DOI: https://doi.org/10.30837/EK.2024.014

Легеза О.М.,
асистент кафедри економічної кібернетики та управління економічною безпекою,
Харківський національний університет радіоелектроніки
ORCID: https://orcid.org/0009-0003-2784-1985
Тесленко І.В.,
асистент кафедри економічної кібернетики та управління економічною безпекою,
Харківський національний університет радіоелектроніки
ORCID: https://orcid.org/0009-0000-0725-3674
Полозова О.О.,
здобувач вищої освіти,
Харківський національний університет радіоелектроніки
ORCID: https://orcid.org/0009-0009-4235-7511
Полозов М.О.,
здобувач вищої освіти,
Харківський національний університет радіоелектроніки
ORCID: https://orcid.org/0009-0007-7886-7551

ВПЛИВ КІБЕРЗАГРОЗ ТА ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ НА ЗАБЕЗПЕЧЕННЯ ФІНАНСОВОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Сучасний бізнес усе більше залежить від цифрових технологій, які не тільки спрощують операційні процеси, але й відкривають доступ до нових ринків і можливостей. Однак разом із цим зростає й рівень загроз, що ставлять під удар фінансову безпеку підприємств. Кіберзлочини, такі як хакерські атаки, фішинг,

витік конфіденційних даних і шахрайство у фінансових транзакціях, можуть спричинити не лише значні фінансові втрати, а й підрив довіри з боку клієнтів і партнерів. Згідно з дослідженнями, збитки від кіберзагроз щорічно зростають, що робить цю проблему однією з ключових у сучасній економіці.

У цьому контексті інформаційні технології відіграють подвійну роль. З одного боку, вони є інструментом для злочинців, які використовують вразливості в системах, а з іншого – стають найпотужнішим засобом захисту. Завдяки впровадженню сучасних IT-рішень підприємства можуть створювати багаторівневі системи безпеки, що дозволяють швидко виявляти загрози, мінімізувати ризики та забезпечувати безперебійну роботу.

Проблематика фінансової безпеки підприємств в умовах цифровізації висвітлювалася у роботах багатьох авторів, серед яких Мехед А. М., Варналій З. С. [1], Маковець О. П., Дрозд І. К. [2], Ковальчук А. М. [3], Мельник В. В., Жук Т. В. [4], Полозова Т. В., Степаненко С. В., Мурзабулатова О. В., Пономарьов С. В. [5], Помогалова Н. В. та інші [6].

На макроекономічному рівні питання забезпечення фінансової та економічної безпеки держави, зокрема в контексті кібербезпеки розглядалися у роботах таких науковців, як Мунько А. Ю. [7], Полозова Т.В., Шейко І. А. [8] та інші [8]. Попри таку кількість публікацій потребує подальшого наукового пошуку проблематика впливу кіберзагроз та використання інформаційних технологій на забезпечення фінансової безпеки підприємства.

Метою дослідження є визначення факторів впливу кіберзагроз та використання інформаційних технологій на забезпечення фінансової безпеки підприємства.

Кіберзагрози впливають на фінансову безпеку підприємств, окремі види атак становлять значну загрозу для бізнесу, а інноваційні технології та стратегії дозволяють ефективно протистояти цим викликам. У свою чергу, штучний

інтелект, блокчейн і системи моніторингу відіграють важливу роль у створенні надійного кіберзахисту.

Кіберзагрози – це потенційні або реальні дії, спрямовані на порушення конфіденційності, цілісності, доступності інформаційних ресурсів або функціонування інформаційних систем. Вони становлять серйозний ризик для безпеки компаній, держав, організацій і приватних осіб.

Ефективне формування та реалізація кібербезпекової політики, що включає комплекс заходів для прогнозування та протидії кіберзагрозам, є важливою умовою розвитку та покращення фінансової безпеки будь-якого підприємства. У контексті глобалізації інформаційних процесів та їх інтеграції в різні сфери суспільного життя провідні країни світу приділяють особливу увагу створенню й вдосконаленню систем захисту критичної інфраструктури від внутрішніх і зовнішніх кібернетичних загроз.

Фінансова безпека є невід'ємною складовою економічної безпеки, а кібербезпека, як частина інформаційної безпеки, відіграє важливу роль у її забезпеченні. Рівень фінансової безпеки підприємства значною мірою залежить від ефективності кіберзахисту.

Сучасний розвиток інформаційних технологій створює нові потенційні загрози для фінансових інтересів бізнесу, які можуть виникати на різних етапах його діяльності. Одним із найбільш небезпечних видів загроз є кіберзагрози, які здатні суттєво впливати на всі аспекти функціонування підприємства в цифровому середовищі.

Кіберзагрози, що виникають у процесі цифровізації, можуть включати кібератаки на фінансові системи, крадіжку конфіденційних даних, фальсифікацію фінансової інформації та інші форми кіберзлочинності (табл. 1).

Таблиця 1 – Основні форми кіберзлочинності та їх характеристики

Форма кіберзлочинності	Опис	Ризики та наслідки
Кібератаки на фінансові системи	Атаки на фінансові платформи, банки, платіжні системи з метою крадіжки грошей або перехоплення фінансових транзакцій	Фінансові втрати, компрометація даних клієнтів, порушення роботи платіжних систем, репутаційні втрати
Крадіжка конфіденційних даних	Неавторизований доступ до особистих, корпоративних чи фінансових даних з метою їх використання для шахрайства, продажу або маніпулювання	Фінансові збитки, втрата довіри клієнтів, використання викраденої інформації для подальших атак або злочинних дій
Фальсифікація фінансової інформації	Зміна або підробка фінансових звітів, транзакцій або рахунків з метою приховати реальні фінансові результати або маніпулювати ринковою інформацією	Порушення фінансової звітності, штрафи та санкції, пошкодження корпоративної репутації, неправдиві інвестиційні рішення
Фішинг	Створення підроблених веб-сайтів або електронних листів для отримання конфіденційної інформації, таких як логіни, паролі, номери карток	Викрадення особистих даних, доступ до банківських рахунків, шахрайство
Використання шкідливих програм (malware)	Встановлення вірусів, троянів, програм-вимагачів на комп'ютери для отримання доступу до важливих даних або блокування доступу до ресурсів підприємства	Втрата даних, зупинка бізнес-процесів, фінансові збитки, втрата репутації
Атаки типу DDoS (Distributed Denial of Service)	Наплив запитів на сервери або веб-сайти з метою їх перевантаження та виведення з ладу	Зупинка роботи систем, витрати на відновлення, можливість використання як тло для інших атак
Шахрайство в електронній комерції	Використання фальшивих веб-сайтів, крадіжка платіжних даних або маніпуляція транзакціями на онлайн-майданчиках для незаконного збагачення	Фінансові втрати для клієнтів, зниження довіри до онлайн-платежів, штрафи для бізнесу за порушення безпеки
Атаки на криптовалюти	Викрадення або маніпулювання криптовалютними транзакціями, доступ до приватних ключів, крадіжка цифрових активів	Втрата криптовалюти, відсутність регулювання криптовалют, труднощі з поверненням вкрадених коштів

Джерело: розроблено авторами.

Такі атаки можуть призвести не лише до безпосередніх фінансових втрат, але й до репутаційних збитків, порушення довіри клієнтів та партнерів, а також до втрати конкурентних переваг на ринку.

З огляду на ці ризики, важливим аспектом забезпечення фінансової безпеки підприємства є створення та впровадження комплексних систем кіберзахисту. Це включає використання передових технологій, таких як штучний інтелект для виявлення аномалій у фінансових транзакціях, блокчейн для забезпечення прозорості та незмінності фінансових записів, а також системи моніторингу для оперативного реагування на можливі загрози.

Надійна кібербезпека стає ключовим фактором для підтримки стабільності фінансових потоків та довгострокового розвитку підприємств у умовах цифрової трансформації. Тому розвиток та вдосконалення кіберзахисту вимагають постійної уваги та ресурсів від керівництва підприємств, адже у сучасному світі кіберзагрози можуть мати руйнівні наслідки для економічної безпеки не лише окремих компаній, але й для національних економік в цілому.

Нормативно-правове регулювання розвитку інформаційного суспільства та заходи з формування державної інформаційної політики повинні відповідати завданням у сфері фінансової безпеки. Вони також мають враховувати практику збереження державної таємниці, захист інформаційно-телекомунікаційної інфраструктури та інформаційних ресурсів від кібератак і загроз у фінансово-економічному просторі. Основними етапами забезпечення ефективного управління кібербезпекою як складовою політики фінансової безпеки підприємства є [4]:

– постійний аналіз можливих кіберзагроз, що можуть вплинути на фінансові операції підприємства. Це передбачає виявлення вразливостей у фінансових системах, облікових записах, базах даних та інших критичних елементах інфраструктури;

– розробка чітких внутрішніх політик із захисту фінансової інформації. Визначення правил доступу до даних, управління паролями, протоколів шифрування та регулярних перевірок безпеки;

– використання сучасних систем моніторингу, заснованих на штучному інтелекті, для виявлення підозрілої активності в реальному часі. Впровадження інструментів для раннього попередження про потенційні загрози та несанкціоновані транзакції;

– використання методів шифрування для збереження конфіденційності фінансових даних. Впровадження багаторівневих систем аутентифікації для захисту доступу до облікових записів та важливих систем;

– регулярне проведення тренінгів для співробітників з метою підвищення їхньої обізнаності про кіберзагрози, такі як фішинг, вірусні атаки та інші види шахрайства. Навчання ефективним методам розпізнавання та уникнення кібератак;

– розробка плану реагування на кіберінциденти, включаючи процедури швидкого реагування на атаки, відновлення фінансових операцій та збереження даних. Визначення команди, відповідальної за кіберзахист та реагування на інциденти;

– проведення регулярних аудитів систем кіберзахисту для виявлення слабких місць та оцінки їхньої ефективності. Використання тестів на проникнення (penetration testing) для перевірки стійкості системи до зовнішніх загроз;

– обмін інформацією про потенційні загрози з банками, страховими компаніями та іншими партнерами. Участь у галузевих ініціативах із забезпечення кібербезпеки та застосування передових практик.

Досліджуючи питання забезпечення фінансової безпеки підприємства, важливо враховувати сучасні підходи до захисту інформації. Пандемія COVID-19 суттєво

вплинула на діяльність компаній у всьому світі. Багато з них були змушені перевести окремих працівників, цілі відділи або навіть усю діяльність на віддалений режим роботи. Це призвело до змін у роботі з внутрішніми даними підприємств.

Непередбачувані обставини, постійні зміни умов роботи, а також недостатня технічна підтримка та оснащення підприємств створили сприятливі умови для успішних кібератак.

Враховуючи специфіку діяльності кожного підприємства необхідно розробляти систему заходів щодо захисту інформаційної системи підприємства. Інформаційне забезпечення фінансової безпеки підприємства вимагає реалізації наступних заходів щодо захисту роботи інформаційної системи (рис. 1).

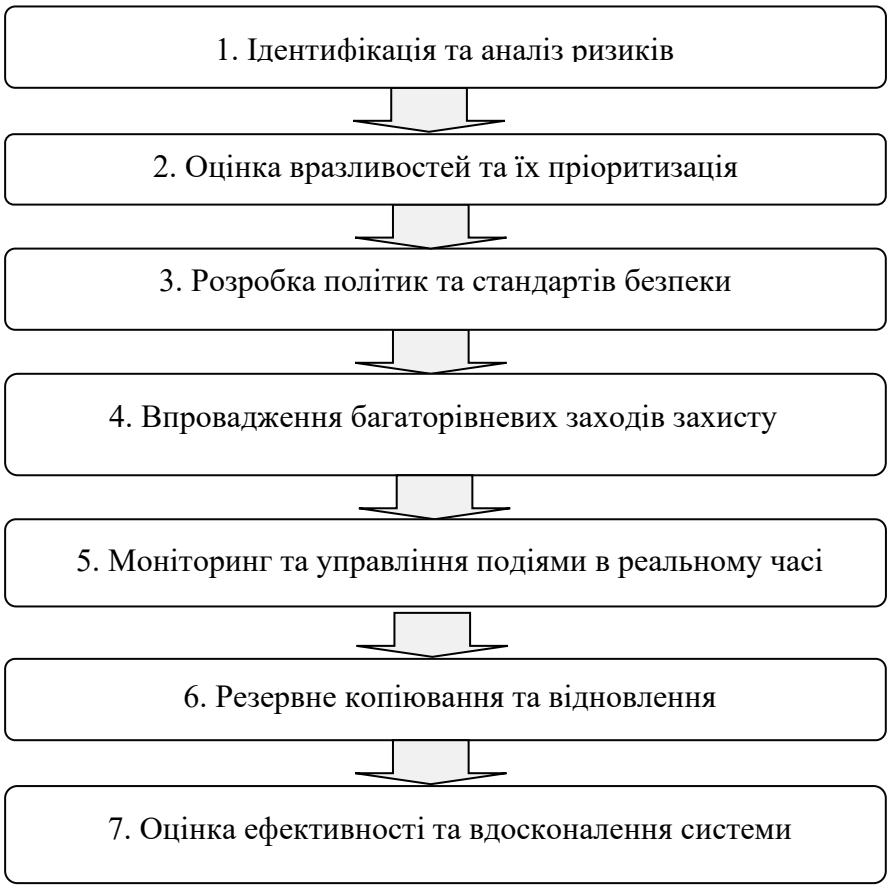

Рисунок 1 – Заходів щодо захисту роботи інформаційної системи фінансової безпеки підприємства

Джерело: складено за даними [7].

Першим і ключовим етапом є виявлення можливих кіберзагроз та оцінка ризиків для інформаційних активів підприємства. Це включає збір і аналіз даних про потенційні атаки, такі як фішинг, DDoS-атаки чи шкідливе ПЗ. SWOT-аналіз допомагає виявити сильні та слабкі сторони інформаційної інфраструктури. Крім того, системи на основі штучного інтелекту можуть автоматично виявляти аномалії в поведінці мережі для запобігання атакам.

Наступним кроком є виявлення вразливостей у системах підприємства. Автоматизоване сканування дозволяє виявити слабкі місця в програмному забезпеченні, мережах або апаратних засобах. Важливо визначити пріоритети для усунення найбільш критичних вразливостей і використовувати поведінковий аналіз для прогнозування потенційних ризиків.

Ефективна політика кібербезпеки повинна враховувати різні рівні доступу до даних і ресурсів. Необхідно розробити правила, що регулюють доступ працівників до інформації та її обробку. Підрядники та партнери також мають дотримуватись встановлених стандартів. Ці політики повинні постійно оновлюватися відповідно до нових загроз і змін у законодавстві.

Захист даних має бути багаторівневим. Важливим елементом є багатофакторна аутентифікація для доступу до критично важливих систем. Необхідно використовувати мережеві екрани та системи виявлення вторгнень, які дозволяють ідентифікувати та блокувати підозрілу активність. Шифрування даних гарантує їхню безпеку як під час зберігання, так і під час передачі.

Підприємству слід створити Центр моніторингу безпеки, який у реальному часі відстежує та аналізує підозрілу активність. Системи SIEM дозволяють збирати та аналізувати журнали подій, а автоматизовані системи реагування (SOAR) забезпечують швидке усунення загроз, мінімізуючи потенційні збитки.

Критично важливі дані мають зберігатися в ізольованих середовищах, а резервні копії мають створюватися регулярно. План безперервності бізнесу (BCP) повинен передбачати швидке відновлення даних після інцидентів, щоб забезпечити мінімальні втрати.

Забезпечення кібербезпеки – це безперервний процес, тому необхідно постійно моніторити ключові показники ефективності. Збір зворотного зв'язку та аналіз інцидентів дозволяють виявити недоліки та покращити систему. Інвестиції в новітні технології, такі як штучний інтелект і блокчейн, забезпечують стійкість системи до нових загроз.

Отже, формування безпечного середовища для формування, розподілу та використанні фінансових ресурсів включає заходи щодо запобігання кібератакам, злочинам, пов'язаним з кіберзлочинністю, і захист фінансової інфраструктури, а також підтримку середовища, яке сприяє технологічному прогресу. Цей напрям безпеки є важливою складовою фінансової безпеки підприємства та вимагає їх подальших наукових досліджень на перетині цих сфер.

Перелік джерел посилання

1. Мехед А. М., Варналій З. С. Фінансова безпека підприємств в умовах цифрової економіки. *Вісник університету банківської справи.* 2021. Вип. 3 (42). С. 55-61.

2. Маковець О. П., Дрозд І. К. Кібербезпека як фактор фінансової безпеки підприємства. *Економіка. Фінанси. Право.* 2020. № 5/3. С. 31-35.

3. Ковальчук А. М. Фінансово-економічна безпека підприємства в контексті адаптації до викликів цифрового середовища. *Економічний вісник «Економіка підприємства».* 2020. Вип. 3. С. 152-159.

4. Мельник В. В., Жук Т. В. Інформаційне забезпечення як складова фінансової безпеки підприємства. *Електронне наукове фахове видання «Ефективна економіка»*. 2021. Вип. 6. URL: www.economy.nayka.com.ua

5. Polozova T., Stepanenko S., Murzabulatova O., Ponomarov S. Specific of the creation and functioning of the financial and economic security system of business entities. *Український журнал прикладної економіки та техніки*. 2023. Том. 8. № 3. С. 70-77.

6. Помогалова Н. В., Полозова О. О. Роль баз даних у забезпеченні фінансової безпеки підприємства. Функціонування соціально-економічних систем в контексті цілей сталого розвитку: колективна монографія / За заг. ред. д.е.н., проф. Т. В. Полозової. Харків: ХНУРЕ, 2023. С. 361-369.

7. Мунько А. Ю. Кібербезпека як складник політики фінансової безпеки держави. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування*. 2023. (7). https://doi.org/10.54929/2786-5746-2023-7-02-09

8. Polozova T., Sheiko I. Role of Ukraine integration into EU and NATO for supporting economic development and national security. *Baltic Rim Economies*. 2024. ISSUE # 1. 24.02.2024. p. 43.