Отримано: 26.02.2026 Прийнято: 24.03.2026 Опубліковано: 23.04.2026

УДК 336.71:004.056.5 **DOI: 10.30857/2786-5398.2026.2.1**

УКРАЇНСЬКІ БАНКИ В УМОВАХ ВОЄННИХ РИЗИКІВ, КІБЕРЗАГРОЗ ТА НЕВИЗНАЧЕНОСТІ

АПАЦЬКИЙ ВЛАДИСЛАВ ВІТАЛІЙОВИЧ
аспірант кафедри фінансів,
Київський національний університет технологій та дизайну, Україна
https://orcid.org/0009-0000-8331-6884
vva0919@gmail.com

Анотація. У статті досліджено сучасні виклики кібербезпеки банківської системи України в умовах воєнних ризиків та активної цифровізації фінансових послуг. Проаналізовано основні кіберзагрози для банківського сектору, зокрема фішингові атаки, шкідливе програмне забезпечення, DDoS-атаки, компрометацію інформаційних систем і ризики, пов'язані з використанням програмного забезпечення іноземного походження. Розглянуто нормативно-правове регулювання кіберзахисту банків в Україні та визначено роль Національного банку України у формуванні системи кіберстійкості фінансового сектору. У роботі проаналізовано динаміку кіберінцидентів в Україні у 2020–2025 роках та встановлено тенденцію до їх зростання в умовах воєнного стану. Окрему увагу приділено кіберризикам мобільного банкінгу та вразливостям мобільних фінансових застосунків. Методологічною основою дослідження стали методи порівняльного аналізу, узагальнення, систематизації та статистичної оцінки даних. Обґрунтовано необхідність посилення систем управління кіберризиками, впровадження сучасних підходів до інформаційної безпеки, зокрема концепції secure-by-design, а також поступової відмови від програмного забезпечення, що створює потенційні загрози для банківської інфраструктури. Практичне значення отриманих результатів полягає у можливості їх використання банківськими установами для підвищення рівня кіберзахисту та мінімізації ризиків у процесі цифрової трансформації. Зроблено висновок, що кібербезпека банківського сектору є важливою складовою фінансової стійкості держави в умовах воєнної невизначеності, а підвищення кіберстійкості банків потребує комплексного поєднання технологічних, організаційних і регуляторних заходів.
Ключові слова: банки; банківська система; кібербезпека; кіберстрахування; ризик-менеджмент.

UKRAINIAN BANKS IN THE CONDITIONS OF MILITARY RISKS, CYBER THREATS, AND UNCERTAINTY

APATSKYI VLADYSLAV
Postgraduate Student, Department of Finance,
Kyiv National University of Technologies and Design, Ukraine
https://orcid.org/0009-0000-8331-6884
vva0919@gmail.com

Abstract. The article examines the current cybersecurity challenges facing Ukraine's banking system under wartime conditions and amid the active digitalization of financial services. The main cyber threats to the banking sector are analysed, including phishing attacks, malware, DDoS attacks, compromise of information systems, and risks associated with the use of foreign-origin

software. The regulatory and legal framework for cybersecurity in the Ukrainian banking sector is considered, and the role of the National Bank of Ukraine in shaping the financial sector's cyber resilience system is determined. The study analyses the dynamics of cyber incidents in Ukraine during 2020–2025 and identifies a growing trend under martial law conditions. Particular attention is paid to cyber risks in mobile banking and vulnerabilities of mobile financial applications. The methodological basis of the research includes comparative analysis, generalization, systematization, and statistical data analysis. The necessity of strengthening cyber risk management systems, implementing modern information security approaches, particularly the secure-by-design concept, and gradually abandoning software that poses potential threats to the banking infrastructure is substantiated. The practical significance of the obtained results lies in their applicability to banking institutions to enhance cybersecurity and minimize risks during the digital transformation. It is concluded that cybersecurity in the banking sector is an essential component of the state's financial stability under wartime uncertainty, and that increasing banks' cyber resilience requires a comprehensive combination of technological, organizational, and regulatory measures.
Keywords: banks; banking system; cybersecurity; cyber insurance; risk management.

Постановка проблеми. Сучасний етап розвитку банківської системи України характеризується стрімкою цифровізацією фінансових послуг, розширенням дистанційного банкінгу, упровадженням технологій відкритого банкінгу та стрімким зростанням обсягів обробки персональних даних. Водночас повномасштабна воєнна агресія російської федерації проти України створила безпрецедентне загострення кіберзагроз, спрямованих на підрив стабільності фінансового сектору та дестабілізацію національної економіки. У таких умовах банківські установи функціонують під постійним тиском кіберінцидентів, що доповнюють інші виклики, пов'язані з воєнним станом. Зокрема, йдеться про фішингові атаки, несанкціонований доступ до внутрішніх інформаційних систем, поширення шкідливого програмного забезпечення, а також спроби компрометації платіжної інфраструктури та каналів обміну фінансовими даними.

Проблему ускладнює те, 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, коли зростає кількість атак, координованих державними та хактивістськими угрупованнями. Таким чином, забезпечення належного рівня кібербезпеки українських банків стає одним із ключових факторів фінансової стійкості та довіри клієнтів у період збройного протистояння та цифрових викликів.

Аналіз останніх досліджень та публікацій. Проблематика кібербезпеки банківського сектору в умовах цифровізації та зростання геополітичних і воєнних ризиків активно досліджується як українськими, так і зарубіжними науковцями. Особливої актуальності ця тема набула після повномасштабного вторгнення російської федерації в Україну, коли кіберпростір перетворився на складову гібридної війни, а банківські установи стали одними з пріоритетних об'єктів кібератак.

У працях вітчизняних дослідників акцентується увага на зростанні системних кіберризиків для банківської системи в умовах воєнного стану. Зокрема, Ю. С. Худолій та М.О. Раєвська [1, с. 51] розглядають кібербезпеку банків як невід'ємний елемент фінансової стійкості держави, підкреслюючи активізацію таких загроз, як DDoS-атаки, фішинг, компрометація платіжної інфраструктури та внутрішніх інформаційних систем банків.

В наступній праці дослідники Т.Р. Андрієць та Ю.С. Худолій [2, с. 58], які аналізують функціонування банківської системи України в період воєнного стану, наголошують на тому, що кібератаки здатні спричиняти не лише прямі фінансові втрати, але й підрив довіри клієнтів до банківських установ, що є критично небезпечним у кризових умовах.

Окрему групу досліджень становлять праці, присвячені впливу цифрової трансформації банківської діяльності на рівень кіберризиків. Так, В. Чапайло [3, с. 20] зазначає, що активне впровадження дистанційних банківських сервісів, мобільного банкінгу, відкритих API та елементів відкритого банкінгу суттєво розширює поверхню потенційних кібератак, водночас підвищуючи вимоги до інтеграції інформаційної безпеки в систему стратегічного управління банком.

Крім того, дослідники Н. Демчишак та А. Шкирі [4, с. 22] обґрунтовують доцільність розгляду кіберризиків нарівні з кредитними й операційними ризиками, підкреслюючи їх потенційно системний характер для фінансового сектору загалом.

Окремої уваги заслуговують наукові праці, присвячені інструментам мінімізації наслідків кібератак. У цьому контексті Б. Рамський та К. Арабаджи [5, с. 2–10] розглядають кіберстрахування як додатковий інструмент управління кіберризиками у банківському секторі. Водночас автори наголошують на обмежених можливостях застосування цього механізму в умовах воєнних ризиків та підвищеної невизначеності безпекового середовища.

Таким чином, аналіз наукових публікацій свідчить, що недостатньо дослідженим залишається комплексний вплив кіберзагроз на діяльність банків у поєднанні з воєнними ризиками та загальною макрофінансовою невизначеністю, що зумовлює потребу в подальших наукових дослідженнях у цьому напрямі.

Мета дослідження полягає у комплексному аналізі та систематизації основних кіберзагроз банківській системі України в умовах воєнного стану та цифровізації, визначенні їх впливу на фінансову стійкість банків, а також обґрунтуванні ефективних механізмів підвищення кібербезпеки та кіберстійкості банківських установ.

Результати та обговорення. Війна російської федерації проти України має екзистенційний характер, тому активне протистояння ведеться тривалий час і в цифровій царині, лише посилюючи свою інтенсивність. Україна стала найбільш пріоритетним напрямом для російських кібератак ще задовго до початку повномасштабного вторгнення у 2022 році. Банківські установи, будучи частиною критичної інфраструктури, є одними із найбільш пріоритетних цілей для ворога, тому важливість їхньої кібербезпеки складно переоцінити.

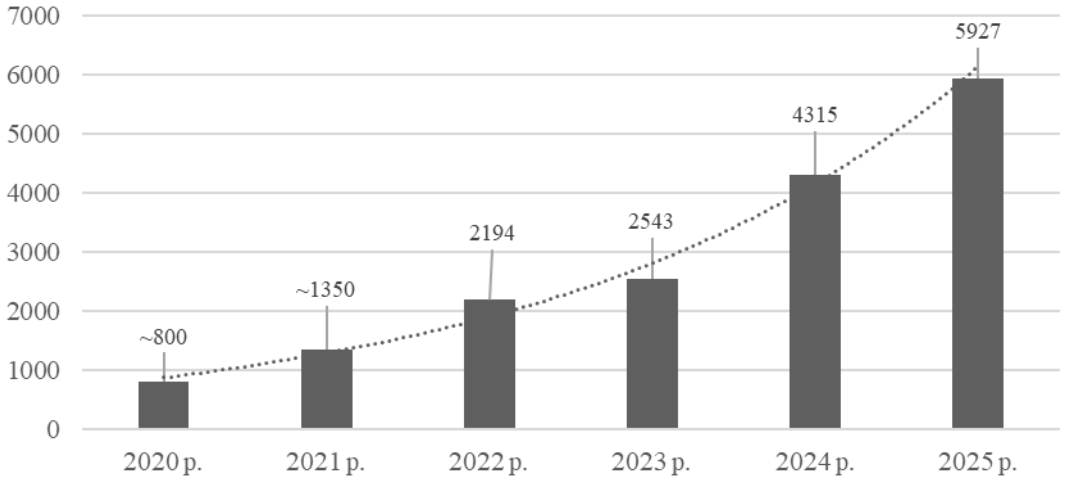
У серпні 2022 року Національний банк України ухвалив Постанову № 178 «Про затвердження Положення про організацію кіберзахисту в банківській системі України» [6]. Цією Постановою було визначено системні вимоги до кіберзахисту банків і порядок функціонування інфраструктури для забезпечення цього кіберзахисту, який включає в себе як апаратні, так і програмні засоби. Цей нормативний акт також запровадив обов'язкове функціонування Центру кіберзахисту НБУ, CSIRT-NBU. Крім того, були укладені, нормативи інформаційного обміну між банками й регулятором з метою швидкого виявлення і реагування на кіберзагрози.

Вкрай важливо, що Положення поширює жорсткіші вимоги саме на системно важливі банки, які є об'єктами критичної інформаційної інфраструктури (ОКІ), зокрема щодо незалежного аудиту інформаційної безпеки та застосування ризик-орієнтованого підходу до захисту систем.

Україна входить до числа держав, які зазнають найбільш інтенсивного кібертиску у світі. 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 [7, 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.

Ще з 2020 року спостерігалося планомірне зростання кількості кіберінцидентів, тоді як уже із 2022 року відбулося різке збільшення їх кількості (рис. 1). Протягом 2025 року національна команда реагування на кіберінциденти CERT-UA, що діє при Держспецзв'язку, опрацювала 5927 кіберінцидентів, що стало на 37,4%, ніж в 2024 році, коли їх налічувалося 4315 [9]. Найбільше кібератак було спрямовано на місцеві органи влади та урядові організації.



Джерело: *побудовано автором на основі даних* [7, 8].

Рис. 1. **Динаміка зареєстрованих кіберінцидентів в Україні протягом 2020–2025**

Варто зазначити, що даних щодо точної кількості кіберінцидентів протягом 2020–2021 років у відкритих звітах не публікувалося; однак урядові джерела оцінювали кількість кіберінцидентів до початку повномасштабної війни в приблизно 850 у 2020 році та 1350 у 2021 році на основі проміжних урядових звітів про загальне зростання атак на критичну інфраструктуру України [8].

Для фінансової галузі найбільш поширеними залишаються фішингові кампанії, спрямовані на викрадення облікових даних користувачів систем дистанційного банківського обслуговування, а також атаки із застосуванням шкідливого програмного забезпечення, зокрема програм-вимагачів і банківських вірусів-троянів. Значну небезпеку становлять також атаки типу DDoS, які спрямовані на порушення доступності онлайн-банкінгу, платіжних сервісів та міжбанківських розрахункових систем. У воєнний період такі атаки часто мають не лише економічну, а й дестабілізаційну мету.

Крім того, важливою загрозою для банківського сектору залишається компрометація внутрішніх інформаційних систем через вразливості програмного забезпечення, соціальну інженерію або атаки на ланцюги постачання IT-рішень. Додаткові ризики виникають унаслідок обстрілів енергетичної інфраструктури та періодичних дефіцитів електроенергії, що може впливати 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.

Чисельні вразливості в українському кіберпросторі, якими вдало користувалася і користується росія для проведення своїх кібератак, пов'язані з тим, що історично

український бізнес, в тому числі й банківські установи, до 2014 року були аж надто орієнтовані на російський економічний простір.

Таблиця 1

Основні кіберзагрози для банків України

Тип загрози	Частота прояву	Потенційні втрати	Приклади атак
Соціальна інженерія, фішинг	Висока	Витік коштів клієнтів, даних	Масові розсилки під виглядом «Приват24», «Ощадбанк», телефонне шахрайство
DDoS-атаки	Середня	Зупинка онлайн-сервісів	Атаки на банки у 2022–2023 рр.
Ransomware	Середня	Втрати даних, викуп	Petya/NotPetya, Ryuk
Внутрішні загрози	Низька (але зростає)	Маніпуляції з рахунками	Несанкціоновані дії співробітників
Атаки на API та fintech	Середня	Злам мобільних застосунків	Уразливості в інтеграції зі сторонніми сервісами

Джерело: *складено автором на основі* [3, 4, 11].

Значним чинником підвищених кіберризиків для банківського та фінансового сектору України тривалий час залишалося і досі залишається використання програмного забезпечення російського походження, зокрема продуктів сімейства 1С та похідних від них рішень. Історично такі програмні продукти були широко поширені в бухгалтерському обліку, управлінні фінансами та внутрішніх бізнес-процесах, що зумовлювалося їх доступністю, адаптованістю до національного законодавства та кадровою інерцією.

Водночас після 2014 року, а особливо з початком повномасштабної війни, використання подібного програмного забезпечення стало розглядатися не лише як економічна чи технологічна проблема, а як безпосередня загроза кібербезпеці та національній безпеці. Неможливість повного контролю над вихідним кодом, потенційна наявність прихованих вразливостей, залежність від розробників із держави-агресора та ризики несанкціонованого доступу до фінансових даних зумовили поетапну відмову від такого програмного забезпечення (ПЗ) в органах державної влади, банках і суб'єктах критичної інфраструктури. В умовах воєнних ризиків та високої невизначеності питання повної заміни програмних рішень російського походження стало складовою стратегії підвищення кіберстійкості фінансово-кредитної системи України.

НБУ вже давно послідовно реалізує стратегію мінімізації використання програмного забезпечення російського і білоруського походження, яке розглядається як елемент кіберризику для фінансового сектору. Ще з 2014 року Національний банк України здійснював поетапну відмову від російського ПЗ у своїх власних інформаційних мережах, переходячи на програмні продукти міжнародних постачальників та локальні розробки, що відповідають вимогам кіберстійкості [9]. У відповідних регуляторних комунікаціях НБУ нагадував українським банкам про ризики, пов'язані з використанням ПЗ російського та білоруського походження, вимагав від них звітування про залежність від такого ПЗ і план дій щодо його мінімізації, а також поставив стратегічну мету «нуля толерантності» до нього на фінансовому ринку. Ці заходи мають не лише рекомендаційний характер: у 2026 році Нацбанк планує провести серію інспекцій інформаційної безпеки та кіберстійкості в окремих банках, що передбачає оцінювання і здатність протидіяти сучасним кібератакам, а отже і прямий вплив на IT-політику та використання стороннього програмного забезпечення.

На національному рівні Державна служба спеціального зв'язку та захисту інформації України включила продукти 1С і BAS до офіційного переліку заборонених програмних продуктів, що підлягають вилученню з використання в держорганах, критичній інфраструктурі та державних підприємствах на підставі постанови Кабінету Міністрів України № 1335 від 22 жовтня 2025 року [10]. Водночас зазначена постанова має переважно обмежувальний характер і не супроводжується чітко визначеним механізмом переходу на альтернативні програмні рішення, що ускладнює практичну реалізацію вимог для суб'єктів

господарювання. Крім того, відсутність у документі перехідних періодів та фінансово-технічної підтримки може стримувати темпи повної відмови від забороненого програмного забезпечення, особливо в умовах воєнних ризиків та обмежених ресурсів.

Незважаючи на очевидні виклики, значна частина українських підприємств продовжує використовувати програмне забезпечення російського походження, хоча воно фактично заборонене для державних структур і критичної інфраструктури, посилаючись, зокрема, і на те, що закон не має зворотної дії. За даними Аналітичного центру Асоціації IT Ukraine, приблизно 75% українських користувачів у бізнесі застосовують програму «1С» або її технічні аналоги типу BAS у щоденній роботі, що свідчить про глибоку інтеграцію цього ПЗ у бізнес-процеси ще до 2022 року й певну інерцію у відмові від нього навіть у 2025–2026 роках, незважаючи на заборону російського програмного забезпечення в держсекторі (за оцінками IT Ukraine, ~75% використання «1С» та суміжних продуктів).

Певні дослідницькі опитування ринку ERP підтверджують, що на частку традиційних продуктів 1С/BAS припадає понад 50–60% ринку облікового та управлінського ПЗ в українських компаніях, що включає й банківські підрозділи, де рішення інтегровані в бухгалтерську, фінансову та операційну автоматизацію. Така ситуація зумовлюється історичною популярністю 1С і BAS, високою адаптованістю до українського обліку та відносно низьким порогом входу для компаній із обмеженими IT-ресурсами.

У контексті поступового зниження залежності від небезпечного ПЗ українські банки та підприємства почали впроваджувати альтернативні інформаційні системи, які відповідають сучасним вимогам кібербезпеки та міжнародним стандартам. Серед основних напрямів – впровадження міжнародних ERP-систем, таких як Microsoft Dynamics 365 Business Central, з гнучкістю для автоматизації обліку, фінансових процесів і управління кадрами, що має переваги щодо стандартів безпеки й інтеграції з іншими корпоративними системами.

Частина бізнес-організацій та фінансових установ також розглядає або впроваджує локальні українські рішення (наприклад, IT-Enterprise, Bookkeeper, Діловод, MASTER: Бухгалтерія, Finmap) як потенційні заміни для «1С»/BAS, хоча ці системи поки що поступаються за функціональністю і масштабами класичному ПЗ. Крім того, уряд та приватні IT-компанії пропонують грантову підтримку для переходу від російських бухгалтерських і ERP-систем до рішень типу Microsoft ERP, що має полегшити міграцію та знизити фінансовий бар'єр для бізнесу [12]. В табл. 2 наведено порівняння сучасних міжнародних ERP-систем з українськими аналогами з позицій відповідності вимогам кібербезпеки.

Таблиця 2

Порівняльний аналіз ERP-систем за критеріями відповідності вимогам кібербезпеки

Критерій	**Міжнародні ERP-системи (Microsoft Dynamics 365, SAP S/4HANA, Oracle ERP Cloud)**	**Локальні ERP-системи (IT-Enterprise, Bookkeeper, Діловод, Finmap)**
Рівень кібербезпеки	Високий. Постійні оновлення безпеки, багаторівневий захист, сертифікації (ISO/IEC 27001, SOC 2).	Середній. Обмежені ресурси на постійні оновлення, залежність від локальних вендорів.
Контроль вихідного коду	Частковий/регламентований (постачальник підтримує, але код часто закритий).	Частковий (інколи відкриті компоненти або адаптовані модулі).
Вразливість до зовнішніх загроз	Низька (часті патчі, моніторинг, threat intelligence).	Вища (рідші оновлення, обмежений threat intelligence).
Інтеграція з SIEM/SOC	Добре підтримується, готові конектори.	Обмежена або потребує кастомної розробки.
Підтримка MFA/Zero Trust	Вбудовані механізми MFA, адаптивний доступ, підтримка Zero Trust.	Часткова або відсутня за замовчуванням, потребує доповнень.
Хмарна безпека (Cloud)	Потужні засоби шифрування, багаторівневі DMZ, контроль доступу.	Обмежені (частіше локальні сервери, слабша сегментація).

Продовження табл. 2

Критерій	Міжнародні ERP-системи (Microsoft Dynamics 365, SAP S/4HANA, Oracle ERP Cloud)	Локальні ERP-системи (IT-Enterprise, Bookkeeper, Діловод, Finmap)
Відповідність регулятору (НБУ, GDPR)	Часткове/активне, залежить від правильних налаштувань і адаптації банку.	Вимагає додаткової адаптації для повної відповідності.
Можливість кастомізації	Висока, але складніша архітектурно; потребує серйозної експертизи впровадження.	Вища (легше кастомізувати під локальні вимоги).
Загальні витрати на підтримку безпеки	Високі (висока вартість підтримки, сертифікацій, контрактів SIEM).	Нижчі, але з меншими гарантіями захисту.
Доступність кваліфікованих фахівців	Висока (широкий ринок спеціалістів).	Обмежена (потреба у вузькопрофільних IT).
Рівень ризику для банківського середовища	Низький/середній при правильній конфігурації.	Середній/високий, якщо не підсилювати безпеку.

Джерело: *систематизовано автором за даними* [7, 13, 15, 16].

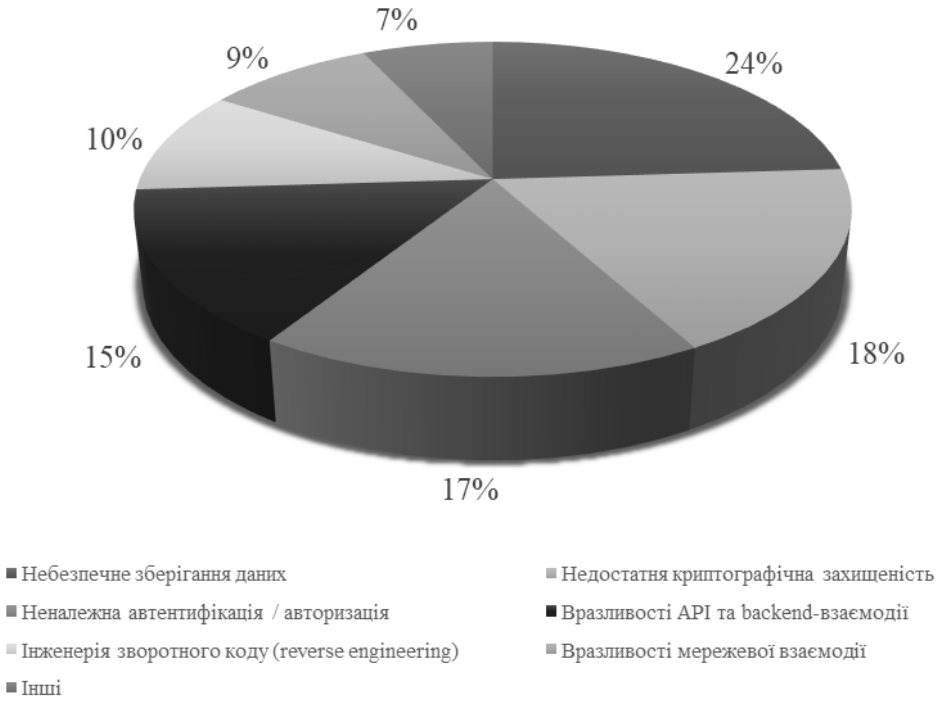
Сучасний банківський сервіс неможливо уявити без мобільних застосунків, які все більше витісняють фізичний формат надання послуг через відділення. В Україні динаміка цього витіснення історично стала швидшою, ніж в багатьох інших країнах Європи, і поступалася вона лише країнам Скандинавії та Нідерландам. Частка клієнтів, які використовують дистанційні сервіси великих банків (ПриватБанк, Monobank, Ощадбанк), перевищувала 70–80% активної клієнтської бази. До 2022 року частка безготівкових операцій в Україні перевищила 60% від загальної кількості транзакцій, а у 2023–2024 роках – понад 65–70% [16, 17]. Причинами такого становища можна виділити кілька специфічних факторів:

– державна політика цифровізації;
– агресивна конкуренція між банками;
– висока IT-компетентність населення;
– відсутність надмірної кількості застарілої банківської інфраструктури та традицій;
– воєнні ризики після 2022 року, які суттєво прискорили впровадження дистанційних сервісів.

Стрімка цифрова трансформація банківського сектору України, що супроводжується активним впровадженням дистанційного обслуговування та мобільного банкінгу, істотно змінила модель взаємодії банків з клієнтами. Мобільні застосунки поступово перетворилися на ключовий інструмент доступу до фінансових послуг, поєднуючи функції платіжних сервісів, ідентифікації користувачів та управління персональними фінансами. Водночас концентрація значного обсягу конфіденційної інформації та фінансових операцій у цифровому середовищі об’єктивно підвищує рівень кіберризиків.

Розширення функціональності мобільних банківських застосунків, інтеграція з зовнішніми сервісами та використання хмарних технологій формують додаткову поверхню потенційних кібератак. У зв’язку з цим дослідження типових вразливостей мобільних банківських застосунків є важливою складовою оцінювання рівня кіберстійкості банківської системи в умовах воєнних ризиків та цифрової невизначеності.

Аналіз вразливостей мобільних фінансових застосунків свідчить, що найбільш поширеними є проблеми небезпечного зберігання даних та недостатньої криптографічної захищеності. Значну частку становлять також вразливості механізмів автентифікації та взаємодії з серверними API, що створює потенційні ризики несанкціонованого доступу до фінансової інформації користувачів. Окрему групу становлять вразливості мережевої взаємодії та можливості аналізу програмного коду застосунків зловмисниками [15].



Джерело: *складено автором на основі* [15].

Рис. 2. **Структура вразливостей мобільних фінансових застосунків за типами**

Вразливості мобільних банківських застосунків мають комплексний характер, поєднуючи програмні, організаційні та поведінкові фактори кіберризику. Зокрема, використання незахищених пристроїв, встановлення стороннього програмного забезпечення та недостатній рівень цифрової грамотності підвищують ймовірність компрометації облікових даних. Для банківського сектору важливим завданням залишається регулярне тестування безпеки мобільних застосунків, впровадження практик secure-by-design, багатофакторної автентифікації та постійний моніторинг підозрілої активності.

Окрім цього, суттєвим чинником зростання кіберризиків у мобільному банкінгу є активне використання відкритих мереж Wi-Fi та недостатній контроль за оновленням програмного забезпечення на стороні користувачів, що створює додаткові вектори атак типу man-in-the-middle та фішингу. За оцінками OWASP Foundation та галузевих досліджень кібербезпеки, ефективне зниження ризиків досягається через поєднання технічних заходів (шифрування, захищені API, threat intelligence) та організаційних механізмів, зокрема навчання користувачів, впровадження політик безпеки та регулярного аудиту інформаційних систем [15].

Стрімкий розвиток штучного інтелекту також створює нові виклики для українських банків. Все частіше зловмисники використовують інструменти ШІ для посилення та збільшення обсягу своїх кібератак, в тому числі для створення шкідливого коду та автоматизації DDOS-атак. Тому банківська кібербезпека повинна бути на крок попереду у використанні новітніх інструментів, запроваджуючи їх максимально ефективно та доцільно.

Для боротьби із одними із найбільш масових загроз – фішинговими атаками – системи на основі штучного інтелекту можуть здійснювати швидкий аналіз величезного обсягу даних, тим самим «навчаючись» на їх основі, аби виявляти та повідомляти про електронні та SMS-розсилки від зловмисників [18]. Такі системи перевіряють підозрілі посилання, домени, неприродню структуру повідомлення та стиль тексту. Крім того, такі системи «навчають» на реальних фішингових кампаніях проти українських фінансових установ, аби вони в майбутньому виявляли загрози максимально швидко ще на етапі їх зародження.

Таблиця 3

Напрями підвищення кіберстійкості банківського сектору України та індикатори оцінювання їх ефективності

Проблеми та прояви кіберризиків	Основні заходи впливу	Рівень реалізації	Очікуваний результат	Індикатори оцінювання ефективності
Зростання кількості кіберінцидентів у банківській системі	Удосконалення нормативної бази кібербезпеки, створення системи координації реагування на кіберінциденти, розвиток центрів моніторингу кіберзагроз	Державний, інституційний	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
Фішингові атаки та соціальна інженерія	Проведення програм кібергігієни, навчання персоналу, інформаційні кампанії для клієнтів, впровадження багатофакторної автентифікації	Інституційний, технологічний	Зменшення випадків шахрайства та несанкціонованого доступу до рахунків клієнтів	Частка інцидентів фішингу; кількість скомпрометованих облікових записів; рівень використання MFA
Поширення шкідливого програмного забезпечення	Аудит інформаційної безпеки, управління вразливостями, регулярне оновлення ПЗ, впровадження систем EDR/XDR	Інституційний, технологічний	Підвищення захищеності інформаційних систем банків	Кількість виявлених уразливостей; кількість інцидентів зараження; рівень оновлення систем
DDoS-атаки на банківські сервіси	Використання систем захисту від DDoS-атак, резервування інфраструктури, застосування хмарних сервісів кіберзахисту	Технологічний, інституційний	Підвищення стабільності роботи онлайн-банкінгу та платіжних систем	Тривалість простоїв сервісів; кількість успішно відбитих атак; доступність онлайн-сервісів (%)
Використання програмного забезпечення ризикового походження	Поступова відмова від ПЗ країни-агресора, впровадження сертифікованих міжнародних і національних рішень, аудит постачальників IT	Державний, інституційний	Зниження ризиків витоку інформації та зовнішнього втручання в банківські системи	Частка використання сертифікованого ПЗ; кількість замінених ризикових систем
Вразливості мобільного банкінгу	Регулярне тестування безпеки застосунків, впровадження secure-by-design, захист API та багаторівнева автентифікація	Технологічний, інституційний	Підвищення рівня довіри клієнтів до цифрових банківських сервісів	Кількість виявлених вразливостей; кількість інцидентів у мобільних застосунках; рівень використання захищених протоколів
Воєнні ризики для інфраструктури	Розвиток систем резервування дата-центрів, хмарні рішення, реалізація планів безперервності діяльності (BCP) та відновлення (DRP)	Державний, інституційний, технологічний	Забезпечення безперервності функціонування банків навіть у кризових умовах	Час на відновлення систем; кількість реалізованих планів BCP/DRP; рівень доступності IT-систем
Недостатній рівень автоматизації кіберзахисту	Інтеграція технологій штучного інтелекту та машинного навчання у системи моніторингу кіберзагроз	Технологічний	Підвищення швидкості виявлення та нейтралізації кіберзагроз	Середній час виявлення інцидентів; частка автоматично оброблених загроз

Джерело: *узагальнено автором на основі* [2, 7, 9].

Для протидії DDoS-атакам системи на основі штучного інтелекту використовують поведінковий аналіз для виявлення «аномалій» у трафіку. Вони визначають «білий список» легітимних запитів та повідомляють про будь-які відхилення від норми, які спричиняють

мережі ботів [19]. Щодо Malware, то використовується комбінація сигнатурного та поведінкового аналізу. Звичайні програми-антивіруси дуже залежні від оновлень бази сигнатур, у той час як штучний інтелект через машинне навчання аналізує і проводить моніторинг зразків шкідливих програм, виявляє напрямок розвитку вірусів за допомогою евристичних моделей [20].

Таким чином, інтеграція технологій штучного інтелекту в систему управління кіберризиками банків виступає не лише інструментом підвищення операційної ефективності, а й стратегічною передумовою забезпечення фінансової стійкості та кіберстійкості банківської системи України.

Важливою складовою забезпечення кіберстійкості банківського сектору є формування ефективної системи управління кіберризиками на рівні окремих банківських установ. Така система передбачає інтеграцію процесів інформаційної безпеки в загальну систему управління ризиками банку, впровадження політик кібербезпеки, регулярне проведення аудиту інформаційних систем і тестування на проникнення. Значну роль відіграють також підготовка персоналу та розвиток культури кібербезпеки, оскільки людський фактор залишається одним із ключових джерел кіберризиків. У сучасних умовах банки дедалі частіше переходять до ризикоорієнтованих моделей кіберзахисту, що передбачають безперервний моніторинг загроз, оцінювання вразливостей інформаційної інфраструктури та оперативне реагування на кіберінциденти.

Висновки. У результаті дослідження встановлено, що кібербезпека банківського сектору України в умовах воєнних ризиків і цифрової трансформації фінансових послуг набуває системного значення для забезпечення фінансової стабільності держави. Активна цифровізація банківських операцій, розвиток мобільного банкінгу та інтеграція фінансових сервісів із зовнішніми цифровими платформами суттєво розширили поверхню потенційних кібератак і підвищили рівень кіберризиків для банківських установ.

Проаналізована динаміка кіберінцидентів у 2020–2025 роках свідчить про стійку тенденцію до їх зростання, особливо після початку повномасштабної війни. Найбільш поширеними загрозами для банківського сектору залишаються фішингові атаки, шкідливе програмне забезпечення, DDoS-атаки, компрометація внутрішніх інформаційних систем, а також вразливості мобільних банківських застосунків. Додатковим чинником кіберризику виступають воєнні загрози для енергетичної та телекомунікаційної інфраструктури, що можуть впливати на стабільність функціонування банківських IT-систем.

Встановлено, що важливою передумовою підвищення кіберстійкості фінансового сектору є поступова відмова від програмного забезпечення російського походження, яке створює потенційні ризики для інформаційної безпеки банків і суб'єктів критичної інфраструктури. Перехід на альтернативні програмні рішення, зокрема міжнародні та локальні ERP-системи, має супроводжуватися посиленням контролю за інформаційною безпекою та розвитком внутрішніх компетенцій у сфері кіберзахисту.

Окремого значення набуває забезпечення безпеки мобільного банкінгу як ключового каналу взаємодії банків з клієнтами. Регулярне тестування безпеки застосунків, впровадження багатофакторної автентифікації, принципів secure-by-design та постійний моніторинг кіберзагроз є необхідними умовами зниження ризиків несанкціонованого доступу до фінансових даних.

Визначено, що перспективним напрямом розвитку систем кіберзахисту банків є інтеграція технологій штучного інтелекту в процеси управління кіберризиками. Використання інструментів машинного навчання для виявлення фішингових кампаній, аномальної мережевої активності та шкідливого програмного забезпечення дозволяє підвищити швидкість реагування на кіберінциденти та ефективність превентивного захисту.

Таким чином, підвищення кіберстійкості банківської системи України потребує комплексного поєднання технологічних, організаційних і регуляторних заходів, спрямованих на адаптацію фінансового сектору до умов воєнної невизначеності, зростання цифровізації та постійної еволюції кіберзагроз.

References

1. Raievska, M. O., & Khudolii, Yu. S. (2024). Kiberbezpeka bankiv Ukrainy v umovakh viiny [Cybersecurity of Ukrainian banks in wartime]. *Ekonomichna bezpeka: derzhava, rehion, pidpryiemstvo: materialy VIII Mizhnar. nauk.-prakt. konf.*, May 16, 2024 (pp. 51–55). Poltava: Nats. un-t im. Yuriia Kondratiuka [in Ukrainian].
2. Khudolii, Yu. S., & Andriiets, T. R. (2023). Zabezpechennia kiberbezpeky bankivskoi systemy Ukrainy u period voiennoho stanu [Ensuring cybersecurity of the banking system of Ukraine during martial law]. *Ekonomichna bezpeka: derzhava, rehion, pidpryiemstvo: materialy VII Mizhnar. nauk.-prakt. Internet-konf.*, May 17, 2023 (pp. 58–61). Poltava: Natsionalnyi universytet imeni Yuriia Kondratiuka [in Ukrainian].
3. Chapailo, V. V. (2025). Pidvyshchennia kiberbezpeky bankiv u konteksti tsyfrovizatsii protsesiv [Improving the cybersecurity of banks in the context of digitalization of processes]. *Visnyk Natsionalnoho tekhnichnoho universytetu "Kharkivskyi politekhnichnyi instytut" (ekonomichni nauky),* 3, 20–24 [in Ukrainian].
4. Demchyshak, N. B., & Shkyria, A. S. (2021). Upravlinnia ryzykamy u finansovomu sektori Ukrainy v konteksti kiberzahroz ta vidnovlennia ekonomiky pislia pandemii [Risk management in the financial sector of Ukraine in the context of cyber threats and economic recovery after the pandemic]. *Innovatsiina ekonomika*, 3–4, 19–27 [in Ukrainian].
5. Ramskyi, A. Yu., & Arabadzhy, K. V. (2023). Kiberstrakhuvannia v bankivskomu sektori: identyfikatsiia ryzykiv ta instrumenty pidtrymky bezpeky [Cyber insurance in the banking sector: risk identification and security support tools]. *Naukovyi visnyk mizhnarodnoi asotsiatsii naukovtsiv*, 2(2). URL: https://elibrary.kubg.edu.ua/id/eprint/47091/ [in Ukrainian].
6. *Pro zatverdzhennia Polozhennia pro orhanizatsiiu kiberzakhystu v bankivskii systemi Ukrainy ta vnesennia zmin do Polozhennia pro vyznachennia ob'iektiv krytychnoi infrastruktury v bankivskii systemi Ukrainy* [On approval of the Regulation on the organization of cyber protection in the banking system

Література

1. Раєвська М. О., Худолій Ю. С. 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. Худолій Ю. С., Андрієць Т. Р. 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. С. 58–61.
3. Чапайло В. В. Підвищення кібербезпеки банків у контексті цифровізації процесів. *Вісник Національного технічного університету "Харківський політехнічний інститут" (економічні науки).* 2025. № 3. С. 20–24.
4. Демчишак Н. Б., Шкиря А. С.: Управління ризиками у фінансовому секторі України в контексті кіберзагроз та відновлення економіки після пандемії. *Інноваційна економіка.* 2021. № 3–4. С. 19–27.
5. Рамський А. Ю., Арабаджи К. В. Кіберстрахування в банківському секторі: ідентифікація ризиків та інструменти підтримки безпеки. *Науковий вісник міжнародної асоціації науковців.* 2023. Том 2, №2. URL: https://elibrary.kubg.edu.ua/id/eprint/47091/
6. 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

of Ukraine and amendments to the Regulation on the definition of critical infrastructure facilities in the banking system of Ukraine: Resolution of the National Bank of Ukraine dated August 12, 2022 No. 178]. URL: https://bank.gov.ua/admin_uploads/law/12082022_178.pdf [in Ukrainian].

7. *Microsoft Digital Defense Report 2025*. URL: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Microsoft-Digital-Defense-Report-2025.pdf.

8. *CERT-UA mynuloho roku opratsiuvala 4315 kiberintsydentiv* [CERT-UA processed 4,315 cyber incidents last year]. URL: https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv [in Ukrainian].

9. *Richnyi zvit NBU za 2022 rik – Power Banking* [NBU Annual Report for 2022 – Power Banking]. URL: https://bank.gov.ua/admin_uploads/article/annual_report_2022.pdf [in Ukrainian].

10. *Pro zatverdzhennia Poriadku formuvannia ta vedennia vidkrytoho pereliku zaboronenoho do vykorystannia prohramnoho zabezpechennia ta komunikatsiinoho (merezhevoho) obladnannia* [On approval of the Procedure for forming and maintaining an open list of software and communication (network) equipment prohibited for use: Resolution of the Cabinet of Ministers of Ukraine dated 10/22/2025 No. 1335]. URL: https://zakon.rada.gov.ua/laws/show/1335-2025-%D0%BF#Text [in Ukrainian].

11. Kopyliuk, O., Zhyhar, N., & Petryniak, A. (2024). Zahrozy finansovii bezpetsi bankivskykh ustanov Ukrainy v umovakh tsyfrovizatsii [Threats to the financial security of Ukrainian banking institutions in the context of digitalization]. *Ekonomichnyi chasopys Volynskoho natsionalnoho universytetu imeni Lesi Ukrainky*, 2, 61–68.

12. *Hrantova pidtrymka ukrainskoho biznesu pry perekhodi z rosiiskykh oblikovykh system na rishennia vid Misrosoft* [Grant support for Ukrainian businesses in transitioning from Russian accounting systems to solutions from Microsoft]. URL: https://chamber.ua/ua/news/hrantova-pidtrymka-ukrainskoho-biznesu-pry-perekhodi-z-rosiyskykh-oblikovykh-system-na-rishennia-vid-misrosoft/ [in Ukrainian].

13. Danik, N., & Torlopov, A. (2024). Vplyv tsyfrovoi transformatsii na bankivskyi sektor Ukrainy [The

Національного банку України від 12.08.2022 р. № 178. URL: https://bank.gov.ua/admin_uploads/law/12082022_178.pdf.

7. Microsoft Digital Defense Report 2025. URL: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Microsoft-Digital-Defense-Report-2025.pdf.

8. CERT-UA минулого року опрацювала 4315 кіберінцидентів. URL: https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv.

9. Річний звіт НБУ за 2022 рік – Power Banking. URL: https://bank.gov.ua/admin_uploads/article/annual_report_2022.pdf.

10. Про затвердження Порядку формування та ведення відкритого переліку забороненого до використання програмного забезпечення та комунікаційного (мережевого) обладнання: Постанова Кабінету Міністрів України від 22.10.2025 р. № 1335. URL: https://zakon.rada.gov.ua/laws/show/1335-2025-%D0%BF#Text.

11. Копилюк О., Жигар Н., Петриняк А. Загрози фінансовій безпеці банківських установ України в умовах цифровізації. *Економічний часопис Волинського національного університету імені Лесі Українки.* 2024. № 2. С. 61–68.

12. Грантова підтримка українського бізнесу при переході з російських облікових систем на рішення від Microsoft. URL: https://chamber.ua/ua/news/hrantova-pidtrymka-ukrainskoho-biznesu-pry-perekhodi-z-rosiyskykh-oblikovykh-system-na-rishennia-vid-misrosoft/

13. Данік Н., Торлопов А. Вплив цифрової трансформації на банківський

impact of digital transformation on the banking sector of Ukraine]. *International Science Journal of Management, Economics & Finance,* 3(3), 95–103 [in Ukrainian].
14. *Microsoft Build 2026: Zero Trust security guidance*. URL: https://learn.microsoft.com/en-us/security/zero-trust/
15. *OWASP Top Ten Web Application Security Risks*. URL: https://owasp.org/www-project-top-ten/
16. *Richnyi zvit NBU za 2023 rik – Finansova fortetsia* [NBU Annual Report for 2023 – Financial Fortress]. URL: https://bank.gov.ua/admin_uploads/article/annual_report_2023.pdf [in Ukrainian].
17. *Richnyi zvit NBU za 2024 rik – Stiikist* [NBU Annual Report for 2024 – Sustainability]. URL: https://bank.gov.ua/admin_uploads/article/annual_report_2024.pdf?v=13 [in Ukrainian].
18. *AI-Driven Phishing Detection Using NLP and URL Analysis*. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5560918.
19. Aamir, M., & Zaidi, S. M. A. (2019). Clustering based semi-supervised machine learning for DDoS attack classification. *IEEE Access,* 7, 436–446.
20. Souri, A., & Hosseini, R. (2020). A state-of-the-art survey of malware detection approaches using data mining techniques. *Computers & Security,* (93). DOI: https://doi.org/10.1186/s13673-018-0125-x.

сектор України. *International Science Journal of Management, Economics & Finance*. 2024. Вип. 3, № 3. С. 95–103.
14. Microsoft Build 2026: Zero Trust security guidance. URL: https://learn.microsoft.com/en-us/security/zero-trust/
15. OWASP Top Ten Web Application Security Risks. URL: https://owasp.org/www-project-top-ten/
16. Річний звіт НБУ за 2023 рік – Фінансова фортеця. URL: https://bank.gov.ua/admin_uploads/article/annual_report_2023.pdf.
17. Річний звіт НБУ за 2024 рік – Стійкість. URL: https://bank.gov.ua/admin_uploads/article/annual_report_2024.pdf?v=13.
18. AI-Driven Phishing Detection Using NLP and URL Analysis. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5560918.
19. Aamir M., Zaidi S. M. A. Clustering based semi-supervised machine learning for DDoS attack classification. *IEEE Access*. 2019. Vol. 7. P. 436–446.
20. Souri A., Hosseini R. A state-of-the-art survey of malware detection approaches using data mining techniques. *Computers & Security*. 2020. Vol. 93. DOI: https://doi.org/10.1186/s13673-018-0125-x.