2. Vernekar S., Gupta A. & Chavan G. A Conceptual Study of Marketing Techniques in the Financial Inclusion of Industry 4.0. *International Journal of Advance Research and Innovation*. 2023. Vol.11(2). P. 1-6. https://doi.org/10.51976/ijari.1122301.

3. Соболевська Л. Маніфест щодо переходу України до Індустрії 5.0. Український кластерний Альянс. 03 лип. 2023. URL: https://www.clusters.org.ua/blog-single/manifest-perehid-ua-industry5-0 (дата звернення 08.01.2025).

4. Вовченко О. С. Фінансова інклюзія як інструмент забезпечення фінансової стабільності банків. *Grail of Science*. 2022. № 12-13. С. 94-95. https://doi.org/10.36074/grail-ofscience.29.04.2022.011.

Євтушенко В. С.

здобувач вищої освіти першого (бакалаврського) рівня зі спеціальності

072 «Фінанси, банківська справа та страхування»

Науковий керівник: Кучеркова С. О.

к.е.н., доцент кафедри фінансів, обліку і оподаткування

Таврійський державний агротехнологічний університет

імені Дмитра Моторного

м. Запоріжжя, Україна

КІБЕРБЕЗПЕКА У ПРОЦЕСАХ ДІДЖИТАЛІЗАЦІЇ ФІНАНСОВОГО СЕКТОРУ

У сучасних умовах глобальної цифрової трансформації фінансовий сектор зазнає суттєвих змін, зумовлених активним впровадженням новітніх технологій. Діджиталізація відкриває широкі можливості для підвищення ефективності банківських операцій, розширення спектра фінансових послуг, підвищення їхньої доступності для споживачів та оптимізації бізнес-процесів. Онлайн-банкінг, мобільні додатки, платіжні системи, технології блокчейн та штучного інтелекту стали невід’ємною складовою сучасної фінансової системи. Однак разом із

позитивними змінами цифровізація фінансового сектору супроводжується зростанням кіберзагроз, які можуть мати катастрофічні наслідки як для окремих фінансових установ, так і для економіки загалом.

Фінансові установи є одними з найбільш привабливих цілей для кіберзлочинців через значні обсяги обробки персональних даних, фінансових транзакцій та конфіденційної інформації. Основними видами загроз є:

Фішингові атаки – шахрайські спроби отримати конфіденційну інформацію шляхом обману користувачів;

DDoS-атаки – масові атаки на сервери фінансових установ, що призводять до їхньої недоступності;

Шкідливе програмне забезпечення – зокрема, програми-шифрувальники та трояни, які проникають у системи та викрадають дані;

Інсайдерські загрози – дії співробітників або підрядників, які можуть становити загрозу для безпеки організації;

Атаки на хмарні сервіси – зростаюча загроза, зумовлена збільшенням використання віддалених серверів для зберігання та обробки даних.

Особливу актуальність ця проблема набуває в умовах активної інтеграції України до європейського фінансового простору, що передбачає необхідність дотримання міжнародних стандартів у сфері кібербезпеки, зокрема рекомендацій NIST (National Institute of Standards and Technology), ISO 27001 та положень Регламенту ЄС про захист персональних даних (GDPR).

Держава відіграє ключову роль у забезпеченні кібербезпеки у фінансовому секторі, розробляючи нормативно-правову базу, що регулює діяльність фінансових установ. У цьому контексті важливими є законодавчі ініціативи щодо захисту персональних даних, кібергігієни та протидії кібератакам. Національний банк України, зокрема, впроваджує вимоги до фінансових установ щодо посилення кібербезпеки, зокрема через впровадження стандартів ISO/IEC 27001.

Деякі з найбільш ефективних методів виявлення кіберзагроз у фінансовому секторі включають наступні [1, с. 36]:

1. Моніторинг мережі – системи моніторингу мережі, щоб відстежувати та аналізувати відправлення та отримання даних. Ці системи можуть виявляти незвичайну активність у мережі, яка може означати, що зловмисники намагаються виконати атаку.

2. Використання аналізу поведінки – використання аналізу поведінки, з метою виявлення незвичайних змін у роботі систем і користувачів. Ці системи можуть виявляти незвичайну активність у проміжку часу та надавати спеціалістам з кібербезпеки сповіщення про підозрілі активності.

3. Управління журналами подій – збір та зберігання журналу подій, щоб мати можливість вивчити що сталось, якщо відбулася атака. Ці журнали містять детальну інформацію про дії користувачів та систем в режимі реального часу, і вони можуть виявити підозрілі дії.

4. Здійснення регулярних тестів на проникнення. Ці тести можуть допомогти виявляти слабкі місця в системі та узгоджувати плани дій на випадок атак.

5. Використання штучного інтелекту.

Одним із ключових аспектів стратегії кіберзахисту є формування культури кібербезпеки серед працівників фінансового сектору та користувачів послуг. За оцінками експертів, більшість кібератак відбувається через людський фактор. Впровадження програм навчання, регулярне підвищення обізнаності персоналу та використання багаторівневих механізмів аутентифікації допомагають зменшити ризики атак.

Кібербезпека – це важливий складник національної безпеки – система стандартів, правил, процедур та відповідальності як держави, так і бізнесу. Діджиталізація бізнес-процесів та системи державного управління – це метод протидії корупційним ризикам, водночас це додаткові кіберризики. І тут повинна бути системна відповідальність і держави, і бізнесу, і громадянського суспільства загалом. Адже на думку експертів в ІТ-галузі від 90% кібератак захиститися можна, якщо не безкоштовно, то дуже малими витратами, оскільки їх левову частку спрямовано на користувача. Тобто формування культури кібербезпеки – це основний елемент стратегії будь-якої організації фінансового сектору [2, с. 54].

Список використаних джерел

1. Гончаренко І. Г. Кіберзагрози фінансового сектора в умовах війни. *Економіка та суспільство* 2023 № 50. С. 34-42 URL: https://economyandsociety.in.ua/index.php/journal/article/view/2442/2362 (дата звернення 09.01.2025).

2. Дорош І. М. Кібербезпека та її роль у фінансовому секторі: загрози та заходи захисту. *Economics. Finances. Law.* 2023. № 10 с.49-56 URL: http://efp.in.ua/uk/journal-article/1169 (дата звернення 09.01.2025).

Івахно П. В.
аспірант кафедри обліку і фінансів
Національний технічний університет
«Харківський політехнічний інститут»
м. Харків, Україна

BIG DATA ТА ШТУЧНИЙ ІНТЕЛЕКТ У ПРОЦЕСІ ОЦІНКИ DEFI-ПРОЕКТІВ

Сучасні децентралізовані фінанси (DeFi) зазнають значних трансформацій під впливом новітніх цифрових технологій, зокрема Big Data та штучного інтелекту (AI). Використання цих технологій створює можливості для поглибленого аналізу ринкових процесів, підвищення точності прогнозів та мінімізації інвестиційних ризиків. Зважаючи на високу динаміку DeFi-екосистеми та її значну волатильність, питання коректної оцінки вартості проєктів є критично важливим для інвесторів, аналітиків та розробників фінансових продуктів. У даній роботі проводиться аналіз основних механізмів застосування технологій Big Data та AI у процесі оцінки DeFi-проектів, визначаються ключові виклики та перспективи їх впровадження в сучасну економічну реальність.