DOI: 10.31388/2519-884X-2023-47-151-163

УДК [336.7+330.131.7](477):004.9

***Трусова Н. В.**, д. е. н., професор*
Таврійський державний агротехнологічний університет імені Дмитра Моторного
trusova_natalya5@ukr.net
***Чкан І. О.**, к. е. н., доцент*
Таврійський державний агротехнологічний університет імені Дмитра Моторного
iryna.chkan@tsatu.edu.ua

КІБЕРЗАХИСТ БАНКІВСЬКОЇ СИСТЕМИ УКРАЇНИ В УМОВАХ ЦИФРОВИХ ТРАНСФОРМАЦІЙ

***Анотація.** В статті актуалізовано проблеми кібератак на банківську систему України, пов'язані зі зламом електронної системи та виманювання коштів. Наведено розмежування поняття безпеки банківського сектору за рівнем і характером дій. Обґрунтовано, що швидкість цифрової трансформації в банківському секторі спричинює появу нових ризиків, особливо кібернетичних. Акцентовано, що урядом приймається нормативна законодавча база з врахуванням вимог ЄС з питання кіберзахисту банківської системи на основі якого забезпечується національна безпека країни.*

***Ключові слова:** економіка, цифровізація, кіберризики, банківська система, кіберзахист, кібербезпека.*

JEL classification: E58, G28, H56

***Trusova N. V.,** Doctor of Economic Sciences, Professor*
Dmytro Motornyi Tavria State Agrotechnological University
trusova_natalya5@ukr.net
***Chkan I. O.,** PhD, Associate Professor*
Dmytro Motornyi Tavria State Agrotechnological University
iryna.chkan@tsatu.edu.ua

CYBER PROTECTION OF THE BANKING SYSTEM OF UKRAINE IN CONDITIONS OF DIGITAL TRANSFORMATIONS

***Abstract.** The article updates the problems of cyberattacks on the banking system of Ukraine, exacerbated by military actions and numerous cyberattacks of the aggressor country, related to the hacking of the electronic system and extortion of funds. Possible cyber threats to the banking system of Ukraine in the conditions of inevitable digitization are analyzed. Demarcation of the concept of security of the banking sector according to the level and nature of actions into the information security of the banking sector, the security of information technologies of the bank and directly the cyber security of the banking institution is presented. Research by international institutes on the analysis of the impact of Fintech on banking activities identified the key risks associated with the development of digital technologies: strategic risk, operational risk, cyber risk, compliance risk. The impact of key risks in banking related to digitalization is shown, where the cyber risk is identified as the key one, the occurrence of which has a direct impact on the entire information system of the state and on national security. New challenges to the banking system of Ukraine, caused by the war, have formed stable business models for banks, taking into account a balanced approach to risks, especially cyber risks. The conducted research gave reasons to state that the joint efforts of commercial banks and the regulator of the financial sector hardened to the biggest shocks and ensured uninterrupted work. It was emphasized that the government adopts a regulatory legislative framework taking into account EU requirements on the issue of cyber protection of the banking system, based on which the national security of the country is ensured.*

***Key words:** economy, digitalization, cyber risks, banking system, cyber protection, cyber security.*

Постановка проблеми. Питання кіберзахисту економічної системи з кожним роком набуває сильнішої проблематики, тому що кібератаки стають все

більш частими та витонченими, зачіпаючи окремо як особу, так і всю міжнародну спільноту. Фінансові установи та інфраструктура фінансового ринку найбільше піддаються кібератакам, специфіка яких змінюється майже щодня. Поширення криптовсесвіту ще більше збільшило ймовірність зломів в масштабі фінансового сектору. Інформаційні технології вже давно є ядром фінансової системи й кібербезпеки та пов'язані з нею загрози знаходяться під пильним, щоденним, безперервним наглядом центральних банків. Тенденція до зростання кіберзлочинності зробила кібербезпеку ключовим питанням державної політики для регуляторних і наглядових органів. Фінансові установи, а саме банки, стають все більш привабливою мішенню для кіберзлочинців, тому що фінансовий сектор приваблює великих інвесторів з інформаційних технологій, виділяючи значні фінансові ресурси.

Саме цифрова трансформація в банківській сфері забезпечує розширення можливостей ведення банківської справи, збереження клієнтської бази, покращення позицій на міжнародному фінансовому ринку, зменшення витрат ведення бізнесу, підвищення конкурентоспроможності тощо. Все це повинно реалізовуватись під щільним контролем виявлення можливих внутрішніх і зовнішніх загроз, суб'єктивного та об'єктивного характерів, на тлі яких кіберінциденти стають найнебезпечнішими. Тому дослідження інструментів кіберзахисту фінансової системи, яка працює за допомогою банківської, потребує виваженого та детального вивчення з метою розроблення ефективного механізму кіберзахисту банківської системи.

Аналіз останніх досліджень і публікацій. Трансформація банківської діяльності під впливом цифрових технологій, створення нових банківських бізнес-моделей в своїх працях розкривають іноземні автори, такі як Forcadell F. J. [5], Eisenbach T. M., Kovner A., Lee M. J. [9] та багато інших. Трофіменко О. Г. [4] та ряд науковців досліджують широкий спектр питань, вирішення яких на основі державно-приватного партнерства створить комплексну протидію кіберзагрозам. Сучасні науковці, такі як Абрамова А. С. [2], Гончарук В., Івлєєва М., Шелудько С. А. у своїх працях досліджують ризики, які

супроводжують банківську діяльність з впровадженням нових цифрових технологій. Удосконалення механізму кібербезпеки економічного простору посилює його пріоритетність серед всіх завдань і функцій уповноважених інститутів його забезпечення. Тому дослідження цифрової трансформації банківського сектору та виявлення шляхів покращення кіберзахисту потребує подальшого дослідження.

Мета статті. Метою статті є аналіз можливих кібернетичних загроз банківській системі України в умовах неминучої дії цифровізації та визначення характеру дій кіберзагроз на різні види захисту цифри банківської системи.

Виклад основного матеріалу. На фоні повномасштабного вторгнення в Україні цифрові атаки стали невід'ємною складовою і війни, на державні сайти та сайти великих системно важливих компаній. Разом з цим кіберзлочинці опановують нові методи кібернетичних атак. Тому завданням регуляторів є збереження системності у протидії кібератакам, а банківському сектору – інвестувати в кібербезпеку. Нажаль, робота банківської системи, посилена умовами війни, в напрямі забезпечення кіберзахисту спрямована на інвестування коштів у пошук засобів захисту даних та рахунків своїх клієнтів та подолання наслідків здійснених кібератак.

За інформацією НБУ у 2022 р. майже усі кібератаки на банківський сектор здійснювались хакерськими угрупованнями, за якими стояла влада країни агресора (групи хакерів Armageddon, Fancy Bears та інші) (рис. 1). Наразі усі кібернапади країни агресора звелись до двох напрямків: DDoS-атаки різного характеру, від яких страждає вся банківська система, але не НБУ та фішингові атаки різних типів (різні види шахрайства). Майже усі фішингові атаки, які спрямовані на банківську систему, є виманюванням коштів у клієнтів банків за різними схемами надання допомоги. Аферисти використовують найпростішу соціальну інженерію, найпростіші методи створення фейкових мобільних додатків та фейкових сторінок банків, де використовується айдентика справжніх банків [1].

Насправді, кібернетичних атак на банківську систему набагато більше, ніж свідчить офіційна статистика. Це пояснюється тим, що багато з кібератак є невдалими, а виявлені прогалини в системі електронного банкінгу швидко відновлюються.

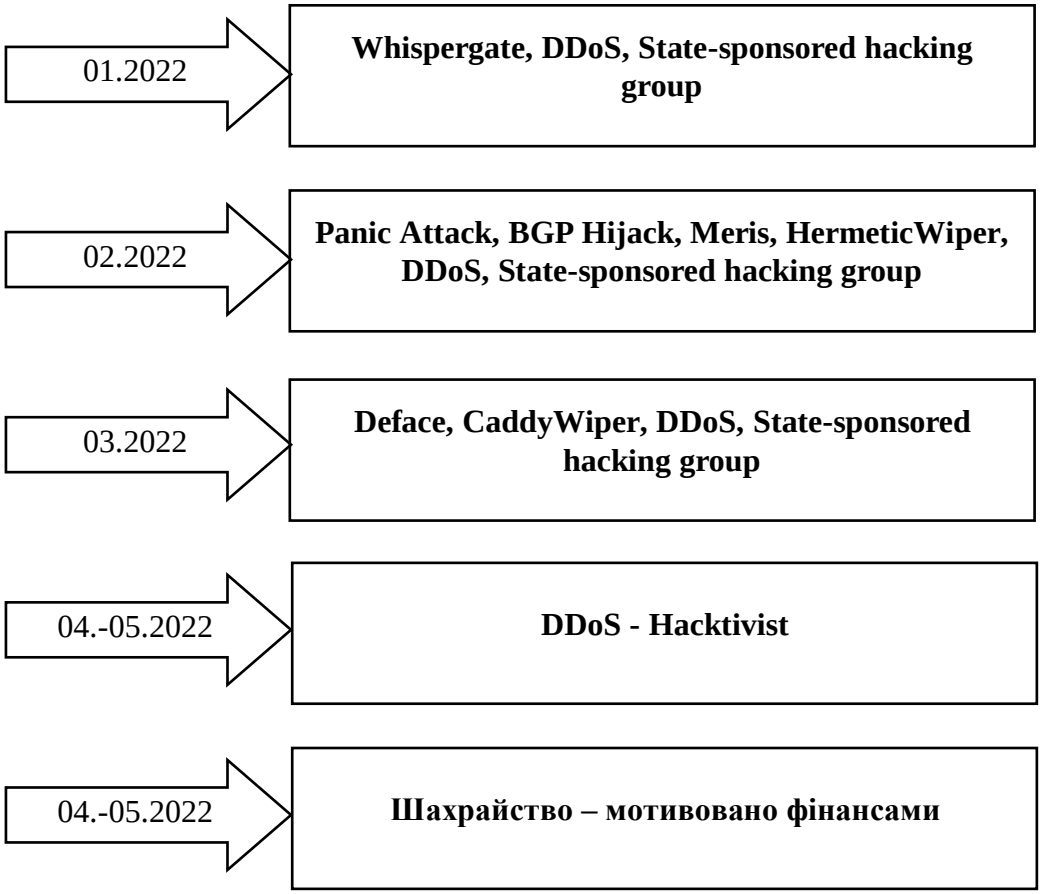

Рис. 1. **Хронологія атак на НБУ та банківську систему України у 2022 році [1]**

Ключовими трендами банківської цифровізації в Україні сьогодні є: оптимізація віддаленої роботи працівників банку, зростання операцій онлайн, спрощення доступу до послуг банку, розвиток каналів дистанційного продажу, боротьба з шахраями та хакерами, широке застосування технологій штучного інтелекту, перехід до управління на основі даних, програми тотальної персоніфікації, імпортозаміщення, розвиток екосистем, розробка власного програмного забезпечення та зростання потреби в ІТ-фахівцях [2, с. 187; 3].

Саме стрімкий розвиток інформаційних технологій надає окремого значення кібербезпеці, зокрема банківського сектору. Розмежування понять

формується на основі посилення їх змісту в глобалізаційному просторі. Безпека банківського сектору може носити різний характер дій. Можна виокремити інформаційну безпеку банківського сектору, безпеку інформаційних технологій банку та безпосередньо кібербезпеку банківської установи.

Інформаційна безпека банківського сектору – це безпека будь-якої інформації, включаючи паперові документи, голосову інформацію, забезпечення банківської таємниці, цензура, фізична безпека, безперервність роботи банківської установи, соціальна інженерія тощо. Найбільшою загрозою для кібербезпеки є людська помилка. Саме люди зрештою піддають ризику дані та системи через те, що їх обманом змусили надати конфіденційну інформацію, не захистили належним чином свої паролі, використали слабкі облікові дані, натиснули шкідливі посилання або відкрили підозрілі вкладення електронної пошти (85% порушень кібербезпеки є наслідком людської помилки, 94% всіх заражених файлів та програм передаються через електронну пошту) [4].

Безпека інформаційних технологій банку полягає у захисті від хакерів, вірусів, спаму, фішингу та інших загроз, що виникають, головним чином, з Інтернету. Встановлення вимог, які пред’являються до обчислювальної та комунікаційної техніки та інформації, яку вона зберігає, обробляє та передає, забезпечує цілісність, доступність та конфіденційність банківської інформації. Якщо інформаційна безпека банківського сектору в значній мірі покладається на нормативи та вимоги з державної безпеки, то організація безпеки інформаційних технологій банку покладається на керівні органи та технічне забезпечення банківської системи і таким чином реалізація захисту проводиться через організаційні та технічні елементи роботи банку. Безпека інформаційних технологій банку полягає в ефективному управлінні забезпечення безпеки банківських процесів, зокрема, використанні кіберстрахування, дотримання відповідності нормативним вимогам безпеки банку, надання гарантій безпеки, забезпечення безперервності роботи банку з виявленням потенційних кіберзагроз. Все це висуває вимоги до компетенції менеджерів банку, фінансистів, економістів, аналітиків, маркетологів, юристів із застосуванням

економіко-математичних методів. У безпеці інформаційних технологій банку все зводиться до процесів управління ризиками.

Банки зобов'язані детально відстежувати потенційні загрози та ризики. 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 [5].

Дослідження Базельського комітету з банківського нагляду з аналізу впливу фінтеху на банківську діяльність (у тому числі трансформації банківських ризиків) ключовими ризиками, пов'язаними з розвитком цифрових технологій, визначає стратегічний ризик, операційний ризик, кіберризик, комплаєнс-ризик [6].

Стратегічні ризики носять масштабний характер передбачення можливих загроз з наслідками фінансових втрат всієї банківської системи. Стратегічні ризики виникають з процесами швидкого розвитку технологій нових банківських продуктів з виходом на міжнародний рівень, що збільшує ризик втрати прибутковості банків через тривалий адаптаційний період. Процеси адаптації до нових продуктів кіберпростору банківського сектору матимуть для окремих банків затяжний характер в порівнянні з учасниками ринку, які надають аналогічні банківські послуги з нарощеною клієнтською базою. Спад прибутковості всього банківського сектору через відсутність гнучкості у взаємодії з клієнтами може послабити здатність діючих банківських установ витримувати цикли ділової активності. Це призведе до послаблення ролі соціальної системи, дестабілізації процесів реалізації державних інтересів.

Операційні ризики виникають в процесі користування електронними системами платіжної інфраструктури банківського сектору, взаємопов'язаної зі всією електронною сіткою як всередині окремої банківської установи, так і всієї мережі банків. Збій на використовуваній електронній платформі та сервері веде до збою роботи всієї банківської IT-інфраструктури, підкріплюючи обмеженим досвідом управління ризиками окремих банківських установ, що робить

складнішим і затратним подолання наслідків кіберінцидентів. Крім того, застарілі банківські ІТ-системи складніше «вилікувати» та адаптувати до удосконалених. Складність уникнення, подолання операційних ризиків банківської системи несуть відносини, які банки мають залучаючи спеціалізовані компанії, роблячи вразливим збереження конфіденційності і чистоти інформації, порушення норм фінансового моніторингу [7]. Але при обмежених власних можливостях забезпечення кібербезпеки банківської установи залучення легальних спеціалізованих ІТ-компаній (IT-outsourcing) на постійній основі є необхідною умовою забезпечення кіберзахисту [8]. Водночас, згідно зі стандартами Базельського комітету з банківського нагляду, хоча частина функціоналу банку може бути передана на аутсорсинг, ризики та зобов'язання, пов'язані з цим, залишаються за банками.

Кіберризики як результат цифрових атак, ризики функціональної моделі банківського обслуговування та ризики зараження і пошкодження персональних даних клієнтів та звітних даних діяльності банків набувають тенденції поширення, тому регулятори банківського сектору відносять до системних кіберризиків – ризик порушення стабільності банківської системи внаслідок реалізації кіберзагроз щодо окремого банку через відповідні недоліки в його кіберстійкості [9]. Кібербезпека самої банківської установи повністю покладається на органи управління банком та фахівців. Втрати цілісності даних і несанкціонованого доступу до даних клієнта, ризики порушення функціонування технічної системи в інформаційному просторі знижують довіру клієнтів, суспільства й держави в цілому у разі неможливості банку забезпечити належний рівень кібербезпеки.

Комплаєнс-ризики призводять до виникнення збитків/санкцій, додаткових втрат або недоотримання запланованих доходів або втрати репутації внаслідок невиконання банком вимог законодавства, коли банки співпрацюють з великою кількістю залучених компаній, кожна з яких прагне отримати доступ до персональних даних клієнтів, що призводить до порушення

правил добросовісної конкуренції, правил корпоративної етики, виникнення конфлікту інтересів і збереження чистоти інформації.

Банківська система під впливом ризиків цифровізації в першу чергу залежить від кібернетичних ризиків, які здійснюють безпосередній вплив на всю інформаційну систему держави і від так на її безпеку (рис. 2).

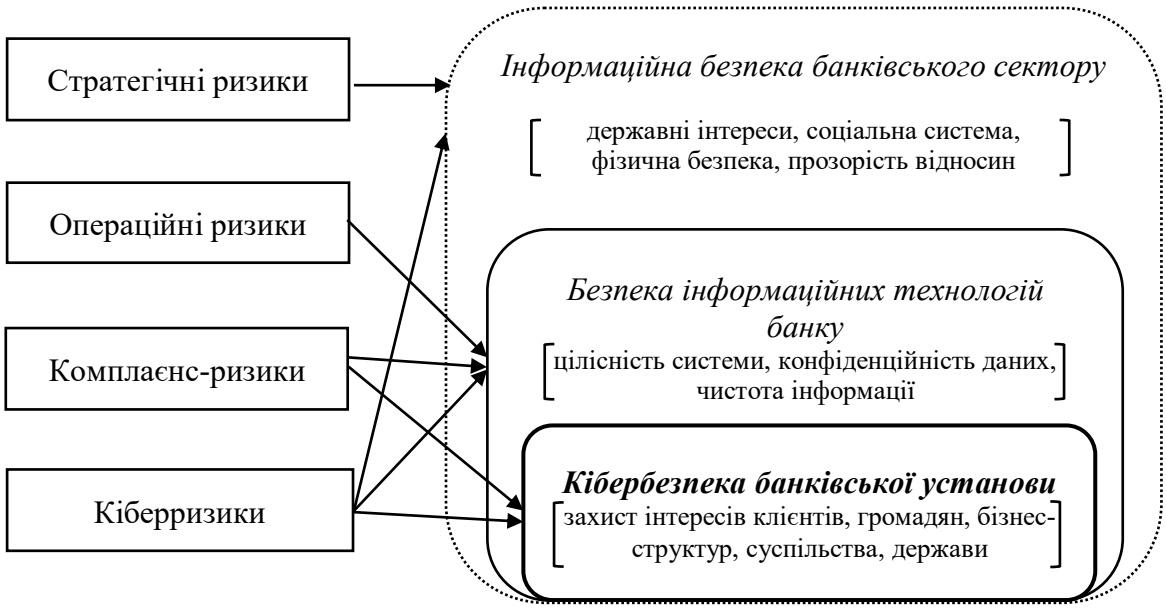

Рис. 2. **Кібербезпека в системі інформаційної безпеки банківського сектору**

Джерело: побудовано авторами

Забезпечення кібербезпеки банківського сектору є досить складним завданням для органів законодавчої влади і безпосередньо для органів управління установою чи організацією. Існує багато стандартів, норм і правових положень, пов'язаних з інформаційною безпекою та кібербезпекою фінансового сектору, зокрема, банківського, які час від часу змінюються, а нові нормативні акти регулярно з'являються. Найпопулярнішим і визнаним стандартом є ISO/IEC 27001 (ISO/IEC 27001 standard) «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги». Стандарт ISO/IEC 27001 підлягає сертифікації. Крім того є стандарти з платформи ISO 27000, які допомагають у впровадженні 27001, надаючи різні поради та передові практики [10].

Система управління кібербезпекою (CSMS), запропонована стандартом IEC 62443 (ISA/IEC 62443 standard) [11], складається з шести основних елементів: впровадити програму CSMS (щоб надати інформацію, необхідну для отримання підтримки керівництва); оцінити ризики високого рівня (виявлення та визначення пріоритетів загроз); детальна оцінка ризику (детальна оцінка технічної вразливості); встановити правила безпеки, організації та поінформованості; вибрати і впровадити контрзаходи (для зниження ризику для організації); підтримувати CSMS (щоб переконатися, що CSMS залишається ефективною і підтримує цілі організації).

Стандарт ISA/IEC 62443 містить вимоги до проектування, безпечної реалізації (програмування), верифікації та перевірки справжності, управління дефектами, управління виправленнями та закінчення терміну служби продукту з урахуванням безпеки. Цей стандарт визначає вимоги до процесу безпечної розробки продуктів, ґрунтуючись на 6 основних принципів [9, 11]: безпека периметра мережі (передбачає встановлення безпеки периметра мережі для контролю тих точок, де чужорідне програмне забезпечення може проникнути в систему автоматизації виробництва); захист робочих станцій (передбачає захист робочих станцій системи управління, щоб утруднити їх зараження шкідливим програмним забезпеченням); управління обліковими записами (передбачає управління обліковими записами); оновлення безпеки (забезпечує актуальність усіх оновлень безпеки для операційної системи та системи управління); резервне копіювання та відновлення (передбачає розробку та реалізацію плану резервного копіювання та відновлення); моніторинг безпеки та оцінка ризиків (включає моніторинг системи на предмет підозрілих активностей та оцінку ризиків).

Центральні банки зазвичай відповідають за управління та нагляд за критичною інфраструктурою (наприклад, платіжними системами) у фінансовому секторі. Відтак, кібератака на центральний банк або критично важливу інфраструктуру може не лише завдати значних грошових і репутаційних збитків самій установі, а й призвести до широкомасштабних збоїв

у фінансовій системі та, зрештою, до значних суспільних витрат. Крім того, центральні банки захищають конфіденційну інформацію, яку часто шукають злочинці. Наприклад, конфіденційний матеріал щодо майбутньої політики може стати мішенню для злочинців і залучених державних організацій в кібершпигунстві.

Національний банк України в системі протидії кіберзлочинності має подвійний статус. З одного боку, як орган державного нагляду та управління не тільки банківською системою, а і всією фінансовою системою, повинен забезпечувати функціонування налагодженого механізму кіберзахисту. З іншого боку, будучи банком, Національний банк України сам підлягає захисту.

Нові виклики банківській системі України, спричинені війною, сформували у банків стійкі бізнес-моделі з урахуванням виваженого підходу до ризиків, особливо кібернетичних. Спільні зусилля комерційних банків та регулятора фінансового сектору загартували до найбільших потрясінь і забезпечили безперебійну роботу. Так, аналітика банківського сектору України у 2022 р. суттєво не змінилась (рис. 3), кількість банків зменшилась на 4 одиниці (з них 2 з російським капіталом – Сбербанк та Промінвестбанк).

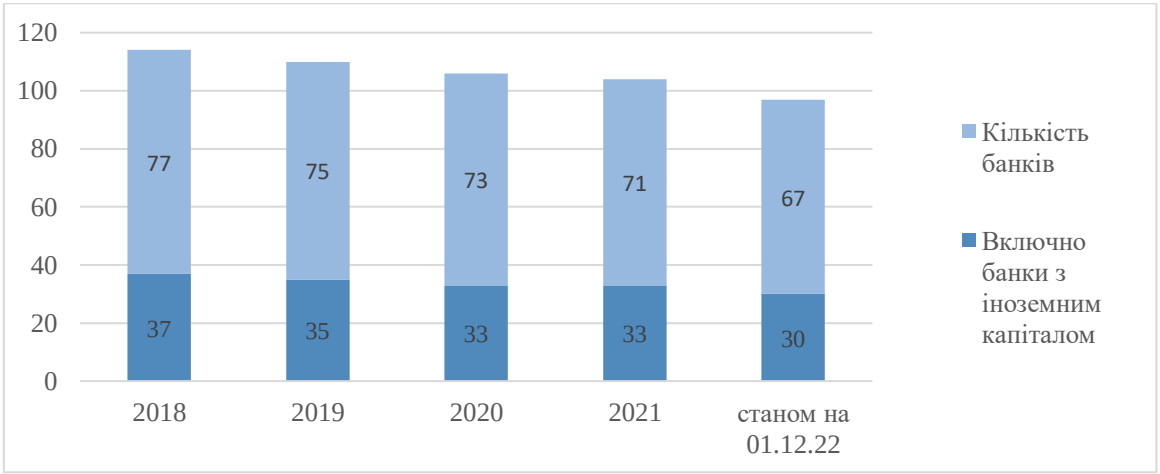

Рис. 1. **Кількість банків в Україні [12]**

Значним кроком в 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 від 12 серпня 2022 року № 178 «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» [13]. Національний банк унормував питання організації і забезпечення кіберзахисту в банківській системі України та визначив:

- основні засади функціонування системи кіберзахисту;

- принципи забезпечення інформаційного обміну між Центром кіберзахисту Національного банку і банками України;

- вимоги щодо заходів із забезпечення кіберзахисту об'єктів критичної інформаційної інфраструктури;

- вимоги щодо проведення незалежного аудиту інформаційної безпеки банків.

Система кіберзахисту в банківській системі України включає суб'єктів, упроваджених систем, комплексів та засобів забезпечення кіберзахисту, взаємопов'язаних заходів організаційного, технічного, інформаційного характеру щодо забезпечення належного рівня кібербезпеки та кіберстійкості системи України. Для цього створений при НБУ Центр кіберзахисту [13].

Крім того, Національний банк України з врахування вимог ЄС встановив відповідальність у разі порушення банківськими установами вимог нормативно-правових актів з питань захисту критичної інфраструктури, кіберзахисту та інформаційної безпеки, оскільки при масштабній загрозі, це може призвести до дестабілізації та платоздатності банківської системи в цілому.

Висновки. Протидіяти кіберзлочинам в сучасних умовах є завданням не тільки міжнародних організацій, а й національних регуляторів в кожній країні. Цей комплекс повинен включати правові, технічні, організаційні та інформаційні заходи й інструменти, ефективність яких залежить від своєчасного виявлення фінансових операцій, що можуть бути пов'язані з

кіберзлочинністю, використанням банківських установ для відмивання коштів, фінансуванням тероризму.

Тому важливим кроком в управлінні кібернетичними ризиками в банківській діяльності є чітко розроблена правова база на основі якої учасники електронно-дистанційного мережі матимуть базу захисту та знатимуть свою відповідальність. Не менш важливим способом кібербезпеки банківського сектору є залучення надійних інвесторів для фінансування заходів забезпечення надійного кіберзахисту, використання послуг кіберстрахування, підготовка кадрів з питань кібербезпеки, вчасне оновлення програмного забезпечення до актуальних, розвиток міжнародного співробітництва.

Таким чином, кібербезпека банківського сектору починається із заходів, які використовує сама банківська установа на основі найсучасніших цифрових технологій, забезпечуючи інформаційну безпеку не тільки банку, а й всієї країни. При цьому важливим на кожному етапі захисту від кібернетичних атак є застосування ефективних способів управління стратегічними, операційними, комплаєнс-ризиками та кіберризиками.

Список використаних джерел

1. Цифрові технології у банках в умовах війни: кейс IBOX BANK та міжнародний досвід (31 серпня 2022). URL: https://ua.news/ua/money/tsyfrovye-tehnologyy-v-bankah-v-uslovyyah-vojny-kejs-ibox-bank-y-mezhdunarodnyj-opyt (дата звернення 30.01.2023)

2. Абрамова А. С. Система ризиків діяльності комерційних банків в умовах цифровізації. *Проблеми і перспективи економіки та управління*. 2021. № 4(28). С. 186-193.

3. Barr, M.S., Harris, A., Menand, L., & Xu, W. Building the Payment System of the Future: How Central Banks Can Improve Payments to Enhance Financial Inclusion. *Center on Finance, Law & Policy*. 2020. P. 1-28. URL: https://financelawpolicy.umich.edu/sites/cflp/files/2021-07/cbotf-paper-3-future-payment-systems.pdf (дата звернення 06.01.2023).

4. Трофіменко О. Г., Прокоп Ю. В., Логінова Н. І., Задерейко О. В. Кібербезпека України: аналіз сучасного стану. *Захист інформації*. 2019. Т. 21, № 3. С. 150-157.

5. Forcadell F. J., Aracil E., & Úbeda, F. The Impact of Corporate Sustainability and Digitalization on International Banks' Performance. *Global Policy*. 2020. № 11 (S1). P. 18-27. https://doi.org/10.1111/1758-5899.12761

6. Regulatory complexity and the quest for robust regulation: Reports of the Advisory Scientific Committee. URL: https://www.esrb.europa.eu/pub/pdf/asc/esrb.asc190604_8_regulatorycomplexityquestrobustregulation~e63a7136c7.en.pdf (дата звернення 03.01.2023)

7. Кондрацька Н. М., Любовська М. М. Фінансово-економічна безпека банківських установ: загрози та шляхи їх подолання. *Вісник НУВГП. Серія «Економіка»*. 2019. № 4(88). С. 51-63.

8. Bahuguna, A., Bisht, R.K., & Pande, J. Country-level cybersecurity posture assessment: Study and analysis of practices. *Information Security Journal*. 2020. № 29 (5). P. 250-266.

9. Eisenbach, T.M., Kovner, A., & Lee, M.J. Cyber risk and the U.S. financial system: A pre-mortem analysis. *Journal of Financial Economics*. 2022. № 145(3). P. 802-826. https://doi.org/10.1016/j.jfineco.2021.10.007.

10. ISO/IEC 27001 and related standards Information security management. URL: https://www.iso.org/isoiec-27001-information-security.html (дата звернення 02.01.2023)

11. International Society of Automation. ISA/IEC 62443 standard. URL: https://www.isa.org/standards-and-publications/isa-standards/search (дата звернення 02.01.2023)

12. Національний банк України. URL: https://bank.gov.ua/ (дата звернення 04.01.2023).

13. 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 від 12 серпня 2022 року № 178. URL: https://bank.gov.ua/ua/legislation/Resolution_12082022_178 (дата звернення 12.02.2023)

References

1. Tsyfrovi tekhnolohii u bankakh v umovakh viiny: keis IBOX BANK ta mizhnarodnyi dosvid (31 serpnia 2022). URL: https://ua.news/ua/money/tsyfrovye-tehnologyy-v-bankah-v-uslovyyah-vojny-kejs-ibox-bank-y-mezhdunarodnyj-opyt [in Ukrainian]

2. Abramova A. S. (2021). Systema ryzykiv diialnosti komertsiinykh bankiv v umovakh tsyfrovizatsii. *Problemy i perspektyvy ekonomiky ta upravlinnia*, № 4(28), 186-193 [in Ukrainian].

3. Barr, M. S., Harris, A., Menand, L., & Xu, W. (2020). Building the Payment System of the Future: How Central Banks Can Improve Payments to Enhance Financial Inclusion. *Center on Finance, Law & Policy*, 1-28. URL: https://financelawpolicy.umich.edu/sites/cflp/files/2021-07/cbotf-paper-3-future-payment-systems.pdf

4. Trofimenko O. H., Prokop Yu. V., Lohinova N. I., Zadereiko O. V. (2019). Kiberbezpeka Ukrainy: analiz suchasnoho stanu. *Zakhyst informatsii*, 21, № 3, 150-157 [in Ukrainian].

5. Forcadell, F. J., Aracil, E., & Úbeda, F. (2020). The Impact of Corporate Sustainability and Digitalization on International Banks' Performance. *Global Policy*, 11(S1), 18-27. https://doi.org/10.1111/1758-5899.12761.

6. Regulatory complexity and the quest for robust regulation: Reports of the Advisory Scientific Committee. URL: https://www.esrb.europa.eu/pub/pdf/asc/esrb.asc190604_8_regulatorycomplexityquestrobustregulation~e63a7136c7.en.pdf

7. Kondratska, N. M., Liubovska, M. M. (2019). Finansovo-ekonomichna bezpeka bankivskykh ustanov: zahrozy ta shliakhy yikh podolannia. *Visnyk NUVHP. Seriia «Ekonomika*, № 4(88), 51-63 [in Ukrainian].

8. Bahuguna, A., Bisht, R.K., & Pande, J. (2020). Country-level cybersecurity posture assessment: Study and analysis of practices. *Information Security Journal*, 29 (5), 250-266.

9. Eisenbach, T. M., Kovner, A., & Lee, M. J. (2022). Cyber risk and the U.S. financial system: A pre-mortem analysis. *Journal of Financial Economics*., 145(3), 802-826. https://doi.org/10.1016/j.jfineco.2021.10.007.

10. ISO/IEC 27001 and related standards Information security management. URL: https://www.iso.org/isoiec-27001-information-security.html

11. International Society of Automation. ISA/IEC 62443 standard. URL: https://www.isa.org/standards-and-publications/isa-standards/search

12. Nacionalnij bank Ukrainy. URL: https://bank.gov.ua/ [in Ukrainian]

13. Pro zatverdzhennia Polozhennia pro orhanizatsiiu kiberzakhystu v bankivskii systemi Ukrainy ta vnesennia zmin do Polozhennia pro vyznachennia obiektiv krytychnoi infrastruktury v bankivskii systemi Ukrainy: postanova Pravlinnia Natsionalnoho banku Ukrainy vid 12 serpnia 2022 roku № 178. URL: https://bank.gov.ua/ua/legislation/Resolution_12082022_178 [in Ukrainian].