УДК 336.71:004.056

Вишивана Б. М.
канд. екон. наук, доцент кафедри фінансів, грошового обігу і кредиту Львівського національного університету імені Івана Франка

КІБЕРБЕЗПЕКА КРЕДИТНОЇ СИСТЕМИ УКРАЇНИ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

Вступ. Із поглибленням інтеграції кредитної системи в цифровий простір зростає її вразливість до кіберзагроз. Збільшення обсягів обробки персональних і фінансових даних, а також активне впровадження інформаційно-комунікаційних технологій у всі сфери суспільного життя зумовлюють необхідність формування ефективної системи кіберзахисту. Це питання набуває особливої актуальності в умовах гібридних загроз, коли кібератаки використовують як інструмент впливу на критичну інфраструктуру держави. Відтак забезпечення кібербезпеки є пріоритетним завданням, що потребує скоординованих дій з боку держави, бізнесу та громадянського суспільства.

Метою роботи є обґрунтування пріоритетних напрямів кіберзахисту кредитної системи України в умовах цифровізації на основі аналізу сучасних загроз та визначення інституційної ролі Центру кіберзахисту Національного банку України у забезпеченні фінансової безпеки держави.

Основна частина. Відповідно до положень українського законодавства, кібербезпека – це захищеність життєво важливих інтересів людини та громадянина, суспільства і держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, а також своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [1].

Кредитна система України особливо вразлива до низки кіберзагроз, серед яких варто виокремити [2–4]:

– фішингові атаки та інші методи соціальної інженерії – найпоширеніший тип кібершахрайства, спрямований на викрадення облікових даних клієнтів фінансових установ через підроблені вебсайти, електронні листи або повідомлення. Зловмисники імітують офіційні сервіси банків для отримання доступу до рахунків або персональної інформації;

– DDoS-атаки – атаки, що мають на меті перевантажити банківські сервери, внаслідок чого тимчасово припиняється робота онлайн-банкінгу, мобільних застосунків або платіжних систем. Їх часто застосовують як інструмент дестабілізації або відволікання уваги під час реалізації складніших кібератак;

– використання шкідливого програмного забезпечення – для викрадення облікових даних, блокування доступу до інформаційних систем із подальшим вимаганням викупу, а також для проведення несанкціонованих фінансових операцій;

– цілеспрямовані атаки з боку державних або організованих злочинних угруповань – складні, тривалі кібероперації, спрямовані на отримання несанкціонованого доступу до критичної фінансової інфраструктури, викрадення конфіденційної інформації або дестабілізацію фінансової системи. Такі атаки часто проводять

за підтримки іноземних спецслужб у межах гібридної війни або з боку висококваліфікованих кіберзлочинців.

Центр кіберзахисту Національного банку України відіграє важливу роль в інституційній моделі забезпечення кібербезпеки у фінансовому секторі. Його створено для координації заходів із захисту банківських і небанківських фінансових установ від кіберзагроз та забезпечення стабільного функціонування цифрової інфраструктури. Найважливіші завдання Центру кіберзахисту Національного банку України такі [5]:

– моніторинг, виявлення та реагування на кіберінциденти, а також збір, накопичення й аналіз відповідних даних у фінансовому секторі;

– аналіз сучасних кіберзагроз, вивчення зразків шкідливого програмного забезпечення, формування індикаторів компрометації та розроблення рекомендацій щодо протидії;

– оперативне інформування суб'єктів кіберзахисту про зафіксовані спроби кібератак, оприлюднення індикаторів кіберзагроз;

– надання консультативної підтримки установам фінансового сектору з питань організації кіберзахисту, реагування на кіберінциденти, усунення їх наслідків і запобігання подібним загрозам у майбутньому;

– розроблення рекомендацій щодо побудови ефективної системи кіберзахисту;

– співпраця з міжнародними організаціями та обмін інформацією з довіреними зовнішніми джерелами в межах реагування на кібератаки та забезпечення кіберстійкості фінансової системи.

Висновки. Ефективна система кіберзахисту має ґрунтуватися на сучасних технологіях, належному нормативно-правовому регулюванні, міжвідомчій координації та постійному підвищенні кваліфікації персоналу. Стабільне функціонування банківської інфраструктури в умовах цифрової економіки можливе лише за умови високого рівня кібербезпеки, що відповідає сучасним викликам.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII зі змінами. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 21.04.2026).

2. Трусова Н. В., Чкан І. О. Кіберзахист банківської системи України в умовах цифрових трансформацій. *Збірник наукових праць ТДАТУ імені Дмитра Моторного (економічні науки).* 2023. № 1(47). С. 151–163.

3. ENISA Threat Landscape: Finance Sector. January 2023 To June 2024. European Union Agency for Cybersecurity. URL: https://www.enisa.europa.eu/sites/default/files/202502/Finance%20TL%202024_Final.pdf (дата звернення: 21.04.2026).

4. Річний аналітичний огляд: ключові події, тенденції та виклики у сфері кібербезпеки у 2024 р. Рада національної безпеки і оборони України. URL: https://www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/20250109/Year%20in%20review_UKR_upd.pdf (дата звернення: 21.04.2026).

5. Центр кіберзахисту Національного банку України. Офіційна інтернет-сторінка. URL: https://cyber.bank.gov.ua/ (дата звернення: 21.04.2026).