Вовченко Оксана,
канд. екон. наук, доцент,
Національний університет «Полтавська політехніка
імені Юрія Кондратюка»

КІБЕРБЕЗПЕКА ЯК СУЧАСНИЙ ТРЕНД РОЗВИТКУ БАНКІВСЬКОЇ СИСТЕМИ УКРАЇНИ

Ключові слова: кібербезпека, кібератака, кіберзагроза, фінтех, фішинг, фінансові втрати, репутаційні ризики.

Oksana Vovchenko,
PhD, Associate Professor,
National University «Yuri Kondratyuk Poltava Polytechnic»

CYBERSECURITY AS A MODERN DEVELOPMENT TREND OF THE BANKING SYSTEM OF UKRAINE

Key words: cybersecurity, cyberattack, cyberthreat, fintech, phishing, financial losses, reputational risks.

В сучасному динамічному світі, де передові фінансові інновації та технології розвиваються в геометричній прогресії, питання кібербезпеки набуває надзвичайно важливого значення. Це особливо стосується банківської системи, яка є одним із ключових елементів фінансової інфраструктури будь-якої країни. Застосування fintech у банківській сфері, враховуючи тренди та перспективи фінтех-галузі, забезпечує вищий рівень обслуговування клієнтів і полегшує доступ до фінансової інформації, проте значно розширює спектр кіберзагроз. Збільшення кількості та складності кібератак, зростання залежності від онлайн-банкінгу та повномасштабна війна в країні, а також зростання фінансових втрат від перелічених чинників, роблять захист банківських систем від кіберзлочинців все більш складним завданням.

Негативний вплив на функціонування банківської системи не лише через фінансові втрати, але й через збільшення репутаційних збитків має витік інформації. Згідно з даними компанії IBM [1], середня вартість витоку даних досягла максимуму у 2023 році та становила 4,45 млн доларів (рис. 1). У порівнянні з 2022 роком, коли вартість витоку була 4,35 млн доларів США, показник збільшився на 2,3%.

Варто відмітити, що інтенсивність кібератак (яка оцінюється European Repository of Cyber Incidents (EuRepoC) за шкалою від 1 до 15 балів, виходячи з фактичних наслідків та соціально-політичної серйозності кіберінциденту), в Україні за 2023 рік зросла до показника 2,76 [2].

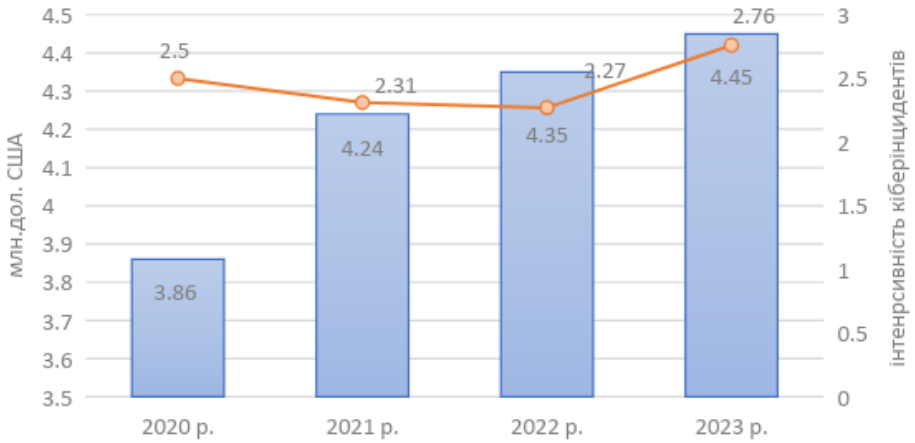

Рис. 1. Динаміка вартості витоку даних та інтенсивності кібератак протягом 2020-2023 років.

Джерело: побудовано автором за даними [1, 2].

Тож до основних кіберзагроз, з якими постійно стикаються українські банки варто віднести:

1. Фішингові атаки – надсилання шахраями електронних листів або текстових повідомлень, що маскуються під повідомлення від легітимних організацій, щоб отримати доступ до конфіденційної інформації клієнтів.
2. Malware – зловмисне програмне забезпечення, яке може бути використано для крадіжки даних, пошкодження систем або вимагання викупу, та поширюється через електронну пошту, веб-сайти або заражені USB-накопичувачі.
3. DDoS-атаки – атаки через бот-мережі чи програмні застосунки, що проявляються у відмові в обслуговуванні та можуть призвести до того, що банківські платіжні системи стають недоступними для клієнтів.

Серед найсучасніших методів кібератак виділяють атаки на ланцюг постачання, атаки з використанням штучного інтелекту, квантові обчислення та атаки на метавсесвіт. У 2023 році наймасштабнішими кібератаками на українські банки, стали атака на метавсесвіт, яка була здійснена на «ПУМБ» та призвела до втрати віртуальних активів банку і його клієнтів; а також DDoS-атака на сервіси «Monobank» із одночасним навантаженням 580 млн запитів [3]. Результатом таких атак можуть бути як прямі фінансові втрати, так і зменшення довіри до безпеки банківської системи, погіршення клієнтського досвіду.

Інтенсивність та різноманіття кібератак вказують на необхідність постійного удосконалення заходів та навичок кібербезпеки. Ще у 2018 році Європейський центральний банк опублікував важливий документ «Очікування щодо нагляду за кіберстійкістю» (CROE) [4], який швидко став головним ресурсом для операторів фінансової інфраструктури в Європі. Цей документ містить рекомендації та очікування відносно забезпечення кіберстійкості в фінансовому секторі. Основні аспекти CROE в банківських установах спрямовані на:

- наявність чіткої стратегії кібербезпеки, яка повинна бути інтегрованою з загальною стратегією та ризик-менеджментом;
- відповідальність керівництва банку за кібербезпеку;

- регулярне проведення та оцінка кіберризиків, щоб виявити та оцінити потенційні загрози, вразливості та впливи;
- впровадження технічних, організаційних та фізичних заходів захисту для зменшення кіберризиків (брендмауери, системи виявлення вторгнень, шифрування, навчання персоналу, контроль доступу, захист даних);
- постійний моніторинг банківських систем на предмет кіберзагроз та інцидентів, а також наявність планів реагування на випадок кібератак;
- регулярне тестування систем кібербезпеки та навчання персоналу щодо кіберзагроз та методів захисту;
- розробка чіткого плану комунікації з регуляторами, клієнтами та іншими зацікавленими сторонами у випадку кіберінцидентів.

Отже, кібербезпека є одним із найважливіших викликів, з якими стикається банківська система України сьогодні. Впровадження комплексного підходу до кібербезпеки, використання передових європейських практик та державна підтримка розвитку кібербезпеки в Україні – це ключові фактори, які допоможуть захистити банківську систему від кібератак та забезпечити стійкість та безпеку фінансового сектору країни.

Список використаних джерел:

1. Cost of a Data Breach Report. *IBM Security*. URL: https://www.ibm.com/downloads/cas/E3G5JMBP (дата звернення: 18.04.2024).

2. Overview of cyber incidents against Ukraine between 01-01-2020 and 01-01-2023. *European Repository of Cyber Incidents (EuRepoC).* URL: https://www.swp-berlin.org/en/swp/about-us/organization/swp-projects/european-repository-on-cyber-incidents-eurepoc (дата звернення: 18.04.2024).

3. Балашова Л., Калашник П. Monobank пережив масштабну DDoS-атаку із навантаженням 580 млн запитів. Хакери майже два роки постійно атакують українські банки. Як це впливає на їхній бізнес. *Forbes Ukraine.* 2023. URL: https://forbes.ua/innovations/tse-prosto-kosmos-monobank-perezhiv-masshtabnu-ddos-ataku-iz-navantazhennyam-580-mln-zapitiv-yak-podibni-ataki-vplivayut-na-biznes-22012024-18687 (дата звернення: 18.04.2024).

4. Cyber resilience oversight expectations for financial market infrastructures. European Central Bank. 2018. URL: https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf (дата звернення: 18.04.2024).