

Секція 5. Сучасні тенденції, проблеми та перспективи розвитку фінансової системи

УДК 336.71:004.056

Боднар Олена Андріївна

*к. е. н., доцентка кафедри фінансів, банківської справи та страхування,
Миколаївський національний аграрний університет (Україна)*

Крижова Вікторія Андріївна

*здобувачка вищої освіти спеціальності 071 Облік і оподаткування,
Миколаївський національний аграрний університет (Україна)*

КІБЕРРИЗИКИ ТА ФІНАНСОВА БЕЗПЕКА БАНКІВСЬКОЇ СИСТЕМИ УКРАЇНИ

JEL classification: G210; G220; G290; E440

У сучасних умовах цифровізації фінансового сектору питання кіберризиків та фінансової безпеки набуває особливої важливості для банківської системи України. Зростаюча кількість кібератак, шахрайських схем та загроз інформаційній безпеці може спричинити значні фінансові втрати та підірвати довіру клієнтів до банківських установ.

Особливо актуальним це питання стає в умовах воєнного стану, коли фінансова система України піддається додатковим ризикам, зокрема хакерським атакам, спробам несанкціонованого доступу до даних та фінансовій дестабілізації.

Забезпечення надійного захисту банківських систем, впровадження сучасних кібербезпекових технологій та розробка ефективних механізмів протидії кіберзагрозам є ключовими завданнями для стабільного функціонування банківського сектору. Тому дослідження кіберризиків та фінансової безпеки є надзвичайно важливим для збереження стійкості економіки та фінансової стабільності України.

Проблема фінансової безпеки банківської системи була завжди актуальною. Цій темі присвячено велику кількість досліджень, серед яких можна назвати таких науковців як О. Амосов, Н. Кравчук, О. Барановський, Л. Фахівець, О. Хитрін, В. Коваленко, Є. Мордань.

Кіберризики в банківській системі України є серйозною загрозою, яка може призвести до фінансових втрат, витоку конфіденційної інформації, підірвати довіру клієнтів та дестабілізувати фінансову систему. У сучасних умовах цифровізації банківських послуг ризики кіберзлочинності суттєво зростають, особливо на тлі воєнного стану та активізації хакерських атак на українські фінансові установи.

Одним із найбільш поширених кіберризиків є хакерські атаки на банківські системи, включаючи DDoS-атаки, які викликають збої в онлайн-банкінгу, та викрадення персональних даних через злом баз даних. Зловмисники також використовують шифрувальне програмне забезпечення (ransomware), блокуючи доступ до даних і вимагаючи викуп.

Фішинг і соціальна інженерія становлять ще одну загрозу: кіберзлочинці підробляють сайти та електронні листи для викрадення логінів і паролів, а також маніпулюють співробітниками банків для отримання несанкціонованого доступу. Шахрайство в електронних платежах включає використання скомпрометованих карток, незаконне втручання в платіжні системи та підробку транзакцій, зокрема махінації з криптовалютами. Внутрішні загрози та витік інформації можуть виникнути через недобросовісних працівників або низький рівень кіберграмотності. Вразливості у програмному забезпеченні також можуть бути використані для атак.

Атаки на фінансову інфраструктуру, такі як злом банкоматів і POS-терміналів, дозволяють злочинцям отримувати доступ до карток клієнтів і маніпулювати міжбанківськими платежами, зокрема у системі SWIFT. Банки зобов'язані детально відстежувати потенційні загрози та ризики [1]. При цьому необхідно чітко розрізняти об'єкти таких кібератак. Якщо згрупувати найбільш типові кібератаки на банківський сектор, можна виділити наступні елементи атаки: конфіденційна чи банківська таємниця; банківська інфраструктура; кошти клієнтів і банку; веб-сайти банків і регуляторів [2].

Безпека банківської системи визначає рівень захищеності кредитно-фінансових відносин, що забезпечує стійке функціонування банків та фінансову стабільність в Україні. Вона гарантує захист життєво важливих фінансових інтересів держави, суспільства та особи, зменшуючи наслідки зовнішніх і внутрішніх загроз.

Фінансова безпека є ключовою для економічної стабільності країни, забезпечуючи захист банків від загроз і їх стійкість до криз. У умовах війни ця проблема стає особливо актуальною, адже банки підтримують платіжну систему, бізнес і кредитування населення. Основними загрозами є: економічна нестабільність, висока інфляція, девальвація валюти та кредитні ризики, пов'язані зі зниженням платоспроможності населення.

Недостатня капіталізація банків також є проблемою, оскільки війна потребує додаткових фінансових впливів для забезпечення ліквідності. Зовнішні чинники, пов'язані з війною, такі як руйнування інфраструктури та блокування міжнародних операцій, створюють серйозні виклики для стабільності фінансової системи. Для підвищення фінансової безпеки необхідно посилити державне регулювання та нагляд за банками, впроваджуючи жорсткіші вимоги до капіталізації, ліквідності та ризик-менеджменту.

Значним кроком у кіберзахисті банківської системи національним регулятором стала розробка вимог до функціонування системи кіберзахисту в банківській системі України, актуалізація для банків критеріїв та порядку віднесення до об'єктів критичної інформаційної інфраструктури. Ці норми містить постанова Правління Національного банку України № 178 від 12 серпня 2022 року «Про затвердження Положення про організацію кіберзахисту в банківській системі України та внесення змін до Положення про визначення об'єктів критичної інфраструктури в банківській системі України» [3].

Важливим напрямом є зміцнення фінансової стійкості банків шляхом залучення додаткових резервів, міжнародної фінансової підтримки та реформування банківського сектору. Також необхідно інвестувати у цифрові технології та вдосконалювати системи кібербезпеки для запобігання кіберзагрозам та фінансовому шахрайству.

Серед проблем захисту банківської діяльності від зовнішніх та внутрішніх загроз стає все більш актуальною необхідність забезпечити захист фінансових ресурсів, інформації та майна банків [4].

Отже, фінансова безпека банківської системи України є ключовим фактором стабільного розвитку економіки, і для її забезпечення необхідно впроваджувати ефективні механізми управління ризиками, зміцнювати фінансову стійкість банків та посилювати державний контроль у сфері кібербезпеки. Успішна протидія кіберризикам потребує комплексного підходу, запровадження європейських стандартів безпеки, співпраці з міжнародними організаціями та постійного вдосконалення методів захисту.

Література

1. Sirenko N., Dubinina M., Melnyk O., Bodnar O., Luhova, O. Current Status and Regulation of the Digital Money Market in Ukraine. *Economic Affairs*. 2023. Vol. 68 (Special Issue). Pp. 955–961. DOI: <https://doi.org/10.46852/0424-2513.2s.2023.44>.
2. Forcadell F. J., Aracil E., & Úbeda F. The Impact of Corporate Sustainability and Digitalization on International Banks' Performance. *Global Policy*. 2020. Vol. 11 (S1). Pp. 18–27. DOI: <https://doi.org/10.1111/1758-5899.12761>.
3. Про затвердження Положення про організацію кіберзахисту в банківській системі України та внесення змін до Положення про визначення об'єктів критичної інфраструктури в банківській системі України : Постанова Правління Національного банку України № 178 від 12.08.2022 р. URL: https://bank.gov.ua/ua/legislation/Resolution_12082022_178 (дата звернення: 31.03.2025).
4. Мартинюк О. Analysis of the level of financial security of commercial banks. *Modern Engineering and Innovative Technologies*. 2023. Vol. 4 (25–04). Pp. 53–61. DOI: <https://doi.org/10.30890/2567-5273.2023-25-04-058>.