодавства, що може призвести до економічних втрат у вигляді штрафів, компенсацій або втрати клієнтської довіри. Правові норми не тільки регламентують внутрішні процедури безпеки, але й забезпечують правову основу для боротьби з кіберзлочинністю, що також має значний економічний ефект для компанії.

1. *Законодавчі акти та регулювання в сфері захисту даних*. Основним правовим інструментом для захисту інформації є національне законодавство та міжнародні нормативні акти, що регулюють питання збереження та обробки персональних даних і конфіденційної інформації. В Україні одним із таких законів є Закон України «Про захист персональних даних» [64], який визначає вимоги до обробки та захисту персональної інформації фізичних осіб. Крім того, підприємства можуть бути зобов'язані дотримуватися міжнародних стандартів, таких як Загальний регламент захисту даних (GDPR) в Європейському Союзі [65].

Дотримання цих норм зменшує ризик отримання штрафів за порушення, що можуть мати значні економічні наслідки. Наприклад, порушення вимог GDPR може призвести до штрафів, що обчислюються в мільйонах євро, що є серйозним ударом по фінансовій стабільності підприємства. Правові норми також допомагають знизити ймовірність витоків даних, захищаючи тим самим репутацію компанії.

2. *Контракти та угоди з партнерами*. Один з важливих правових інструментів – це укладення договорів та угод з партнерами, що чітко регламентують умови обробки та захисту інформації. Договори з клієнтами, постачальниками та підрядниками повинні містити положення щодо захисту конфіденційної інформації, обов'язків сторін у випадку порушення безпеки, а також санкцій за невиконання умов [66, С. 97]. Це є важливою частиною правової стратегії захисту інформації, оскільки у разі порушення умов договору компанія може вимагати компенсацію збитків, що виникли внаслідок витоку або зловживання інформацією.

Для підприємства такі контракти виступають не тільки як засіб правового захисту, але й як економічний інструмент, що допомагає зберегти фінансову стабільність у випадку виникнення інцидентів з безпекою.

3. *Захист інтелектуальної власності*. Окрім захисту персональних даних і конфіденційної інформації, важливою частиною правової безпеки є захист інтелектуальної власності підприємства. Це включає патенти, авторські права, торгові марки та комерційну таємницю. З юридичної точки зору підприємства повинні застосовувати правові інструменти для запобігання несанкціонованому використанню своїх інтелектуальних активів, що може призвести до значних економічних втрат [67, С. 38].

Правові інструменти для захисту інтелектуальної власності, такі як реєстрація патентів, авторських прав і торгових марок, допомагають компанії зміцнити свою конкурентоспроможність і забезпечити ексклюзивне право на використання своїх розробок. Це важливий аспект економічної безпеки, оскільки захист інтелектуальних активів дозволяє уникнути фінансових

збитків від контрафакції, плагіату або порушення прав на інтелектуальну власність.

4. *Законодавство щодо кібербезпеки*. Окремо варто зазначити розвиток законодавства, що стосується кібербезпеки, яке є важливим аспектом інформаційної безпеки підприємств, зокрема у контексті протидії кіберзлочинності. Закони, що регулюють кібербезпеку, визначають вимоги до систем захисту інформаційних технологій і програмного забезпечення, а також обов'язки компаній щодо повідомлення про інциденти безпеки.

В Україні з 2017 року діє Закон України «Про основи кібербезпеки України» [68], який встановлює правові основи для забезпечення кібербезпеки на державному та приватному секторах. Порушення вимог цього законодавства може призвести до санкцій, а також зниження рівня довіри з боку партнерів і клієнтів, що має економічні наслідки у вигляді зменшення прибутковості та втрати конкурентних переваг.

5. *Стандартизація та сертифікація*. Для забезпечення відповідності міжнародним вимогам з інформаційної безпеки підприємства можуть застосовувати сертифікацію за міжнародними стандартами, такими як ISO 27001 (система управління безпекою інформації) [69]. Ці стандарти допомагають підприємствам визначити та впровадити найкращі практики в галузі захисту інформації, що дозволяє зменшити ризики фінансових та репутаційних втрат.

Наявність сертифікації за міжнародними стандартами є доказом високої надійності підприємства, що може покращити його репутацію на ринку і допомогти залучити нових інвесторів або клієнтів. Це також може знизити витрати на юридичні ризики та штрафи, оскільки відповідність міжнародним стандартам часто є підставою для звільнення від санкцій або зменшення їх розміру [70].

Правові інструменти забезпечення інформаційної безпеки мають важливе значення для підтримки економічної стабільності підприємства. Вони не тільки регламентують внутрішні процеси захисту даних, а й знижують

ризики фінансових втрат від інцидентів з безпекою. Закони і регулювання забезпечують правову основу для боротьби з кіберзлочинністю, а також визначають обов'язки підприємства перед клієнтами та партнерами. Інвестування в правову безпеку допомагає компаніям уникнути значних витрат, пов'язаних з порушеннями законодавства та втратами репутації, а також забезпечує підвищення конкурентоспроможності на ринку.

Інтеграція інструментів інформаційної безпеки в загальну стратегію підприємства має не тільки технічний, а й економічний аспект, оскільки безпека інформації тісно пов’язана з фінансовими результатами та довгостроковою стабільністю компанії. Недостатній захист інформації може призвести до значних економічних втрат, які проявляються через зниження довіри клієнтів, репутаційні втрати, штрафи за невиконання регуляторних вимог та витрати на відновлення систем [71].

1. Прямі економічні вигоди від застосування інструментів інформаційної безпеки

Безпосередні економічні вигоди від інтеграції інструментів інформаційної безпеки полягають у значному зниженні витрат, пов'язаних з ліквідацією наслідків інцидентів безпеки. Це включає витрати на відновлення втрачених або пошкоджених даних, виплати компенсацій за порушення умов контрактів чи відшкодування клієнтських вимог. Наприклад, у разі кібератаки або витоку конфіденційної інформації компанія не тільки повинна витрачати кошти на технічне відновлення систем, а й може бути змушена сплачувати штрафи або компенсації за невиконання умов угод з партнерами та клієнтами [72, С. 14].

Інвестиції в технічні засоби захисту, такі як брандмауери, антивірусні програми та системи резервного копіювання, здатні значно знизити ці витрати. Зазвичай витрати на впровадження і підтримку систем безпеки виявляються значно меншими, ніж економічні збитки, що виникають через інциденти безпеки, що робить ці інвестиції економічно обґрунтованими.

2. *Зменшення витрат на усунення наслідків інцидентів інформаційної безпеки***.** Один з найбільших економічних ризиків для підприємства пов’язаний із витратами на ліквідацію наслідків кіберінцидентів. Якщо система безпеки підприємства не є належно захищеною, витрати на відновлення даних і відновлення роботи бізнес-процесів можуть бути значними [73, С. 56-57]. Наприклад, простій у роботі через несанкціонований доступ або атаки на інформаційні системи може призвести до втрати клієнтів, що непоправно вплине на доходи компанії.

Інструменти шифрування, контроль доступу та моніторинг допомагають уникнути або мінімізувати масштаби таких інцидентів. Вчасне виявлення загроз та запобігання несанкціонованому доступу дозволяє зберегти функціонування системи без значних економічних втрат. Це особливо важливо для компаній, що працюють з великими обсягами даних або у високоризикових сферах, де кожен інцидент може коштувати мільйони доларів.

3. *Репутаційні ризики та економічні втрати*. Репутаційні збитки є однією з основних економічних загроз для підприємства в разі порушення безпеки. У сучасному світі, де довіра клієнтів і партнерів є важливим активом, будь-який інцидент, пов’язаний із витоком конфіденційної інформації або порушенням систем безпеки, може мати катастрофічні наслідки для бізнесу. Зниження рівня довіри клієнтів призводить до зменшення продажів, втрачених контрактів і, зрештою, фінансових втрат [73, С. 59-60].

Витрати на відновлення репутації також є частиною загальних витрат підприємства на забезпечення безпеки. Створення та підтримка високих стандартів інформаційної безпеки допомагає підприємству зберегти довіру та підтримувати свою репутацію на високому рівні, що в результаті сприяє зростанню економічної стійкості та привабливості на ринку.

4. *Фінансові наслідки від невиконання регуляторних вимог*. У деяких галузях, особливо у фінансовому секторі та галузях, пов’язаних із персональними даними, невиконання вимог законодавства з інформаційної

безпеки може призвести до накладення значних штрафів та санкцій. Закони, такі як Загальний регламент захисту даних (GDPR) в Європейському Союзі або закони про захист персональних даних в інших країнах, визначають жорсткі вимоги щодо захисту інформації. Порушення цих вимог може призвести до штрафів, що обчислюються у мільйонах доларів [74].

Впровадження систем захисту та регулярне оновлення політик безпеки дозволяє не тільки мінімізувати ризики таких штрафів, але й підтримувати прозорість у відносинах із клієнтами та державними органами, що безпосередньо впливає на фінансову стабільність підприємства.

5. *Вплив на конкурентоспроможність підприємства*. Інвестиції в інструменти інформаційної безпеки також мають значний економічний ефект через підвищення конкурентоспроможності підприємства. Безпечне зберігання даних, надійний захист від кібератак та здатність швидко відновлювати роботу у разі інциденту забезпечують бізнесу стабільність і привабливість для клієнтів [75]. Це дозволяє підприємствам зберігати лідерські позиції на ринку, підвищуючи свої фінансові результати.

Таким чином, вкладення в інформаційну безпеку створюють значну економічну цінність, оскільки вони не тільки знижують ризики витрат, але й сприяють стабільному розвитку та підвищенню прибутковості компанії.

Загалом, інтеграція інструментів інформаційної безпеки в стратегію управління економічною безпекою підприємства є важливим кроком для забезпечення не тільки технологічної надійності, а й економічної стабільності. Підприємства, що інвестують у відповідні інструменти та заходи, можуть значно знизити ймовірність фінансових втрат, репутаційних ризиків і отримати конкурентні переваги на ринку.

Забезпечення інформаційної безпеки є важливим аспектом загальної стратегії економічної безпеки підприємства, оскільки від ефективності захисту інформаційних ресурсів безпосередньо залежить його фінансова стабільність, репутація, а також здатність зберігати конкурентоспроможність на ринку. Розглянуті технічні та правові інструменти забезпечення інформаційної

безпеки є необхідними елементами системи управління економічною безпекою підприємства, оскільки вони не тільки мінімізують фінансові витрати, пов’язані з потенційними інцидентами безпеки, але й створюють правову та організаційну основу для управління ризиками.

Технічні інструменти, такі як системи шифрування, антивірусні та антималварні програми, а також системи виявлення і запобігання вторгнень (IDS/IPS), дозволяють знижувати ймовірність витоків або несанкціонованого доступу до конфіденційної інформації, що є критично важливим для збереження економічної стабільності підприємства. Окрім того, ці інструменти зменшують витрати на відновлення пошкоджених чи втрачених даних, а також на зниження можливих штрафів та санкцій, що виникають у випадку порушення законодавства в галузі захисту персональних даних або інших нормативних актів.

З правової точки зору, системи правового регулювання та нормативно-правові акти, такі як національні закони і міжнародні регламенти, встановлюють вимоги щодо обробки та захисту інформації, зокрема персональних даних. Вони формулюють обов'язки підприємства щодо захисту інформації, а також визначають санкції за порушення цих вимог. При цьому дотримання цих норм забезпечує юридичну стабільність компанії, знижує ймовірність фінансових збитків, пов'язаних з порушенням законодавства, а також допомагає уникнути репутаційних ризиків. Порушення правових норм щодо захисту даних або інтелектуальної власності може призвести до значних фінансових штрафів, що мають серйозний економічний ефект, особливо в контексті міжнародних стандартів, таких як GDPR.

Не менш важливим є використання правових інструментів для забезпечення захисту інтелектуальної власності, що дозволяє компанії зберегти свої інновації і технології від несанкціонованого використання. Дотримання правових норм у сфері захисту інтелектуальної власності сприяє не тільки захисту фінансових активів підприємства, але й зміцненню його позицій на ринку, оскільки володіння патентами, торговими марками та

іншими правами інтелектуальної власності є важливим фактором конкурентоспроможності.

Таким чином, система правових та технічних інструментів, що забезпечує інформаційну безпеку підприємства, має суттєвий економічний ефект. Вона не лише знижує потенційні ризики, пов'язані з інформаційними загрозами, а й дозволяє підвищити фінансову стабільність підприємства, забезпечуючи йому ефективне функціонування в умовах постійної еволюції загроз та викликів у сфері інформаційних технологій. Тому інвестиції в інформаційну безпеку мають стратегічне значення для розвитку підприємства та його здатності підтримувати конкурентні переваги на глобальному ринку, одночасно зберігаючи економічну стійкість і виконуючи вимоги національних та міжнародних норм.

3.3. Організаційні заходи для покращення рівня інформаційної безпеки

Організаційні заходи є ключовим компонентом системи забезпечення інформаційної безпеки підприємства, оскільки вони забезпечують створення структурованої і системної моделі захисту інформаційних ресурсів від потенційних загроз. В умовах швидкої цифровізації та розвитку інформаційних технологій, які постійно змінюються, підприємства стикаються з новими викликами у сфері безпеки. Зважаючи на те, що інформація стає одним з найцінніших активів організації, без належного її захисту може відбутися втрата конкурентних переваг, репутаційні та фінансові втрати, а також порушення прав і довіри клієнтів, партнерів і держави.

Організаційні заходи для забезпечення інформаційної безпеки підприємства мають на меті створення ефективної та стійкої системи захисту інформаційних ресурсів і збереження інформаційної цілісності на всіх рівнях діяльності організації. В умовах глобалізації та інтеграції інформаційних технологій, ці заходи набувають надзвичайної важливості для забезпечення безперебійної діяльності підприємства, захисту від зовнішніх і внутрішніх

загроз, а також збереження довіри клієнтів і партнерів. Головною метою організаційних заходів є мінімізація ризиків, пов'язаних із порушенням інформаційної безпеки, забезпечення безперервності бізнес-процесів, а також підтримка економічної стійкості організації [77, С. 105].

Основною метою організаційних заходів є створення системи, яка дозволить забезпечити належний рівень захисту інформаційних ресурсів підприємства і забезпечити їх збереження, цілісність і конфіденційність. Це включає в себе створення ефективної організаційної структури управління інформаційною безпекою, розробку внутрішніх стандартів і політик, а також навчання персоналу для своєчасного виявлення та усунення загроз, що можуть виникнути в процесі функціонування інформаційних систем.

Крім того, організаційні заходи спрямовані на зниження ризиків, пов’язаних із інцидентами безпеки, і забезпечення безперервності інформаційних потоків. Вони також мають за мету підтримку високого рівня довіри з боку клієнтів та партнерів, що є важливим аспектом у глобальному бізнес-середовищі.

Основні завдання організаційних заходів.

1. *Розробка і впровадження політик і стандартів безпеки*. Основною задачею організаційних заходів є розробка чітких і детальних політик, регламентів і стандартів, що визначають основні правила і принципи захисту інформаційних активів підприємства. Це включає в себе формулювання політики безпеки на рівні організації, визначення вимог до технічного оснащення та засобів захисту інформаційних систем, а також створення механізмів для виконання цих вимог.

2. *Створення організаційної структури управління безпекою*. Організаційні заходи включають формування відповідної організаційної структури, яка забезпечить ефективне управління безпекою інформаційних систем. Визначення відповідальних осіб за забезпечення інформаційної безпеки на рівні підприємства, формування комітету з питань безпеки та

створення окремих підрозділів для здійснення контрольних функцій є важливою складовою частиною цієї задачі.

3. *Ідентифікація та оцінка ризиків безпеки. Для* забезпечення високого рівня інформаційної безпеки важливо виявити можливі загрози, які можуть вплинути на функціонування підприємства. Оцінка ризиків дозволяє визначити ймовірність та потенційну шкоду від можливих інцидентів безпеки, що допомагає ухвалити відповідні організаційні рішення щодо їх усунення або зниження.

4. *Навчання та підвищення обізнаності персоналу***.** Оскільки людський фактор є однією з найбільших загроз для інформаційної безпеки, організаційні заходи повинні включати систематичне навчання персоналу. Це передбачає не лише навчання правилам безпеки та використанню програмного забезпечення для захисту інформаційних систем, але й підвищення обізнаності щодо ризиків, які існують у повсякденній діяльності, та створення відповідної корпоративної культури безпеки.

5. *Моніторинг і контроль за виконанням політик безпеки*. Для забезпечення ефективного функціонування системи інформаційної безпеки необхідно постійно здійснювати моніторинг і контроль за виконанням політик і процедур. Це включає в себе регулярні перевірки відповідності внутрішнім стандартам безпеки, аудит інформаційних систем, а також оцінку ефективності заходів, що вживаються.

6. *Розробка і впровадження плану реагування на інциденти безпеки*. Інциденти безпеки, як-от атаки, витоки даних або збої в роботі інформаційних систем, є неминучою частиною діяльності підприємства. Тому необхідно розробити та впровадити чіткий ***план реагування на інциденти безпеки***, який має включати процедури для оперативного виявлення, оцінки та ліквідації наслідків таких інцидентів. Важливою складовою є визначення ролей і відповідальностей співробітників у разі виникнення таких інцидентів.

7. *Забезпечення відповідності законодавчим та нормативним вимогам*. Організаційні заходи мають також включати забезпечення

відповідності вимогам національного та міжнародного законодавства в сфері інформаційної безпеки. Це може включати дотримання стандартів та вимог щодо захисту персональних даних, захисту прав інтелектуальної власності, а також виконання інших нормативних актів, що стосуються інформаційної безпеки.

Мета та задачі організаційних заходів для забезпечення інформаційної безпеки підприємства полягають у створенні ефективної системи управління безпекою, яка забезпечить збереження та захист інформаційних ресурсів, забезпечить безперервність бізнес-процесів та мінімізує ризики, пов'язані з порушеннями безпеки. Для цього підприємства повинні розробляти чіткі політики безпеки, визначати відповідальних осіб і підрозділи, навчати персонал та регулярно оцінювати ризики. Усі ці заходи сприяють створенню стійкої і надійної інформаційної системи, що здатна ефективно протистояти сучасним загрозам та інцидентам безпеки [73, С. 112-114].

Організаційні заходи для забезпечення інформаційної безпеки є важливою складовою частиною загальної стратегії захисту інформаційних ресурсів підприємства. Вони охоплюють широкий спектр дій, спрямованих на забезпечення надійності інформаційних систем і захисту від внутрішніх та зовнішніх загроз. Організаційні заходи можуть бути різних видів, кожен з яких має свою специфіку, мету та способи реалізації. Загалом їх можна розподілити на кілька категорій, зокрема, за напрямками впливу, на:

1. інституційні заходи;
2. процедурні заходи;
3. мотиваційні заходи;
4. інформаційно-просвітницькі заходи;
5. контрольні заходи.

Кожен з цих видів має своє значення в загальній системі управління інформаційною безпекою на підприємстві, і для їх ефективної реалізації необхідно взаємодіяти з іншими елементами безпекової інфраструктури [77].

Інституційні заходи є основою для формування організаційної структури, яка забезпечує інформаційну безпеку підприємства. Вони передбачають створення і розвиток спеціалізованих підрозділів, визначення відповідальних осіб та розподіл повноважень, а також впровадження політики та стратегій в області безпеки.

Основні інституційні заходи:

1. Створення підрозділів з інформаційної безпеки. Організація підприємства повинна мати чітко визначену відповідальність за інформаційну безпеку, що включає в себе створення окремого підрозділу або відділу, на який покладається моніторинг, аналіз і забезпечення виконання всіх процедур безпеки.

2. Призначення керівників з питань безпеки**.** У рамках інституційних заходів важливо призначити відповідальних осіб за різні аспекти інформаційної безпеки. Це може бути як загальний керівник безпеки, так і спеціалізовані менеджери, що відповідають за технічну безпеку, управління ризиками, правове забезпечення тощо.

3. Розробка політик і стандартів безпеки. Одним із головних інституційних заходів є розробка і впровадження корпоративних стандартів і політик інформаційної безпеки, які визначають основні принципи і правила захисту даних, а також процедури реагування на інциденти безпеки [78].

Процедурні заходи включають встановлення чітких внутрішніх процесів і стандартів для забезпечення безпеки інформаційних систем підприємства. Вони мають на меті визначити, як організувати роботу з інформаційною безпекою, щоб забезпечити її належний рівень.

Основні процедурні заходи:

1. Ідентифікація та оцінка ризиків. Процедурний аспект безпеки включає в себе регулярне виявлення і оцінку ризиків, пов’язаних з інформаційними системами. Для цього необхідно розробити методику і систему оцінки, що дозволяє вчасно виявляти потенційні загрози, такі як

втрати даних, кіберзагрози, збої в роботі інформаційних систем, і визначати їхній можливий вплив на організацію.

2. Розробка та реалізація плану реагування на інциденти безпеки. План реагування на інциденти є важливим процедурним елементом, що допомагає оперативно вирішити проблеми, пов’язані з порушенням інформаційної безпеки. Такий план повинен включати чіткі інструкції щодо дій у випадку атаки, втрати даних або інших інцидентів, а також визначення відповідальних осіб та процедур.

3. Процедури відновлення та резервного копіювання даних. Процедури відновлення даних є необхідними для того, щоб швидко відновити роботу інформаційних систем у разі інциденту безпеки. Вони включають в себе регулярне резервне копіювання важливої інформації та розробку процедур для відновлення даних у разі їх пошкодження або втрати [79].

Мотиваційні заходи орієнтовані на підвищення рівня залученості співробітників у процес забезпечення інформаційної безпеки, шляхом створення відповідних стимулів та умов для їх активної участі в цьому процесі.

Основні мотиваційні заходи:

1. Заохочення та винагороди. Для підвищення рівня обізнаності співробітників та їхнього зацікавлення в дотриманні стандартів безпеки важливо впроваджувати системи винагород і заохочень за виявлені ініціативи в галузі безпеки або за успішне виконання обов’язків, пов'язаних з безпекою.

2. Створення корпоративної культури безпеки. Розвиток корпоративної культури, де кожен співробітник розуміє свою роль у забезпеченні безпеки інформації та несе відповідальність за її збереження, є важливим мотиваційним фактором. Важливо, щоб питання інформаційної безпеки були інтегровані в загальні цінності компанії [80].

Інформаційно-просвітницькі заходи передбачають розповсюдження знань про інформаційну безпеку серед працівників, щоб підвищити їхню обізнаність і підготувати до ефективного реагування на можливі загрози. Ці

заходи допомагають сформувати правильне розуміння важливості інформаційної безпеки.

Основні інформаційно-просвітницькі заходи:

1. Проведення навчальних тренінгів та семінарів. Регулярні тренінги для співробітників організації з питань інформаційної безпеки є необхідними для підвищення їхньої обізнаності про сучасні загрози та методи захисту. Це включає в себе навчання на теми захисту персональних даних, кібербезпеки, а також способів реагування на інциденти.

2. Розповсюдження внутрішніх інформаційних матеріалів. Регулярне оновлення інформаційних бюлетенів, презентацій і статей на тему інформаційної безпеки дозволяє підтримувати інтерес співробітників до цієї теми і нагадувати про важливі аспекти захисту інформаційних ресурсів [81].

Контроль та аудит є важливими інструментами для перевірки ефективності системи інформаційної безпеки на підприємстві. Вони дозволяють оцінити відповідність внутрішнім стандартам, виявити недоліки в процесах та своєчасно внести корективи.

Основні контрольні заходи:

1. Регулярний аудит інформаційної безпеки. Аудит безпеки дозволяє виявити недоліки в існуючих заходах з захисту інформаційних систем і оцінити їхню ефективність. Це включає перевірки політик і процедур безпеки, а також оцінку рівня відповідності чинному законодавству.

2. Моніторинг інформаційних систем. Моніторинг є постійним процесом, що включає відстеження подій і дій в інформаційних системах. Це дозволяє своєчасно виявляти аномалії, збої або порушення безпеки, що може допомогти запобігти інцидентам або швидко на них реагувати [82].

Види організаційних заходів для забезпечення інформаційної безпеки охоплюють широкий спектр активностей, які разом створюють систему управління безпекою на підприємстві. Організаційні заходи, спрямовані на забезпечення інформаційної безпеки підприємства, є основою для створення стійкої та ефективної системи захисту інформаційних ресурсів, що має не

лише технічний, а й економічний ефект. Вони дозволяють підприємству знизити потенційні фінансові втрати, пов'язані з інцидентами безпеки, покращити управління ризиками і забезпечити безперервність бізнес-процесів. Враховуючи значні економічні витрати на відновлення після кіберінцидентів, організаційні заходи з інформаційної безпеки можна вважати ефективними інвестиціями, що дозволяють уникнути великих фінансових збитків.

Підприємства, які здійснюють впровадження організаційних заходів для підвищення рівня інформаційної безпеки, здатні значно знизити ймовірність фінансових втрат, пов'язаних з витоками конфіденційних даних, порушеннями внутрішніх політик безпеки та репутаційними ризиками. Наприклад, витрати на впровадження політик безпеки, навчання персоналу та створення системи моніторингу можуть бути меншими за потенційні збитки від витоку даних або зупинки бізнес-процесів через кібератаки.

Економічний ефект від організаційних заходів можна оцінити через зниження витрат на ліквідацію наслідків інцидентів безпеки. Інвестиції в розробку внутрішніх процедур, системи моніторингу та навчання персоналу дозволяють підприємству мінімізувати втрати, пов'язані з відновленням після інцидентів безпеки, компенсувати витрати на відновлення даних та репутаційні втрати, а також уникнути штрафів та санкцій, що можуть бути накладені за порушення вимог законодавства або контрактних зобов'язань.

Організаційні заходи включають також створення чіткої організаційної структури, що дозволяє забезпечити ефективну взаємодію між усіма підрозділами підприємства, підвищити рівень координації в разі виникнення загрози, що також сприяє зниженню витрат на ліквідацію інцидентів і забезпечує швидке відновлення нормальної роботи підприємства.

Підвищення обізнаності персоналу щодо вимог інформаційної безпеки і формування корпоративної культури безпеки також має важливе значення в економічному контексті. Освічений і відповідальний персонал здатний мінімізувати ймовірність помилок, що можуть призвести до порушень

безпеки, тим самим знижуючи ризики для підприємства. Це також сприяє економії ресурсів, оскільки впровадження політик безпеки та навчання співробітників є менш витратним у порівнянні з витратами на ліквідацію наслідків інцидентів.

Загалом, організаційні заходи для забезпечення інформаційної безпеки мають значний економічний аспект. Вони сприяють не лише зменшенню витрат на усунення наслідків інцидентів безпеки, але й підвищенню ефективності бізнес-процесів, збереженню стабільності підприємства та розвитку довгострокових конкурентних переваг. Таким чином, інвестування в організаційні заходи є економічно виправданим і необхідним для сталого функціонування підприємства в умовах цифрової трансформації та зростаючих кіберзагроз.

ВИСНОВКИ

Дослідження проблематики інформаційної безпеки показало, що в умовах сучасного бізнес-середовища інформаційна безпека є не лише технічним, але й економічно обґрунтованим завданням для підприємств. Проведений аналіз дозволив сформувати такі основні висновки.

У роботі доведено, що забезпечення інформаційної безпеки є невід'ємною частиною економічної стратегії компанії, оскільки забезпечує захист ключових інформаційних активів, які є основою конкурентоспроможності та фінансової стабільності. Втрата або пошкодження цих активів, наприклад, через витік комерційної інформації чи зловмисне втручання, може призвести до фінансових збитків і втрати ринкових позицій. Систематичні інвестиції в інформаційну безпеку розглядаються як стратегічно вигідні, оскільки вони знижують ризики, які могли б значно зменшити прибутковість або навіть призвести до припинення діяльності підприємства.

Кіберзагрози, такі як DDoS-атаки, фішингові кампанії, програми-вимагачі, а також витоки конфіденційної інформації, стають все більш поширеними. За оцінками міжнародних досліджень, бізнеси щороку зазнають значних втрат від таких загроз, які в середньому становлять від 1 до 5% від річного доходу. Економічні збитки охоплюють не тільки прямі витрати на відновлення після інцидентів, але й непрямі втрати, такі як зниження репутації, скорочення клієнтської бази, підвищення страхових витрат та можливі штрафи за порушення законодавства. Таким чином, запобігання загрозам стає економічно виправданим рішенням, що дозволяє уникнути значних втрат.

Три ключові аспекти інформаційної безпеки – конфіденційність, цілісність і доступність – мають прямий економічний вплив на бізнес-процеси підприємства. Конфіденційність забезпечує захист комерційних таємниць, які є джерелом конкурентних переваг і унікальних бізнес-рішень компанії. Втрата конфіденційності призводить до ризику витоку інновацій, що можуть бути

використані конкурентами, знижуючи таким чином цінність підприємства на ринку. Цілісність інформації дозволяє уникнути фінансових помилок і спотворень у процесі прийняття управлінських рішень, що забезпечує точність і актуальність фінансових звітів. Нарешті, доступність інформації гарантує безперервність операційних процесів: тимчасовий недоступ до інформаційних ресурсів може спричинити втрату доходів через зупинку сервісів або виробництва.

У дослідженні виділено три основні групи методів забезпечення інформаційної безпеки: технічні, організаційні та правові.

Технічні заходи включають засоби шифрування, антивірусне програмне забезпечення, системи виявлення вторгнень, резервне копіювання та управління доступом. Інвестиції в ці технології мають високий коефіцієнт окупності (ROI), оскільки дозволяють запобігати або мінімізувати економічні збитки від несанкціонованих втручань і простоїв.

Організаційні заходи включають навчання персоналу, розробку політик безпеки, контроль доступу та регулярні аудити інформаційної безпеки. Економічна доцільність цих заходів полягає в зменшенні ризиків від дій внутрішніх користувачів, зокрема ненавмисних помилок, які можуть призвести до збитків. Згідно з дослідженнями, до 40% інцидентів інформаційної безпеки пов’язані саме з внутрішніми помилками персоналу, що підтверджує важливість організаційних заходів.

Правові заходи забезпечують дотримання законодавства щодо захисту інформації та даних, таких як GDPR в ЄС або відповідні норми національного законодавства. Це дозволяє уникати штрафів та судових процесів, що економічно обґрунтовує такі заходи як превентивні інвестиції.

Впровадження міжнародних стандартів, таких як ISO/IEC 27001, сприяє структурованому та ефективному підходу до інформаційної безпеки, що забезпечує фінансові вигоди для компанії. По-перше, сертифікація за такими стандартами може підвищити довіру клієнтів і партнерів, що сприяє розширенню ринкових можливостей. По-друге, стандартні процедури

мінімізують ризик виникнення інцидентів, які можуть призвести до значних витрат. Нарешті, відповідність стандартам спрощує взаємодію з партнерами, що також позитивно впливає на економічний результат.

Інвестиції у системи інформаційної безпеки можуть швидко окупитися завдяки зменшенню кількості атак, простоїв і витоків даних. Наприклад, впровадження багаторівневої аутентифікації та політик управління доступом дозволяє скоротити інциденти, пов’язані з несанкціонованим доступом, на 30–50%, що значно знижує ризик економічних втрат.

Постійне оновлення загроз і технологічні інновації вимагають від підприємств регулярної модернізації систем захисту. Хоча це потребує додаткових інвестицій, забезпечення актуальності та гнучкості захисних систем має стратегічне економічне значення, оскільки знижує ризики простоїв, втрати даних і збоїв у бізнес-процесах. Постійна адаптація до змін зміцнює позиції компанії на ринку, захищає її інтелектуальну власність, підтримує довіру клієнтів і покращує репутацію.

Інформаційна безпека є не просто елементом технічної інфраструктури, а критичним економічним чинником, який впливає на стабільність, рентабельність та конкурентоспроможність підприємства. Результати дослідження підтверджують, що впровадження комплексних систем інформаційної безпеки забезпечує суттєві економічні вигоди у вигляді зниження операційних витрат на відновлення, мінімізації фінансових втрат від простоїв та втрат даних, а також покращення репутації компанії серед клієнтів та партнерів.

Таким чином, інформаційна безпека стає важливим інструментом підтримки та зростання економічної стійкості підприємства, що дозволяє зменшити економічні втрати від зовнішніх та внутрішніх загроз і забезпечити стабільне функціонування в умовах постійних змін та кіберризиків.

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. Таціенко 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.