УДК 336.7:004.056

Апацький В.В., здобувач третього (освітньо-наукового) рівня вищої освіти
Тарасенко І.О., д.е.н., професор
Київський національний університет технологій та дизайну, м. Київ, Україна

ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ БАНКІВСЬКОГО СЕКТОРУ В УМОВАХ ВОЄННИХ ЗАГРОЗ ТА НЕВИЗНАЧЕНОСТІ

Сучасний етап розвитку банківської системи України характеризується стрімкою цифровізацією фінансових послуг, розширенням дистанційного та упровадженням технологій відкритого банкінгу, стрімким зростанням обсягів обробки персональних даних. Водночас повномасштабна війна з боку російської федерації проти України призвела до безпрецедентного загострення кіберзагроз, спрямованих на підрив стабільності фінансового сектору та дестабілізацію національної економіки (фішингові атаки, несанкціонований доступ до внутрішніх інформаційних систем, поширення шкідливого програмного забезпечення, спроби компрометації платіжної інфраструктури і каналів обміну фінансовими даними). Проблема ускладнюється тим, що значна частина банківської ІТ-інфраструктури досі не повністю відповідає сучасним стандартам кіберзахисту, а ризики, пов’язані з використанням хмарних сервісів, інтеграційних платформ і технологій відкритого банкінгу, залишаються недостатньо врегульованими. Попри впровадження Національним банком України низки нормативно-правових актів у сфері кіберзахисту, існує потреба в подальшому вдосконаленні системи управління кіберризиками, зокрема в умовах воєнної невизначеності.

Серед українських вчених, які досліджували проблеми кіберризиків для банківської системи доцільно виокремити праці таких як: Ю. С. Худолій, М. О. Раєвська, Т. Р. Андрієць [1; 2]. Окремої уваги заслуговують наукові праці, присвячені інструментам мінімізації наслідків кібератак [3], в яких розглядаються питання кіберстрахування як інструменту управління кіберризиками у банківському секторі. Аналіз цих праць свідчить, що недостатньо дослідженим залишається комплексний вплив кіберзагроз на діяльність банків в умовах воєнних ризиків та загальної макрофінансової невизначеності, що зумовлює потребу в подальших наукових дослідженнях у цьому напрямі.

За даними Microsoft Digital Defense Report (2025), у першій половині 2025

року Україна посідала п’яте місце у світі та третє в Європі за кількістю кібератак [4, с. 10]. Значна частина інцидентів пов’язана з війною та спрямована на критичну інфраструктуру, державні інформаційні ресурси та фінансовий сектор. Водночас міжнародні дослідження кіберзлочинності відносять Україну до групи країн з підвищеними кіберзагрозами, що зумовлено поєднанням геополітичних факторів і високого рівня цифровізації економіки. За результатами дослідження визначено основні напрями підвищення кіберстійкості банківського сектору України, які представлено з визначенням основних заходів впливу, рівнем реалізації, очікуваними результатами та індикаторами оцінювання (див. табл. 1).

Таблиця 1

Напрями підвищення кіберстійкості банківського сектору України та індикатори оцінювання їх ефективності

Проблеми	Основні заходи впливу	Результат	Індикатори оцінювання
1	2	3	4
Рівень – державний, інституційний			
Зростання кількості кіберінцидентів у банківській системі	Удосконалення нормативної бази, створення системи координації реагування на кіберінциденти, розвиток центрів моніторингу кіберзагроз	Зниження частоти та масштабів кіберінцидентів, підвищення рівня координації між суб’єктами фінансового сектору	Кількість зафіксованих кіберінцидентів; середній час реагування на інцидент; рівень виконання вимог регулятора
Використання програмного забезпечення ризикового походження	Впровадження сертифікованих міжнародних і національних рішень, аудит постачальників ІТ	Зниження ризиків витоку інформації та зовнішнього втручання в банківські системи	Частка використання сертифікованого ПЗ; кількість замінених ризикових систем
Фішингові атаки та соціальна інженерія	Проведення програм кібергігієни, навчання персоналу, інформування клієнтів, багатофакторна автентифікація	Зменшення випадків шахрайства, несанкціонованого доступу до рахунків клієнтів	Частка інцидентів фішингу; кількість скомпрометованих облікових записів; рівень використання MFA
Поширення шкідливого програмного забезпечення	Аудит інформаційної безпеки, управління вразливостями, оновлення ПЗ, впровадження систем EDR/XDR	Підвищення захищеності інформаційних систем банків	Кількість виявлених уразливостей та інцидентів зараження; рівень оновлення систем
DDoS-атаки на банківські сервіси	Використання систем захисту від DDoS-атак та хмарних сервісів кіберзахисту, резервування інфраструктури	Підвищення стабільності роботи онлайн-банкінгу та платіжних систем	Тривалість простоїв сервісів; кількість успішно відбитих атак; доступність онлайн-сервісів (%)
Вразливості мобільного банкінгу	Регулярне тестування безпеки застосунків, впровадження secure-by-design, захист API та багаторівнева автентифікація	Підвищення рівня довіри клієнтів до цифрових банківських сервісів	Кількість виявлених вразливостей й інцидентів у мобільних застосунках; рівень використання захищених протоколів

Продовженяя таблиці 1

1	2	3	4
Рівень – інституційний, технологічний			
Рівень – державний, інституційний, технологічний			
Воєнні ризики для інфраструктури	Розвиток систем резервування дата-центрів, хмарні рішення, реалізація планів безперервності діяльності (BCP) та відновлення (DRP)	Забезпечення безперервності функціонування банків навіть у кризових умовах	Час на відновлення систем; кількість реалізованих планів BCP/DRP; рівень доступності IT-систем
Рівень – технологічний			
Недостатній рівень автоматизації кіберзахисту	Інтеграція технологій штучного інтелекту та машинного навчання у системи моніторингу кіберзагроз	Підвищення швидкості виявлення та нейтралізації кіберзагроз	Середній час виявлення інцидентів; частка автоматично оброблених загроз

Узагальнено авторами на основі [1, 4, 5].

Для фінансової галузі найбільш поширеними залишаються: фішингові кампанії, спрямовані на викрадення облікових даних користувачів систем дистанційного банківського обслуговування; атаки із застосуванням шкідливого програмного забезпечення; атаки типу DDoS; компрометація внутрішніх інформаційних систем через вразливості програмного забезпечення, соціальну інженерію або атаки на ланцюги постачання IT-рішень. Додаткові ризики виникають унаслідок обстрілів енергетичної інфраструктури і перебоїв з електроенергією, що впливає на стабільність роботи дата-центрів, телекомунікаційних мереж і каналів зв'язку. У поєднанні з активною цифровізацією банківських послуг це формує новий рівень кіберризиків, який вимагає від банків України посилення систем управління інформаційною безпекою, впровадження принципів кіберстійкості та постійного моніторингу загроз. Стрімкий розвиток штучного інтелекту також створює нові виклики для українських банків. Тому банківська кібербезпека повинна бути на крок попереду у використанні новітніх інструментів, запроваджуючи їх максимально ефективно та доцільно.

Література

1. М.О. Раєвська, Ю. С. Худолій: Кібербезпека банків України в умовах війни // Економічна безпека: держава, регіон, підприємство : матеріали VIII Міжнар. наук.-практ. конф., 16 трав. 2024 р. – Полтава : Нац. ун-т ім. Юрія Кондратюка, 2024. – С. 51–55.

2. Ю. С. Худолій, Т. Р. Андрієць: Забезпечення кібербезпеки банківської системи України у період воєнного стану // Економічна безпека: держава, регіон, підприємство : матеріали VII Міжнар. наук.-практ. Інтернет-конф., 17 трав. 2023 р., Полтава : Національний університет імені Юрія Кондратюка, 2023 р., с. 58–

61.

3. Рамський А. Ю., Арабаджи: Кіберстрахування в банківському секторі: ідентифікація ризиків та інструменти підтримки безпеки / Науковий вісник міжнародної асоціації науковців / Том 2, №2, 2023, – Київ, Київський університет імені Бориса Грінченка. Режим доступу: https://elibrary.kubg.edu.ua/id/eprint/47091/

4. Microsoft Digital Defense Report 2025 [Електронний ресурс]. Режим доступу: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Microsoft-Digital-Defense-Report-2025.pdf

5. Річний звіт НБУ за 2022 рік – Power Banking [Електронний ресурс]. Режим доступу: https://bank.gov.ua/admin_uploads/article/annual_report_2022.pdf

УДК 336.148

Гавриленко Н.Я., здобувач освіти,
Тарасенко І. О., науковий керівник д.е.н., професор,
Київський національний університет технологій та дизайну, м. Київ, Україна

НАПРЯМИ РОЗВИТКУ ДЕРЖАВНОГО ФІНАНСОВОГО КОНТРОЛЮ В УКРАЇНІ

Державний фінансовий контроль (ДФК) є ключовим елементом системи державного управління, спрямованим на забезпечення законності, ефективності та раціональності використання ресурсів державного бюджету. Його значення особливо яскраво проявилося на тлі економічної нестабільності та інтеграції України до європейського економічного простору [1, 2, 3].

Сутність ДФК полягає в регулюванні формування, розподілу та використання ресурсів державного бюджету з метою виявлення порушень, запобігання зловживанням і підвищення ефективності управління бюджетом. Основною метою ДФК є забезпечення відповідності використання бюджетних ресурсів принципам законності, економії та ефективності. Державна аудиторська служба України (ДАСУ) займає центральне місце в системі державного фінансового контролю. Як центральний орган виконавчої влади, вона відповідає за реалізацію державної політики у цій сфері [5].