інтегруватись у глобальний ринок як технологічно розвинений і надійний партнер.

Список використаних джерел

1. Korzachenko, O., & Ostapenko, V. (2023). Automation of the processes of the energy sector of Ukraine: current status, prospects and challenges. *Modeling and Information System in Economics, 103*, 117-136. http://doi.org/10.33111/mise.103.10

2. *Цифровізація енергетики: як технології Smart Grid допоможуть відбудувати українські енергомережі*. (2024). Mind.ua. https://mind.ua/publications/20273149-cifrovizaciya-energetiki-yak-tehnologiyi-smart-grid-dopomozhut-vidbuduvati-ukrayinski-energomerezhi

Кучмійова Т. С.,
кандидат економічних наук, доцент,
Орешко А. Ф.,
здобувачка першого (бакалаврського) рівня вищої освіти,
Миколаївський національний аграрний університет

КІБЕРРИЗИКИ У ФІНАНСОВОМУ СЕКТОРІ: ЗАПОБІГАННЯ ТА КОНТРОЛЬ

У сучасну епоху цифрової трансформації фінансовий сектор активно інтегрується в електронне середовище. Це відкриває нові можливості для автоматизації операцій, прискорення транзакцій і покращення клієнтського сервісу. Проте водночас цифровізація створює й нові виклики – особливо у сфері інформаційної безпеки. Фінансові установи стають однією з основних цілей для кіберзлочинців через високу вартість інформації та значні обсяги коштів, якими вони оперують. Зростання кількості та складності атак на банки, страхові компанії й платіжні сервіси свідчить про актуальність проблеми кіберзагроз і необхідність системного підходу до їх подолання.

Кіберризики у фінансовому середовищі – це сукупність загроз, що виникають унаслідок використання цифрових технологій і можуть призводити до порушення конфіденційності, втрати доступу до даних, збоїв у роботі систем або фінансових втрат. Їх небезпека посилюється специфікою галузі, де навіть

короткочасна втрата контролю над даними чи операціями може призвести до серйозних наслідків. Ці ризики класифікують за кількома напрямами, залежно від джерел походження та методів впливу.

По-перше, зовнішні кіберзагрози, які переважно здійснюються хакерами або організованими злочинними групами. Серед поширених методів – фішингові кампанії, DDoS-атаки та впровадження шкідливого програмного забезпечення (віруси, трояни, кейлогери).

По-друге, внутрішні загрози, пов’язані з людським фактором. Це можуть бути як навмисні дії персоналу (витік або крадіжка даних), так і ненавмисні помилки (відкриття шкідливих файлів, порушення процедур безпеки).

По-третє, технологічні ризики – наслідок вразливостей у самій ІТ-інфраструктурі: застаріле ПЗ, недоліки в системах автентифікації, порушення у процесах резервного копіювання.

Окрему категорію становлять ризики, пов’язані з використанням послуг третіх сторін. Партнери, хмарні провайдери чи постачальники програмного забезпечення можуть стати джерелом витоків або порушень, якщо не дотримуються стандартів кібербезпеки.

Зростання впливу інновацій також породжує нові виклики. Використання штучного інтелекту або потенційна поява квантових обчислень змінює характер загроз, даючи зловмисникам доступ до нових інструментів маніпуляцій і зламів.

Для протидії таким загрозам фінансові установи мають впроваджувати комплексні заходи кіберзахисту. Вони включають:

- інформаційну політику та навчання персоналу (політики безпеки, тренінги, симуляції атак);
- технічні засоби захисту, такі як багатофакторна автентифікація, шифрування, SIEM-системи та регулярне оновлення програмного забезпечення;
- управління ризиками: аудит, аналіз загроз, розробка планів реагування на інциденти;
- контроль за підрядниками та партнерами, включаючи вимоги безпеки в договорах;

- використання новітніх технологій: AI для аналізу транзакцій, блокчейн для прозорості, кібербезпека як сервіс;
- дотримання регуляторних вимог, як-от GDPR, ISO/IEC 27001, PCI DSS, DORA, та співпраця з відповідними державними органами [2].

Отже, посилення кіберзахисту у фінансовому секторі є не лише питанням технологічної модернізації, а й критично важливою умовою стабільного функціонування установ, збереження довіри клієнтів та захисту економічної безпеки держави. Успішна протидія кіберзагрозам потребує системного підходу, в якому поєднуються технічні, організаційні та регуляторні інструменти.

Список використаних джерел

1. Гончаренко, І. (2023). Кіберзагрози фінансового сектора в умовах війни. *Економіка та суспільство*. https://doi.org/10.32782/2524-0072/2023-50-82

2. Єфремова, К. (2024). Технології цифрової економіки та фінансова безпека. *Право та інновації*, *2*(42), 7-11. https://doi.org/10.37772/2518-1718-2023-2(42)-1

3. Приходько, Б. (2025). Кіберризики фінансового сектору в умовах цифрової трансформації. *Herald of Khmelnytskyi National University. Economic Sciences*, *340*(20), 125-139. https://doi.org/10.31891/2307-5740-2025-340-20

Лазарєва С.Ф.,
к.е.н, доцент,
Марченко М.О.,
здобувач другого (магістерського) рівня вищої освіти,
Київський національний економічний університет ім. В. Гетьмана

ВИКОРИСТАННЯ СМАРТ-ТЕХНОЛОГІЙ В ГАЛУЗІ МЕДІА ДЛЯ ПРИЙНЯТТЯ УПРАВЛІНСЬКИХ РІШЕНЬ В ЦИФРОВУ ДОБУ

Сучасний етап цифровізації висуває нові вимоги до системи прийняття управлінських рішень, особливо в медіа-сфері. Високі темпи зміни технологій, мультиплатформеність, інтеграція каналів комунікації та перехід до