Література

1. Національний банк України. Огляд банківського сектору. 2024, листопад. URL: https://bank.gov.ua/ua/news/all/oglyad-bankivskogo-sektoru-listopad-2024-roku.
2. Національний банк України. Звіт про фінансову стабільність. 2024, червень. URL: https://bank.gov.ua/ua/news/all/zvit-pro-finansovu-stabilnist-cherven-2024-roku.
3. Національний банк України. Статистика фінансового сектора. Грошово-кредитна статистика. URL: https://bank.gov.ua/ua/statistic/sector-financial#1ms.
4. ФРП. Інформація про результати державної програми доступні кредити 5-7-9. URL: https://bdf.gov.ua/publichna-informatsiia/informatsiia-pro-rezultaty-derzhavnoi-prohramy-dostupni-kredyty-5-7-9/.

УДК 336.711

Худолій Юлія Сергіївна,
кандидат економічних наук, доцент
Андрієць Тетяна Романівна, *магістрантка*
Національний університет «Полтавська політехніка імені Юрія Кондратюка» (Україна)

ІНФОРМАЦІЙНА БЕЗПЕКА ВІТЧИЗНЯНИХ БАНКІВ: ВИКЛИКИ ТА МАЙБУТНІ РІШЕННЯ

Зростання кількості кібератак унаслідок політичної нестабільності та воєнного стану призвело до збільшення тиску на банківські установи. У 2022 році майже всі кібератаки були спровоковані хакерськими угрупуваннями, що працюють на рф. Основними напрямками стали фішингові та DDoS атаки. У відповідь на це українські банки активізують свої зусилля в напрямку впровадження багаторівневих ступенів захисту, таких як використання шифрування, багатофакторної аутентифікації та сучасних систем моніторингу.

Безпеку банку визначають як стан життєдіяльності при якому забезпечується реалізація основних інтересів та пріоритетних цілей банку, захист від зовнішніх і внутрішніх дестабілізуючих факторів [1].

Важливо визначити ключові виклики для банківських установ у сфері інформаційної безпеки та ефективні шляхи для їх подолання. Основними викликами інформаційної безпеки банківської системи є кібератаки, захист персональних даних клієнтів, нестача кваліфікованих фахівців, інтеграція новітніх технологій, впровадження системи автоматизації та штучного інтелекту, управління хмарною безпекою та інші.

Також виклики можна класифікувати як:

1) технологічні виклики (застаріла інфраструктура та відсутність сучасного кіберзахисту, використання вразливих систем);

2) соціальні виклики (людський фактор та фішингові атаки);

3) організаційні виклики (складність інтеграції новітніх систем захисту, брак фінансування на забезпечення інформаційної безпеки).

Майбутні рішення у сфері інформаційної безпеки українських банків повинні включати комплексний підхід. У сфері технологічних інновацій важливим є впровадження рішень на основі ШІ та машинного навчання, що допоможе виявляти аномалії та миттєво реагувати на загрози. Використання багатофакторної аутентифікації для доступу до систем, шифрування даних, технології блокчейну для захисту транзакцій та інші передові технології допоможуть зміцнити рівень інформаційної безпеки. Активний розвиток системи моніторингу та реагування на інциденти в реальному часі допоможуть протидіяти інформаційним загрозам та мінімізувати їх наслідки.

Отже, забезпечення інформаційної безпеки в банківському секторі України вимагає комплексного підходу, що включає в себе впровадження сучасних технологій, підвищення інформаційно грамотності населення та адаптацію до нових викликів у кіберсфері.

Література

1. Ахрамович В.М., Чегренець В.М. Управління ризиками інформаційної безпеки комерційного банку. *Сучасний захист інформації*. 2019. №2. С. 54-59.
2. Yehorycheva S., Hlushko A., Khudolii Y. Issue of Ukrainian financial sector information security. *Development Management.* 2023. №22(4). P. 45-52.
3. Onyshchenko S., Yanko A., Hlushko A., Maslii O., Cherviak A. Cybersecurity and improvement of the information security system. Journal of the Balkan Tribological Association. 2023. 29(5). pp. 818–835.
4. Onyshchenko, S., Yanko, A., Hlushko, A., Maslii, O., Skryl, V. (2023). The Mechanism of Information Security of the National Economy in Cyberspace. Proceedings of the 4th International Conference on Building Innovations, 791–803. doi: https://doi.org/ 10.1007/978-3-031-17385-1_67